Search RISKS using swish-e

THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

ACM Committee on Computers and Public Policy, Peter G. Neumann, moderator

Index to Volume 11

Sunday, 30 June 1991

Search RISKS using swish-e

Report problems with the web pages to the maintainer

THE RISKS DIGEST

Forum On Risks To The Public In Computers And Related Systems

ACM Committee on Computers and Public Policy, Peter G. Neumann, moderator

Search RISKS using swish-e

The RISKS Forum is a moderated digest. Its USENET equivalent is comp.risks. (Google archive)

- Vol 26 Issue 47 (Monday 6 June 2011) <= Latest Issue
- Vol 26 Issue 46 (Saturday 4 June 2011)
- Vol 26 Issue 45 (Tuesday 24 May 2011)

- News about the RISKS web pages
- Subscriptions, contributions and archives

Feeds

RSS 1.0 (full text)

RSS 2.0 (full text)

ATOM (full text)

RDF feed

WAP (latest issue)

Simplified (latest issue)

Smartphone (latest issue)
Under Development!!

You can also monitor RISKS at Freshnews, Daily Rotation and probably other places too.

Please report any website or feed problems you find to the website maintainer. Report issues with the digest content to the moderator.

Selectors for locating a particular issue from a volume

Volume number: Volume Issue Number: Issue

Get Specific Issue

Volume Index

The dates and counts do not include the index issues for each volume.

Index to the RISKS Digest

Volume Number	Date Range	Number of Issues
Volume 1	*1 Aug 1985* - *31 Jan 1986*	*45 issues*
Volume 2	*1 Feb 1986* - *30 May 1986*	*56 issues*
Volume 3	*4 Jun 1986* - *30 Oct 1986*	*91 issues*
Volume 4	*2 Nov 1986* - *6 Jun 1987*	*96 issues*
Volume 5	*7 Jun 1987* - *31 Dec 1987*	*84 issues*

Volume 6	2 Jan 1988 - 31 May 1988	94 issues
Volume 7	1 Jun 1988 - 22 Dec 1988	98 issues
Volume 8	4 Jan 1989 - 29 Jun 1989	87 issues
Volume 9	6 Jul 1989 - 30 May 1990	97 issues
Volume 10	1 Jun 1990 - 31 Jan 1991	85 issues
Volume 11	4 Feb 1991 - 28 Jun 1991	95 issues
Volume 12	1 Jul 1991 - 24 Dec 1991	71 issues
Volume 13	6 Jan 1992 - 2 Nov 1992	89 issues
Volume 14	4 Nov 1992 - 27 Aug 1993	89 issues
Volume 15	2 Sep 1993 - 29 Apr 1994	81 issues
Volume 16	2 May 1994 - 22 Mar 1995	96 issues
Volume 17	27 Mar 1995 - 1 Apr 1996	96 issues
Volume 18	5 Apr 1996 - 31 Mar 1997	96 issues
Volume 19	1 Apr 1997 - 23 Sep 1998	97 issues
Volume 20	1 Oct 1998 - 31 Jul 2000	98 issues
Volume 21	15 Aug 2000 - 29 Mar 2002	98 issues
Volume 22	1 Apr 2002 - 27 Oct 2003	98 issues
Volume 23	7 Nov 2003 - 2 Aug 2005	96 issues
Volume 24	10 Aug 2005 - 30 Dec 2007	93 issues
Volume 25	7 Jan 2008 - 1 Apr 2010	98 issues
Volume 26	8 Apr 2010 - 6 Jun 2011	47 issues

Search RISKS using swish-e

THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

ACM Committee on Computers and Public Policy, Peter G. Neumann, moderator

Volume 11: Issue 1

Monday 4 February 1991

Contents

Re: Enterprising Vending Machines

Allan Meers - Sun Education <allans@ebay.sun.com>
Thu, 31 Jan 91 22:21:02 PST

USER-HOSTILE VENDING-MACHINE PROGRAMMING

My wife stopped at a Post Office yesterday to buy some stamps, and had a run in with some technology. They have a vending machine for stamps, which takes old-fashioned paper money of up to $20 denominations. To prevent you from using the machine as a change machine, the bill-counter attachment is programmed to give you change of a very limited amount, forcing you to spend

about 2/3 of whatever cash you insert. She tried a $10 in this USPS slot-machine.

Not until she had put money into the bill-counter would it tell her that the selection was sold out by saying so on a display above the selection buttons. There were no little soldout lights by each sample like on some types of machines, and the display would not activate until you fed some cash into this one-armed bandit. Worse yet, even for a sold-out selection, you had to put in as much money as the selection costs to find out that it was sold out - otherwise the first/only message you got was "Need $.cc more".

Fortunately the common stamps were in multiple channels - unfortunately these were all sold out also. So here's the rock and the hard place. There is no sold out lights, no display on the panel without some money, no indication that a particular selection is sold out til you have put in enough money (which can be up to $25.00), and NO refunds without purchase. Additionally, you have to spend about 70% of the cash you put in. Goldie settled on a bunch of 15c postcard stamps that can be used next week when the letter rates go to 29c.

The risk here is that this machine is meant to be used by the general public, and many of them are likely to be using it for the first time. It's operation and behavior differ greatly from the more normal soda and candy machines, unfortunately - with much greater amounts of cash involved than with a Snickers bar.

The bill-collecting portion appears to be an added-on unit, with no feedback from the dispensing unit regarding product availability until AFTER the money part has received the purchase price for that selection. Extra programming added in later to prevent the machines use as a change machine (for the bus stop outside), did not take into account sold-out selections - which should have been checked first, with or without money. I believe that this unit was a retrofit on an old machine, with additional programming adding later making it a one-of-a-kind unit which acts like it didn't get much QA on the customization.

SUMMARY:

No (sold out) light always on.

No light if you push the button without money to test.

No light even with money entered, unless the amount is enough for that particular selection.

No refund without purchase.

No tag backs, no refunds, all sales final - gotcha.

I kinda thought you would appreciate the risks of a hostile-programmed vending machine. Especially one that would be in an environment like a post-office, where people wouldn't necessarilly use it every day, and with a high percentage of first-time users, who could get skunked by the over-zealous application of the rules.

Re: Risks of automatic flight

<henry@zoo.toronto.edu>
Fri, 1 Feb 91 00:52:25 EST

>It's ludicrous to believe that any airman would allow his pink flesh to be
>routinely thrown at the ground without some control ...

I can think of one possible legitimate motive for this, which makes it a bit less ludicrous than it first sounds. The way for aircraft to survive in combat is to get as low as possible. In a real war, with serious and capable opposition (it is not clear whether Iraq qualifies at present), a lot of flying would be done at altitudes circa 50 feet. The trouble is that flying at 50ft is very different from flying at 500ft, which is a more usual training altitude for the USAF. The South African air force trains at 50 ft. So do the Israelis. But the USAF considers training at realistic altitudes to be unacceptably dangerous for peacetime. The intent might have been to get the benefits of the low altitude without the political difficulties of relatively dangerous peacetime training or the fearful attrition rate associated with having to learn new basic skills while being shot at.

Henry Spencer at U of Toronto Zoology utzoo!henry

Voting by Phone & public-key cryptography

Evan Ravitz <eravitz@isis.cs.du.edu>
Fri, 1 Feb 91 08:54:08 MST

Phil Zimmerman (prz@sage.cgd.ucar.edu (303)444-4541) is a computer security consultant working with the Voting by phone foundation on public-key cryptographic protocols used for voter authentication and privacy. His group's scheme would prevent the government from entering bogus votes, using the PINs of those who had not voted at the end of the election, to use PGN's example.

For those who doubt that a PIN could not be anonymous I suggest drawing them from a hat (perhaps using a device like we used to select gumball prizes with). The other worries, like caller ID and wire-tapping can be avoided by simply voting from any other phone. I'm sure I pass a dozen a day.

Paranoia is justified, but apply it to how we vote now, as well. Don't you think that a government that can photograph your license plate from outer space can install a tiny video camera that watches how you vote in a booth?

Please read our brochure (E or regular mail) before picking at a system you don't have full info on. Contact Phil for his ingenious cryptographic system, or myself for the brochure (eravitz@nyx.cs.du.edu)

Re: Random Voting IDs and Bogus Votes (Vote by Phone)

Mike Beede <beede@SCTC.COM>
Fri, 1 Feb 91 12:24:07 CST

>Each voter is given an id number to vote, but is told that the number is either
>positive or negative. Suppose there are two candidates, Alice and Bob. If the
>number is negative, a vote for Alice is actually counted as a vote for Bob.

Now suppose there are four candidates. We give each voter a complex number X. A vote for Alice is (1+i)X, while Bob is (1-i)X, Carol is (-1+i)X, and Ted is (-1-i)X. For up to 16 candidates we issue each voter a quaterion, but this has the drawback that only people with graduate degrees in mathematics are able to vote.

I believe that phone voting is trying to solve a problem that is already solved pretty well. The goals are 1) make it convenient for the voter to vote, 2) make it impossible, or nearly so, to determine anyone's vote, and 3) make it very difficult to falsify results. I argue that 1) is already met closely enough that the virtual sacrifice of 2) and 3) in the vote-by-phone schemes are not justified in the least.

Mike Beede, Secure Computing Technology Corp, 1210 W. County Rd E, Suite 100
Arden Hills, MN 55112 (612) 482-7420

Re: Patriot (Leichter, RISKS-10.85)

Steve Mitchell <steve@caticsuf.CSUFresno.EDU>
Fri, 1 Feb 91 09:31:15 PST

A thought on the RISKS of evaluating the Patriot system's performance:

The arguments I've heard in the digest and in the media lately seem to leave out an important aspect of this discussion. By pointing out numerous successes in the Persian Gulf theater, proponents of this system, proponents of complex weapons systems, and even advocates for SDI are now implying that ALL of their Patriots, complex weapons systems, and SDI systems will function *as promised*. The question here has never been whether the Patriot can shoot down rather easy targets. The question here (and the question in evaluating the cost/performance ratio, practicality, and effectiveness of any weapons system), is whether the Patriot system can function in the role for which it was designed.

If the Iraqi's had effective ECM operating, radar busting aircraft deployed, and were attempting coordinated attacks on these cities with maneuverable aircraft, would the Patriot be as effective as it was designed to be? The results from the Persian Gulf theater are inconclusive at best. The Patriot system's design advantages and sophistication, the very aspects of the system that make it so expensive, are still relatively untested in combat. These are the aspects of the system that have been used to rationalize it's development and deployment costs.

If GM claimed that it's new Family Van Mk IV was amphibious, would you label it a magnificent success just because you saw 30 of them cruise down the highway

at 50 MPH? If all you need is a Family Van that can cruise down the highway at 50 MPH, why not save a few million and go for the Family Van Mk III that doesn't claim the amphibious capabilities.

I do not feel that the Patriot's "amphibious" capabilities have been demonstrated here.

Steve_Mitchell@csufresno.edu

Re: Patriots: Reprogramming, SDI implications (RISKS-10.82)

Steven Philipson <stevenp@decwrl.dec.com>
Thu, 31 Jan 91 16:09:04 -0800

Nathaniel Borenstein <nsb@thumper.bellcore.com> writes:
>I'm awestruck that they're willing to reprogram the Patriot [...] right
>in the middle of the war! [...]

Wartime modification and upgrade of systems is a common and time honored practice by military units. Experience is gained on a daily basis and both sides modify both their systems and tactics to make use of it. If one can't adapt, one is placed at a tremendous disadvantage. It would likely be deemed unacceptable if modifications could NOT be made in this timeframe.

>[...] Patriots may never again be as useful as they are being in this war,
>because "now that their capabilities are known, it will be trivial to
>make the next generation of missiles able to fool them.

There are large inventories of missiles with current and relatively outdated technologies. The SCUD itself is considered an archaic weapon. The Patriot will have a place in defense against these weapons. Patriot upgrades, both software and hardware, will likely increase effectiveness against more advanced threats. Certainly current assessments of their capabilities will be of limited usefulness in estimating future performance.

karn@thumper.bellcore.com (Phil R. Karn) writes:

>Even the Pentagon admits Patriots are of little use against SCUDs armed
>with chemical warheads since they would merely disperse the chemical over
>the target. [...]

If such dispersal were guaranteed, then the Patriot would be an effective countermeasure. Chemical weapons are effective only when chemicals can be delivered with sufficient concentration. Isolated high altitude airbursts of the chemical containers will cause the material to disperse as it descends, this lessening concentration and reducing effectiveness.

One of the things we've seen with the Patriots is that some but not all intercepts disable warhead arming. Thus some intercepted SCUDS hit the ground without detonating, but some explode anyway. This has major implications for an SDI terminal area defense against nuclear weapons for which a nuclear near-miss may be as good as a direct hit.

Steven Philipson

Re: Patriot Missile

Michael H. Riddle <riddle@hoss.unl.edu>
Fri, 1 Feb 91 08:18:46 cst

Until about a year ago, my brother worked for Teledyne Brown Engineering in Hunstville, on contract to the Army Ballistic Missile Division. He claims credit for a small part of the SDI technology that was retrofit to the Patriot, although for obvious security reasons will not say more. He has confirmed, however, that SDI technology was used in some of the follow-on modifications to both the Patriot missile itself (rocket motors) and the command/control radars and software.

riddle@hoss.unl.edu postmaster%inns@iugate.unomaha.edu
University of Nebraska, College of Law, Lincoln, Nebraska, USA

SDI -> Patriot? and related topics

Fri, 1 Feb 1991 07:17:20 PST

> The [Patriot] system was contracted for 15 years ago by the Redstone
> Arsenal. It was initially to be an anti-aircraft missile, and it still
> is, but about four years ago, unspecified software upgrades on the ground
> equipment and hardware upgrades on the missile's detonation fuze were
> made so that the system willa also be able to destroy tactical missiles,
> such as the Russian Scud.

> Various news organizations have alluded to or asserted outright that the
> upgrades are technologies developed under the Strategic Defense
> Initiative program. "That is bull! There is no 'Star Wars' hardware or
> software in Patriot," [Redstone Arsenal public affairs officer David]
> Harris said. "There has been no 'Star Wars' funding of Patriot. This is
> all Army." He said the SDI Organization is planning to provide $40
> million for continuing development of the Patriot's advanced seeker
> (nose-cone radar), but it has not been received by the Army yet.

This from "Portrait of a Patriot" by Brian Santo. Unfortunately I have no idea where this appeared; the clipping was posted in our coffee room this AM and I have been unable to run down the source! However, the technical content is high and consistent, so I am inclined to believe that the foregoing is a true reflection of the [US Army Missile Command's version of the] history of the Patriot.

The article *does* assert that "[t]he missile itself has its own radar. . .which kicks in as it nears its target," but the description of operation is otherwise consistent with Henry Spencer's recent posting (RISKS DIGEST 10.85):

> Even Patriot's homing is actually controlled by the ground computers; the
> missile itself has no brains to speak of, just a receiver system that
> picks up radar reflections off the target and relays them to the ground

> for assessment

so possibly a passive radar was meant but not explicitly stated. On the other hand, if SDIO sees an application it seems more likely that the Track Via Missile (TVM) radar is active, not passive.

Finally, in the same message Henry remarks

> I've never understood why it is fundamentally impossible to put "man in
> the loop" for space-based systems. I'd be interested in seeing this
> explained. There is clearly a serious shortage of time for
> decision-making, but the same is true of terminal defence against
> tactical missiles -- which have much shorter flight times than ICBMs --
> and short-notice decision-making in combat is both possible and
> practical, as any fighter pilot can testify.

I'd say alertness. Crews, even highly-trained fighter pilots, need time to come up to combat-readiness from standby. Note that in the current case of "terminal defence against tactical missiles" (Santo again)

> [t]he detection and firing sequence is entirely automatic, and the only
> intervention required of a human operator is to stop the Patriot from
> firing.

This kind of tripwire arrangement looks unacceptable, at least for boost phase. I suppose one could quibble over the the use of the word "fundamentally," but *I* wouldn't want to have to design a robust system of this type.

Mark <MJackson.Wbst147@Xerox.COM>

Patriots

"Clifford Johnson" <GA.CJJ@Forsythe.Stanford.EDU>
Fri, 1 Feb 91 10:16:27 PST

Henry writes:
> The recent incident of an accidental launch against
> aircraft is silly as a test case, since the Patriot system
> reportedly was in antimissile mode and thus probably wasn't
> expecting evasive action.

It would seem that this mistake exhibited a flaw in the antimissile software design, though further details are needed for confirmation. Namely, there was no effective software check of observed radar track for ballistic trajectory. A launch against returning planes should have been precluded by a simple trajectory test.

Man-in-the-loop on SDI

<henry@zoo.toronto.edu>

Fri, 1 Feb 91 12:59:22 EST

> ... one could quibble over the the use of the word "fundamentally," but
> *I* wouldn't want to have to design a robust system of this type.

The question, of course, is whether one can design a better system without humans involved, where "better" includes not just probability of functioning well when desired but probability of functioning when not desired. If you compare fallible, inattentive humans against the Pentagon's imaginary perfect computers, then of course you conclude that the man-in-the-loop system is inferior. Against real computers running real software, I'm not so sure.

Henry Spencer at U of Toronto Zoology
henry@zoo.toronto.edu utzoo!henry

Re: Broadcast local area networks (Cooper, RISKS-10.84

Curt Sampson <curt@cynic.wimsey.bc.ca>
Thu, 31 Jan 91 03:42:27 PST

> From: Brinton Cooper <abc@BRL.MIL>
> Subject: Re: Broadcast local area networks are a'comin (Tom.Lane, RISKS-10.83

Brinton Cooper <abc@BRL.MIL> writes:

> the risk for spectral chaos seems to be quite high. Imagine the RFI
> (radio frequency interference) implications of a central city full of
> wireless ethernets(tm?) attempting to coexist with cellular phones, [etc.]

Interference will only be had by devices operating on the same frequencies. If the networking system is given its own band of frequences it won't interfere with cellular phones any more than FM radio does.

There are other risks to this scheme, though. Ethernet is based on a collision detection scheme. If two nodes send out a message at the same time they detect the collision (because the data is scrambled) and then wait a random amount of time before retrying the send. It would be relatively simple to build a small box which would output a short burst of RF every few milliseconds. The more often this box "squawked" the more collisions it would create on the network and the slower the network would get. Generate these pulses often enough and you could bring the entire network to a halt. The box would certainly be able to operate for several days powered from a normal nine volt battery, and would be small enough to hide easily.

Now what if several major financial firms relied on wireless networks in their office and I decided that I wanted to create a little chaos and impede their ability to respond on the morning of a large takeover bid? Simply drop by for a "visit" and toss one of these boxes in a nearby garbage can.

curt@cynic.wimsey.bc.ca curt@cynic.uucp {uunet|ubc-cs}!van-bc!cynic!curt

---

Re: Broadcast local area networks are a'comin

<Donald.Lindsay@GANDALF.CS.CMU.EDU>
Thu, 31 Jan 1991 23:28-EST

I'm not familiar with Apple's proposal, but I am very pleased with Motorola's WIN (Wireless In-building Network) proposal.

WIN is to use 10 MHz channels within the 18-19 GHz band, and this has some very special propagation characteristics. Each "microcell" network can ignore another network's use of the same channel, 120 or 200 feet away - less if a concrete floor or wall intervenes. (Unlike infrared, 18 GHz can pass through drywall and partitions.)

The system uses "low power" (I don't have a number). It also uses a fair bit of multiplexing and packetizing, with source/destination pairs changing at 1 MHz. But best of all, 18 GHz reflects off walls, causing a considerable multipath problem (ie multiple out-of-phase copies of the signal). Some very clever design was required to allow in-cell reception at all: things should be pretty well incoherent, a very small distance away. WIN is probably as secure as the office suite it's in.

Don D.C.Lindsay .. temporarily at Carnegie Mellon Robotics

Re: broadcast LANs (Letts, RISKS-10.85)

John Stanley <stanley@phoenix.com>
Fri, 01 Feb 91 15:58:51 EST

->Reading the notices about the approach of broadcast LAN's reminded me of a
->semihumorous incident that happened about 2 years while I was doing some
->consulting for a "local" oil company. ...

->All of the remote telemetry units were communicating with the
->master station computer via low power Johnson radios, and I had made sure that
->we had dummy loads on all of the antennae so as to cut down the range of the
->transmissions. This screwed up SWR's and about everything else,

Dummy loads are designed not to screw up the SWR's. They are a perfect match, unless you are using the wrong dummy loads. Somehow, in this case, that wouldn't surprise me. But I quote this section as anecdotal evidence that the system was not licensed for data communications work.

->Sporadically, we would get bursts of errors for seemingly no reason, and then
->good comm again for a while. ...

->Much to my surprise, I heard
->some poor fella in a delivery truck complain about "there's that doggone
->buzzing sound again" to his dispatcher at the same time that our comm
->efficiency dropped to zero!

This is quite humorous. Ha. And quite lucky that you were not using radios that just happened to be tuned to the hospital or other emergency frequency. But you were probably saved by using radios that were licensed for business band voice communications, so all you screwed up were all the other users of that frequency.

->It was kinda fun listening to all of those guys swear at the strange
->interference that they were getting.

Yes, many sick people DO find it quite a hoot to cause deliberate interference to licensed users of the spectrum (and the moment you identified the source of the interference to YOU, you became deliberate interference to the pizza service). I don't think the FCC feels like it is a fun game. They tend to levy fines on people for doing it.

---

re: Broadcast local area networks are a' comin

Jerry Leichter <leichter@lrw.com>
Fri, 1 Feb 91 17:37:29 EDT

Two responses to points raised by some recent messages on this issue:

1. Ian Clements is concerned about possible effects on medical devices such as implanted heart monitoring devices. All thing are possible, but there are already TONS of transmitters out there. This is hardly a new or poorly understood problem. However, note that a broadcast LAN, designed to work over a 150 foot radius, is likely to use much lower power than a cellular telephone, which must work over many miles.

2. Rich Rosenbaum comments that some of these technologies use spread-spectrum techniques, hence may be inherently secure. Well, yes and no - but mainly no. There are several different spread-spectrum techniques, but let's take a simple one, frequency hoping. In this technique, we select a broad channel - say 100Mhz wide. We consider it to be subdivided into 100 1Mhz-wide slots. Traditionally, we then parcel those slots out to 100 users. In frequency hoping, we instead send signals on ALL the bands. Each "channel" corresponds to a sequence of slots spread over the entire channel. The sender hops through its sequence at a rapid rate - say, it switches every millisecond. The receiver follows the same sequence of slots, synchronized with the sender. A receiver that follows some other sequence has only a one in a hundred chance of intercepting the signal at any given time. So a receiver listening on a a "channel" receives very little junk from any given unrelated channel. It's possible to choose a large number (<> 100) of different "channels" (sequences) such that any subset of, say, 20 transmitting hardly interfere. This means that you can have many more than 100 users on the channel, who can almost always get through (unless too many want to do so at once).

Now, if you don't know the particular sequence the sender is using, you have a hard time reading his message. In fact, it's not even easy to tell that he's sending! The acronyms in use to describe this stuff include LPD/LPI/LPE (Low Probability of Detection (enemy can't even tell you are there)/Intercept (enemy knows you are sending but can't extract any significant features of the message)/Exploitation (even if the enemy can "read" your signal, he can't tell what it means)). The flip side of this is AJ, Anti-Jam (i.e., jam-resistant).

However, keeping the sequences secret complicates the system. It's much simpler to use fixed, pre-assigned, publically known sequences. What's traded off is the protection the modulation technique COULD provide. In the case of a broadcast LAN, LPD and LPI are of little importance; what you care about is LPE. If you were to use strong, secret sequences, you'd get those - but the hardware needed (which must generate a cryptographically strong sequence of slot numbers) is comparable to the hardware you'd need to do encryption, and you'd still have to add all sorts of stuff to complete the system: You can use the same key safely on a lot of different messages, but you can never safely re-use a hop sequence (so there's a whole synchronization problem to solve).

-- Jerry

Search RISKS using swish-e

THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

ACM Committee on Computers and Public Policy, Peter G. Neumann, moderator

Volume 11: Issue 2

Tuesday 5 February 1991

Contents

Bogus draft notices are computer generated

Jonathan Rice <rice@willow.cray.com>
Tue, 5 Feb 91 9:21:58 CST

Last night's local news reported that "hundreds, perhaps thousands" of draft notices have been posted around the Minneapolis campus of the University of Minnesota. The official looking notices are replete with convincing official jargon, announcing that men in a certain age group are to report for immediate duty. Readers are directed to report to a room in the Hennepin County Courthouse (the room is vacant) or to call one of two telephone numbers. The numbers are those of the Minneapolis Star & Tribune news desk, and of a blameless lady in St. Paul who seemed from the interview to have kept her sense of humor despite the barrage of calls. Interviews with young men on campus indicated that many had not thought to doubt the authenticity of the notices.

What caught my ear was a statement that University officials would be "checking their computer facilities" to see if the notices had been composed and printed there.

The risk is one that has been pointed out before: laser printers enable several types of fraud -- forged checks, phony invoices, letterheads for nonexistent businesses -- that once would have been ruled out by the need to have a professional print shop as an accomplice. But this is a new twist.

Jonathan C. Rice, Cray Research, Inc., 655F Lone Oak Drive Eagan, MN 55121
UUCP: uunet!cray!rice 612-683-5370

People working at home on important tasks

Mike Albaugh <albaugh@dms.UUCP>
Mon Feb 4 15:22:33 1991

An article on the accuracy of medical tests in the latest "Parade" (a syndicated Sunday Supplement) had the following "interesting" statement. Some context: A women died of cervical cancer not detected due to screwups in handling her pap smear. The lab tech who mishandled the test in question was working at home. The woman's attorney is quoted:

> "Working at home might be fine for computer programmers, but it's reckless when your job involves making selective judgements that can affect someone's life."

We can all rest easier knowing that computer programmer's can have no negative effect on people's lives.

Mike Albaugh

Predicting system reliability

Martyn Thomas <mct@praxis.co.uk>
Mon, 4 Feb 91 17:14:45 BST

It is hard to define what evidence we need, in order that we can have confidence that a system meets its designed level of reliability.

(I am using reliability, loosely, to mean that the system does what you wanted it to do, when you wanted it, for the period that you wanted it).

It seems clear that the following argument is unsound:

System X has been shown to meet its requirements.
System Y is no more difficult than System X.
Therefore System Y meets its requirements.

Therefore, even if an SDI system had been shown to work before, it would not be evidence that a new SDI would work. A fortiori, any degree of success of the Patriot system provides no evidence that SDI would work.

I think the confusion arises because two different arguments get conflated:

Argument 1: A system as complex as SDI could never be designed so that it worked correctly. (I do not support this argument - any [computable] system *could* be designed so that it worked correctly [even by chance]. I am more interested in how we accumulate the evidence which allows us to form the opinion that a *particular* system has achieved its design objectives. This is argument 2, below).

Argument 2: A system as complex as SDI can never be evaluated in a way which would give reasonable grounds for claiming that it would work correctly when deployed. (I believe that this is true. SDI would be too complex for formal proof of correctness - and the specification may be wrong. SDI would be impossible to test under operational conditions. In general you need to test for more than 10 times the period of fault-free operation you are looking for, with no faults found, to achieve 99% confidence that you will meet the requirement. SDI would probably only need to work correctly for a few days, so a few weeks fault-free operation [under operational conditions - ie under attack!] would demonstrate achievement. The time isn't the problem, but creating the test conditions is surely impossible).

When we move the argument to some other safety-critical systems, the time factor becomes dominant. A constant-control system, such as the A320 fly-by-wire, needs 10^-8 probability of failures per hour. This implies 10^9 hours of fault-free operation to justify a claim (to 99% confidence) that the requirement has been met. This is clearly absurd, so how do we judge whether or not the requirement has been met?

On-demand critical systems, such as spacecraft course-correction or reactor shutdown systems, may only need to operate correctly for a few minutes or hours during their whole design lifetime. This is clearly testable (if we can be sure that the operational conditions can be reproduced accurately enough - which becomes the problem).

I would welcome further discussion of these basic questions: how should we form an opinion about the probable future reliability of a system; what justification is needed for that opinion, if it is to stand up to critical appraisal by other engineers; what is the practical limit (in terms of failures/hour) which we can realistically expect to be able to justify, and how is this limit affected by the complexity of the system?

Martyn Thomas, Praxis plc, 20 Manvers Street, Bath BA1 1PX UK.
Tel: +44-225-444700. Email: mct@praxis.co.uk

Re: Patriots (RISKS-10.83)

Steven Markus Woodcock <swoodcoc@isis.cs.du.edu>
Mon, 4 Feb 91 23:30:55 MST

Regarding the use of Patriots:

I work for Martin Marietta, and know several people who helped design and build the Patriot. I also work at the National Test Bed, so I'm quite familiar with SDI's role in the Patriot's development.

The Patriots fired at the aircraft in Turkey missed precisely because they were loaded with terminal defense missile software--a much simpler interception problem than hitting an aircraft that's actively avoiding you. If they had been loaded with their anti-aircraft software, it would probably have been a different story (although isn't there a ground destruct override on those things?).

Patriots, ballistic missiles and aircraft

Mark Levison <levisonm@qucis.queensu.ca>
Tue, 5 Feb 91 12:29:24 EST

On the subject of the Patriot missile system: while the SCUDs they are firing against are archiac, the basic problems do not change. The only short to medium range ballastic missile that change the problem significantly was the Pershing II. This system had a terminal guidance phase, allowing course changes during or after a counter missile launch. Improvements in ballastic missile technology since the SCUD are in the areas of speed (not significant), accuaracy, range and payload.

Against aircraft the problem changes significantly, while aircraft are capable of evasive action they are also much slower moving targets typically Mach 0.6 (for an A6 or A10 on an attack run) to Mach 2+ (fast moving ie Mirage F1, 2000 etc) vs Mach 3 - 7 for a ballastic missile. So ignoring ECM, chaff and similiar capabalities aircraft should not significantly more difficult than ballastic missiles. Of course we have not seen and hopefully will never need to see examples of the Patriot system shooting down an aircraft in a real combat situation.

As should be obvious here I am only trying to demonstrate that Patriot missile is probably capable of doing the job that its designers claim it can do. I am ignoring all issues of ECM and radars because of my scant knowledge in this area. I am also ignoring whether you actually want to shoot down missiles that might be chemical/biological armed.

Mark Levison levisonm@qucis.queensu.ca

Hungry copiers (another run-in with technology)

Scott Wilson [CHTM] <swilson@pprg.unm.edu>
5 Feb 91 04:33:35 GMT

I too have encountered some poorly thought out additions to old technology. Get this:

Went down to the library to copy a paper. Didn't have enough change, but saw a bill changer on the machine. (What will they think of next?) Put in a $5 bill.

Put the paper in place, hit <COPY>. Machine grumbles, proceeds to hang, saying "Check Paper". I begins to smell a rat.

I track down the student assistants at the front desk - thay cannot fix the machine. They are the only attendants on duty (Murphy applies here). I press "Change return" and it says "Must make at least one copy".

The add-on bill changer was programmed to avoid use as a source of change by requiring at least one copy. If the machine jams on the first copy, your bill stays in until you can find a way to get it unjammed. If that cannot be accomplished, then your imaginary copy costs you the bill!

I figured that if I wasn't going to get the bill back by arranging to have the machine fixed, then I was at liberty to try other means. Found the power cord, unplugged said machine. Plugged back in. Bill changer complained about "out of order". Unplugged again. Plugged back in. Changer starts thumping, spews out my $5 bill. I guess it was trying to clear itself.

Too many more "consumer improvements" and I'll scream!

Scott Wilson

Re: Enterprising Vending Machines

<davy@erg.sri.com>
Tue, 05 Feb 91 08:23:29 -0800

Most post office vending machines I've used tell you to press the button before putting your money in, and it will tell you whether it's sold out or not. These are the USPS machines with the "light bar" for messages across the top and about four tiers of stamps.

So perhaps your surmise about this being an old retrofitted machine is correct.

--Dave

> [Dave and I share a vending machine in the Menlo Park CA Post Office that tells you to press the button before putting money. But first-time apparently get burned quite frequently. Here is another example of ordinary mortals having to gain sophistication in the vagaries of automated systems in order to maintain their cool. (My use of "their" was intentionally ambiguous.) PGN]

Broadcast LANs

Peter da Silva <peter@taronga.hackercorp.com>
Tue, 5 Feb 1991 04:56:03 GMT

A lesser problem that reduces the quality of the working environment is likely to be plain old EMI. Already it's impossible to tune AM radio stations in modern office buildings, and low-power FM ones (like the local PBS station) are kind of marginal. I'd hate to think of what a wireless LAN would do to my

Classical or Jazz fix, let alone All Things Considered.

Re: Broadcast local area networks are a'comin (Tom Lane, RISKS-10.83)

<scott@huntsai.boeing.com>
Tue, 5 Feb 1991 09:58:37 -0600

<>If I ran a corporate network, I wouldn't touch this with a 10-foot pole.

How much of your data on the average network is really a security issue?
I work here at Boeing and, at least in my area, sensitive data is not
kept on the network (and it is over 150' to the nearest area off campus
anyway, not to mention a couple of concrete/steel walls)

Even in a small company I bet most data could be sent with little to no
encryption without any danger of sensitive material being lost.

In summary this WOULD be a good system for many (most?) networks where
cost/difficulty of cableing would be a major deterent, but (due to
limited channels and security risks) it would not be for everyone.

The existence of security risks does not negate the possible benefits of
technology per say, but rather is a side effect that must be
acknowleged and responsibly handled.

Scott Hinckley, Boeing AIC, 110 Pine Ridge Road #608 Huntsville Al35801
(205)461-2073 UUCP:..!uunet!uw-beaver!bcsaic!huntsai!scott

Search RISKS using swish-e

THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

ACM Committee on Computers and Public Policy, Peter G. Neumann, moderator

Volume 11: Issue 3

Wednesday 6 February 1991

Contents

Tube Tragedy

Pete Mellor <pm@cs.city.ac.uk>
Tue, 5 Feb 91 21:43:18 PST

The Sun, Tuesday, February 5th, 1991, p. 6:

A tube passenger was dragged to his death after getting his arm trapped in a train's automatic doors.

Four pals inside the carriage watched as the victim was pulled along the platform and smashed against the tunnel wall at London's Kings Cross. He was then sucked under the moving train. But the friends have not come forward, and the man - believed to be Italian - has not been identified.

****

I was puzzled that this was not reported in the Guardian, or on the evening TV news, so I rang London Underground's PR department for confirmation.

It happened on Sunday night, on the Northern Line. Apparently the man, being separated from his friends as the doors closed, had opened them by operating the butterfly clasp on top of the carriage. (Presumably this is intended for staff use only, to open doors in exceptional circumstances.) The doors then closed faster than he expected, so trapping him before he could get on. (The fact that the butterfly clasp had been operated, presumably meant that no warning signal was sent.) According to the PR department, neither the guard (still employed on older parts of the underground) nor the driver were to blame. LU PR are surprised, however, that the man was able to reach and operate the clasp.

It looks like a case of "No system is foolproof. It all depends on the size of the fool!", but there may be some design implications here. Surely, for instance, a warning should be given if a door is open for *any* reason?

In the meantime, London Underground is making 1000 staff redundant to cut costs. According to one union leader, this will lead to unmanned stations at night, and take the underground closer to being a "passenger-hostile system".

Peter Mellor, Centre for Software Reliability, City University, Northampton Sq.,London EC1V 0HB +44(0)71-253-4399 Ext. 4162/3/1 p.mellor@uk.ac.city (JANET)

New Zealand Computer Error Holds Up Funds

<TASHKOVI@CRNLGSM.BITNET>
Wed, 6 Feb 91 11:40 EST

>From the New Zealand Herald, January 15th, 1991, p. 4.

NZPA -- Wellington A computer processing error at Databank has thrown many savings account balances out of kilter. Misalignment of account number suffixes prevented Databank's computers from identifying some recipient accounts. The computer posted payments to a safe holding file until the problem could be resolved, Databank said yesterday. Although current accounts (those with 00 suffixes) were not affected, accounts with other suffixes (such as 02, 03) may not have received payments made on Friday. This problem would show up on automatic teller machine and Eftpos inquiries into savings and special accounts. All bank in New Zealand were affected but the problem was expected to be resolved by start of business today, Databank said.

"Inquiry into cash machine fraud"

Stella Page <sp@cs.city.ac.uk>
Mon, 4 Feb 91 11:33:31 GMT

Extracts from Finance and Economics article, The Guardian, 1 February 1991:

A bank engineer is being interviewed by police investigating unauthorised withdrawals from cash machines. It is alleged that money was withdrawn from customers' accounts through information gained during the servicing of machines operated by Clydesdale Bank.
... Since the first cash machines appeared ... all banks have denied that "phantom withdrawals" are possible, despite the fact that public complaints alleging such withdrawals make up the biggest single item in the banking Ombudsman's caseload. In only one of many hundreds of complaints has the Ombudsman found in the customer's favour ... Last year, 482 complaints about cash machine withdrawals were lodged ... None were resolved in the customer's favour. The only time the Ombudsman did find for the customer, in 1988, it was on a legal technicality. The first Ombudsman ... said his office accepted the banking industry line that withdrawals could only be made by a person using a card and a number.
The banks have never accepted that cash-machine withdrawals could be made as a result of computer error or internal security breaches. Clydesdale said: "Unauthorised transactions were revealed as a result of our investigative procedures and the police advised. Only a very small number of accounts has been affected and the bank has written to them."

Stella Page, Centre for Software Reliability, The City University,
Northampton Square, London EC1V OHB, United Kingdom.

Quick n' easy access to Fidelity account info

Carol Springs <carols@drilex.dri.mgh.com>
Tue, 5 Feb 91 13:37:38 EDT

Robert Powell reports in the Boston Herald, February 5, 1991, that from January 8 to February 4 callers were able to access info on any Fidelity Investments shareholder's account for which blocking had not been specifically requested -- solely via the investor's SSN. The access is still available for most Fidelity accounts. From the article:

> The program, introduced Jan. 8 and called Fidelity Telepeople Collection, lets folks dial an 800 telephone number. After being prompted by a computer, callers key in their or any customer's Social Security number to learn holdings of stocks, options, and mutual funds.
>
> People who knew the Social Security numbers of Fidelity's bigwigs like Chairman Edward C. Johnson or Peter Lynch could easily learn whether Johnson put his

> money where his firm is, or just how many shares of the
> Magellan Fund Lynch owned.
>
> The Social Security numbers of most executive officers
> of investment advisory firms is on file with the
> Securities and Exchange Commission. Fidelity, in
> reaction to a story in yesterday's Wall Street Journal,
> blocked the public's access to Fidelity executives'
> accounts.

The article goes on to add that individual shareholders can request that telephone access to their accounts be blocked, according to Tracey Gordon at Fidelity. Marketing manager Judith McMichael adds that

> ...Fidelity changed the access code to the telephone
> service from a customer's account number to his or her
> Social Security number because of overwhelming customer
> support during the company's research. And Fidelity
> has only received three complaints to date, she said.

Eric Kobren, the president of Mutual Fund Investors Association, is requesting that his subscribers call Fidelity to ask them to require a PIN tag for the service.

Carol Springs carols@drilex.dri.mgh.com

Re: Enterprising Vending Machines (Allan Meers, Risks 11.01)

<mjackson.wbst147@xerox.com>
Tue, 5 Feb 1991 12:55:01 PST

In Risks 11.02, PGN writes:

> Here is another example of ordinary mortals having to gain sophistication
> in the vagaries of automated systems in order to maintain their cool.

Who are you calling a mere mortal?-) Despite having read Allan Meers' posting (Risks 11.01) *I* got burned this morning, and not by an older machine, either.

Around 11 AM I entered the lobby of the (brand-new) post office in Webster NY. Approximately 35 people were waiting in line, so I turned to the (brand-new) stamp vending machine. Several of the selections were flashing "SOLD OUT" but (great!) rolls of "F" stamps were still available for $29.00.

There was a puzzled couple ahead of me; they'd fed a dollar into the machine thinking they could buy *one* F stamp, and were now trying to figure out what to do (no purchase, no change; cheapest non-sold-out option was 10 23 cent stamps for $2.30). I offered to feed the machine a $10 and a $20 bill, buy the $29.00 roll, and split the $2 change. (There was a big sign posted next to the machine warning about no change without purchase, noting that change up to $5 would be given in coins.) No problem. . .until I got my stamps. Displayed credit dropped from $31.00 to $2.00. Pressed the CHANGE button. . .display

changed to flashing "OUT OF COINS - NO CHANGE AVAILABLE"!

Gotcha! There was *no* warning of this state until change was requested. Getting a refund required pushing to the front of the line, flagging down a clerk, then filling out a long postal refund form IN DUPLICATE. . .and, for all I know, waiting for a government check to arrive from Washington. We decided to feed the machine some more change and take our change in 23 cent stamps, so the other guy put in 35 cents (no nickel). . .and THEN we noticed that the machine had quietly eaten the $2 credit. At this point we gave up; final score me -$1, them -$1.35, USPS +$2.35.

It seems the programmers did anticipate this problem (credit stuck in the machine with no means of recovery). From the Postal System's point of view, this is a problem because IT DISABLES THE MACHINE. So, apparently, the solution is to clear unused credit after 60 seconds of inactivity, thereby "resetting the trap."

Mark <MJackson.Wbst147@Xerox.COM>

"This U.S. stamp, along with 25 [cents] of additional U.S. postage,
is equivalent to the 'F' stamp rate"

- Official Algorithm of the US Postal Service

Risks of no escape paths

Geoff Kuenning <geoff@prodnet.la.locus.com>
Fri, 1 Feb 91 16:01:42 -0800

I just got a phone message from one of my credit card companies, asking for a return call. However, when I called their 800 number, I got a computerized answering system. The second prompt was "please enter your 16-digit account number now." Happens I have two cards from that company; which had they called about? Hang up, try again -- this time I figure I'll pretend to have a dial telephone and talk to a human. Wrong. The hardware is actually smart enough to detect dialing on a dial phone, and my fancy PBX won't let me masquerade by flashing the hook. Okay, I'll wait for a timeout. Wrong. After the timeout it insists on a number. Okay, how about an obviously incorrect number? After 16 5's, it pauses and then complains that the account number is incorrect, returning me to the original prompt.

In frustration, I begin composing this message. While typing, I notice that there is a "flash" button on my PBX phone. Maybe that'll let me pretend to be a dial phone. Nope. But my PBX is screwy enough that this attempt put the line on hold without my noticing. 60 seconds later I notice the flashing light and pick up, just in time to get a voice saying "Hello?" I say "hello," and the person at the other end asks for my account number. But now I've got a human, and when I tell him my problem, he is smart enough to handle me without insisting on the account number. Surprise! I have more than two cards with that company, because they just bought out another of my cards! So now which card do they care about?

The only good thing (other than a chuckle) about this whole thing is that the phone answering system is still on trial, so if I can remember to call on Monday, I can talk to a responsible person and perhaps (especially by mentioning RISKS) affect their go/no go decision.

If I didn't love them so much, I'd hate computers...

Geoff Kuenning geoff@la.locus.com geoff@ITcorp.com

A risky gas pump

<RMG3@PSUVM.PSU.EDU>
Saturday, 2 Feb 1991 14:14:32 EST

I guess risks readers haven't stopped for gas on the Ohio turnpike lately.

A new service is being offered on the Ohio turnpike by Sohio (a division of BP Oil). I'll quote their flyer:

" New from SOHIO and the Ohio Turnpike ... [Their ellipses]
Now, RAPID PUMP lets you charge your gas quickly and conveniently right at the pump. If you need a receipt, RAPID PUMP will give you one. No need to walk to the cashier. Just charge your gas at RAPID PUMP, and drive away. "

On another flyer the operation is explained:

" 1 Just insert and remove your card ...
RAPID PUMP automatically checks for authorization. If you would like to cancel at any time before pumping fuel, use the CANCEL button. You may also press the HELP button at any time for assistance

2 Need a Receipt?
Watch the display screen and select either the YES or the NO button

3 Then select your fuel ...
[text irrelevant to risks]

4 Stop when you want ...
When you reach the dollars and gallons you want, slide the lever down, replace the nozzle and your gas cap. If you did not request a receipt, your transaction is complete and you may drive away.

5 If you requested a receipt ...
RAPID PUMP automatically prints your receipt for you. Take it and drive away! "

Having read risks for a while (or rather, having read the archive recently),
I did not try this 'convenience' out. Just in the time I was pumping gas
I came up with several _risky_ questions about the process:
What verification is there that the card that is authorized is really mine?
What happens if the receipt disagrees with the amount pumped?
How about if my number is not cleared from the pump's memory and I get
billed for the entire day's gas from that pump?
How do I get that receipt if the machine is out of paper? Will is _always_
know that it can't print _before_ I pump the gas?

There are quite a few that risks readers could come up with. This situation
does start to merge in to the 'Americard' type of risks as well. Perhaps
this gas pump is a harbinger of the 'Americard'. I hope not.

Bob Grumbine

Electronic traffic signs endanger motorists...

nexus.yorku.ca? <rsnider@xrtll>
Tue, 5 Feb 91 16:19:31 EST

Recently in Toronto the Ministry of Transportation has introduced a system to
regulate/inform motorists while driving on a large section of highway that
crosses almost centrally through the city (also known as the 401). This
highway has approx 16-20 lanes of traffic which has the daily weekday tendancy
to come to a full and complete stop during morning and afternoon rush hours.

The system they have given us consists of electronic signs much like typical
Stadium Scoreboards on which they will display messages about traffic
conditions ahead, behind, or wherever that they collect from a set of TV
cameras and wire loop sensors that are installed along the highway.

On a smaller highway that runs through the city they installed a single smaller
version of the big signs now installed, and for the last year or so they have
been conducting tests with it (I assume).

Now usually this smaller sign has contained a simple message saying what the
next exit is, but a few times it has displayed messages about weekend highway
closures. This has resulted in the best chaos I have seen next to the typical
rush hour stuff.

There is a serious danger here of people crashing into others who are either
reading the message, or trying to avoid someone else who is. This is ONE sign.
I figure there are about 30 of the big ones now going to be used. I can only
imagine what we are going to see happen when they start displaying things like
"LEFT LANE BLOCKED, USE COLLECTORS AHEAD" and 700 motorists first slow down to
read this and then try and pull over to the two rightmost lanes in order to
exit off that section of the highway. I suppose they could use some of the
other signs available to tell of the impending disaster in the collector lanes.

ISOTECH Computer Industries, Toronto, Canada ....Rich (rsnider@xrtll) Ls not 1s
....uunet!itcyyz!xrtll!rsnider

Re: Predicting system reliability

Richard.P.Taylor@nve.crl.aecl.ca <taylorrp@nve.crl.aecl.ca>
Wed, 6 Feb 91 11:37:45 EST

I would like to expand on the issues raised by Martyn Thomas concerning reliability requirements, expectations and predictions.

Mr. Thomas points out that it is unsound to predict the reliability of one system from knowledge of the reliability of another, "similar" system. In my opinion, this is the major problem with using reliability growth models to predict the reliability of a system. Whenever changes are made to fix errors discovered by testing, the result is a new system. The new system will certainly be similar to the old system, but because the changes may have introduced or uncovered new faults, we cannot predict that the reliability of the new system will have any fixed relationship to the reliability of the old system.

It seems clear to many investigators of software reliability that the only way to gain confidence that a given level of reliability has been achieved is to have a period of failure-free operation longer than the required period. Therefore we must change some of our reliability requirements and definitions in order to make reliability testing practical. I believe that someone has already pointed out in a previous RISKS debate concerning the A320, that there are great differences in the control requirements and safety requirements between takeoff, level flight, and landing. It is much more feasible to test a system over a large number of simulated takeoffs and landings than it is to test for an extremely long operating time. Similarly, as Mr. Thomas points out, for on demand systems.

My own concern is with nuclear reactor shutdown systems. While these systems are "on-demand" (they are only required to "act" to shut down the reactor when some kind of process anomaly is detected), they are in continuous operation in a monitoring role. In order to make reliability testing feasible, it is necessary to design the system in such a way that each individual test need not include the months of steady-state operation which generally precedes a shutdown demand. We must also be careful to define our reliability requirements to separate the shutdown function and from the less critical monitoring and reporting functions.

The Canadian Atomic Energy Control Board is currently working on ways to define, test and review software safety system reliability. I would also welcome further discussion of these issues in RISKS.

Richard P. Taylor, Atomic Energy Control Board (AECB), P.O. Box 1046, Station B, 270 Albert St., Ottawa, Canada, K1P 5S9 (613) 995-3782

the new California licenses

Chris Hibbert <hibbert@xanadu.UUCP>
Tue, 5 Feb 91 11:02:13 PST

California did indeed introduce a new format of Driver's License. I've been following the issue for a while as part of CPSR's Palo Alto working group on Computers and Civil Liberties. Here are some of the details:

There will be a magnetic stripe on the back with three tracks encoded on it. The middle track will be encoded in the same format as your credit cards, and will therefore be readable with ordinary commercial readers. This track will only contain 40 bytes of information, and will only contain the name, driver's license number, and expiration date. The other two tracks will be in a format that is incompatible with current commercial readers, and will contain the rest of the information that is printed on the front: birth date, eye color, hair color, height, weight etc.

The picture on the front will be an ordinary photo (I'm not sure whether it'll be color or B&W), with a hologram of the state and DMV seals to make counterfeiting harder. There will apparently be a different version for people under the legal drinking age: the picture will be on the right instead of the left. (This tidbit from the Mercury News. I hadn't noticed it before.)

The DMV says that the first and third stripes will be encoded at a higher density and "corrosivity." Apparently corrosivity is resistance to changing the pattern of magnetization. (I welcome corrections or expansions on this point.) I'm not sure whether "Orsteds" are measures of density or corrosivity, but they say that the standard specifies 30 Orsteds, and that's what the middle stripe will use, while the other two stripes will be encoded at 3600 Orsteds. The difference in density is for incompatibility with current commercial readers, though I'm not convinced that new readers won't be made available soon to the California business community. The difference in magnetization is intended to make the cards harder to erase or rewrite. I don't know whether it'll do any good, or whether there will be penalties for carrying an erased card around. I fully intend to see if I can erase my card first thing when I get one.

The primary purpose of the new cards, according to the DMV, is to make it easier for police officers to fill out tickets correctly and quickly. There will be readers for the new cards in all state police cars, though I don't know what the schedule for installation is. They'll probably wait until a significant proportion of the citizenry have the new licenses. A secondary purpose is to save money and time when issuing renewal licenses. The DMV (actually, the contractor who won the bid) will keep digitized records of the picture and other data on the card, and when renewal time comes around, they'll be able to just pop a brand-new card in the mail. This will get rid of the certificates of renewal and address update cards that Californians now carry around with their licenses until they get a new card.

Another purpose (as evidenced by the fact that the stripes are partially compatible with commercial readers) is making the information more easily available to merchants. Since the information is accessible, merchants will find a way to use it. The most likely way is to keep track of customers and their habits. More efficient access to the bad-check data bases is a laudable goal, but it's cost will be that more information will be stored about

everybody who's willing to let their licenses be scanned in the name of efficency. I've tried to explain this point to members of the state legislature, but without success. The fact that I didn't find out about the plan until after the DMV had gotten some approval and had requested and started processing bids didn't help my case.

In a response to a letter of mine, Assemblywoman Delaine Eastin (Chairwoman of the committee on Governmental Efficiency and Consumer Protection; now there's a pair of incompatible goals for one committee to work on!) wrote: "I share your concern that the stripes, if used improperly or if expanded beyond the current plan, could constitute an invasion of privacy. A society where people carry around magnetically coded `ID' cards for use by police and store-keepers would not be one most of us want to live in. Nevertheless, the DMV plan, limited in its scope, seems like a relatively benign way to save time and money for everyone."

The new licenses constitute exactly the "magnetically coded `ID' cards for use by police and store-keepers" that she said we wouldn't find acceptable. Merchants will start asking customers for their licenses, and most customers will comply unthinkingly. Those who see the deeper privacy issues and don't want their identity recorded along with their buying habits in yet another computer system will have to contend with clerks who just do what the boss tells them to. They won't be allowed to ignore those behind them in line who can only tell that someone is interrupting the routine and making them wait longer. I'm afraid that we've lost a little more of our privacy, and it's going to be very hard to get it back.

Chris

Phone Voting -- Really a Problem?

Michael Barnett <mbarnett@cs.utexas.edu>
Tue, 5 Feb 91 13:03:29 CST

I must agree with Mike Beede in RISKS-11.01 that phone voting is basically a solution in search of a problem. I understand that we are all in technological fields, but surely there must be times that we can see the answer to a problem does not lie in technology. What is the problem that phone voting is trying to solve? It appears to me that the main problem with elections in this country is the low turnout. I find it hard to believe that it is the difficulty of physically going to vote that accounts for that. Why not try the solution many countries have -- either make election day a holiday, or conduct it on Sundays when most of the population is not working? (Of course, I'm tempted to say that having a real choice on the ballot may be the best cure.)

Michael Barnett

Re: Voting by Phone (Ravitz, RISKS-11.01)

<daemon@celit.UUCP>
6 Feb 91 08:40:10 GMT

eravitz@isis.cs.du.edu (Evan Ravitz) writes:

> (in regards to voting via phone)
>Paranoia is justified, but apply it to how we vote now, as well. Don't you
>think that a government that can photograph your license plate from outer space
>can install a tiny video camera that watches how you vote in a booth?

Sure the government could install a video camera in every voting booth. Could they keep it secret? I don't think so. However, accessing a database and cracking a cryptographic code is something that could be done by a small group of people working in secret. That's the risk inherent. I doubt that the government proper will ever conduct a project like spying on the voters but a small group, ala Ollie North and Friends, could very easily do it given a relatively small amount of resources.

David L. Smith, FPS Computing, San Diego ucsd!celit!dave or dave@fps.com

---

Re: Electronic cash completely replacing cash

Barry Wright <ronin@ronin.sbi.com>
Tue, 5 Feb 91 13:16:53 EST

> Think about it. Drug deals, muggings, corruption, businesses
> concealing their income - they all require cash and secrecy. A monetary
> system bases solely on electronic currency would leave a trail that would
> cripple such enterprises.

Fat chance. When was the last time you "hacked" a supposedly secure system, just to prove you could? I remember when BART (Bay Area Rapid Transit) was just starting, with its supposedly secure, tamper-proof, "electronic tokens" (cards that registered the amount in the commuter's "account" and allowed a ticket purchase if there was enough remaining -- somewhat similar to the electronic cash scenario).

A Berkeley councilman, suspecting the BART cards weren't quite as secure as claimed, offered a cash reward (only $100, as I remember) to 50 UC Berkeley students, if they could find a way to steal from the proposed system. He got fifty different successful hacks.
^^^^^^^^^
Electronic cash would only breed electronic thieves. A better breed, perhaps, but thieves nonetheless... :^)

B. Wright ronin@ronin.sbi.com

[By the way, there is still an enormous collection of pending messages on mastercards and on americards. If I have the patience to prune it a little, you'll get to see it. Otherwise, it may just drop through the crack. It required much more moderation on the part of your moderator than usual... PGN]

Report problems with the web pages to the maintainer

Search RISKS using swish-e

THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

ACM Committee on Computers and Public Policy, Peter G. Neumann, moderator

Volume 11: Issue 4

Thursday 7 February 1991

Contents

---

subway door accidents (Pete Mellor, RISKS-11.03)

Mark Brader <msb@sq.com>
Thu, 7 Feb 1991 14:07:00 -0500

Here in Toronto, the subway staff can open one door on each side of each car, but they need a key to do so. There is an interlock so that any door open more than 1-2 cm prevents acceleration from being applied, and opening the door with

the staff key apparently does not override the interlock. (At least, the usual indicator lights do come on.) All of this is exactly the way I would expect sensibly run systems everywhere to do it. So let's hear about the counterexamples...

It *is* possible for a train to run with a door open, in case the door fails; to do so requires the operation of an override control concealed under the passenger seats. In that case the door-open warnings do not light. On using the override, the crew place large "Danger - Do Not Use" banners across the doorway. This too seems entirely sensible.

The open-door interlock is not sufficient to prevent accidents of the type described above. The closing doors can trap things like a coat sleeve or a trailing purse, and people don't always react properly. There was a fatal accident here last year which may have been of this type (the exact cause was not proved); it resulted in a long inquest and a lot of unfavorable publicity for the transit system; and as a result of this, we now have what seem to me to be annoyingly paternalistic advertisements, basically telling us that it's always better to wait for the next train than to try to catch one that's just leaving.

The operating practice here is to start the train the instant all doors are closed -- often the driver sets the control to accelerate as they start closing, and lets the interlock start the train when they finish. On a past visit to New York, on the other hand, I noticed that there they wait a couple of seconds after closing the doors and before starting the train. And as I recall London does the same. I then read about an accident in New York where someone had tried to force the doors open during those seconds, and gotten caught and killed. My conclusions were that New York does not have a door/power interlock (though I suppose it might be that the fool merely managed to not trigger it) and that it is actually safer to start away at once because it reduces the temptation to those who would try this sort of thing.

Mark Brader SoftQuad Inc., Toronto utzoo!sq!msb, msb@sq.com

"Virus" destroys part of Mass. state budget plan

Adam M Gaffin <adamg@world.std.com>
Thu, 7 Feb 1991 17:36:00 GMT

Reason 4,012 to back up documents: A case study

Middlesex News, Framingham, Mass, 2/7/91

By Adam Gaffin
NEWS STAFF WRITER
BOSTON - State officials say a computer virus destroyed 50 pages of Gov. Weld's budget proposal earlier this week, but a computer consultant with experience in fighting the bugssays uit sounds more like a case of inadequate maintenance than anything sinister.
Michael Sentance of Maynard, a legislative aide to Weld, had typed in 50 pages of the governor's proposed budget on a Macintosh computer

when he tried saving the document to the machine's hard drive around 3 a.m. on Monday - only a few hours before it was due to be submitted to the Legislature.

But instead of being saved, the document disappeared, according to Liz Lattimore, a Weld spokeswoman. Sentance was eventually able to retrieve an earlier draft, filed under a different name, minus the 50 pages, she said. Because of the snafu, Weld was forced to delay submitting the plan by a day.

When Sentance ran a program to check for the presence of viruses on the machine, it responded with a message indicating a ``type 003 TOPS network'' virus, Lattimore said. TOPS is the name of the network used by the Executive Office of Administration and Finance to connect its Macintoshes.

Sentance had borrowed one of that office's computers because he was more familiar with Macs than with the older Wang system in the governor's suite, Lattimore said.

Viruses are small programs that can take control of a computer's operating system and destroy other programs and data, and can be spread through people unwittingly sharing ``infected'' programs or disks.

Lattimore said officials managed to transfer data from the ailing computer to another machine, adding that they are now checking all of Administration and Finance's Macintosh computers for possible infection.

But Eileen Hoffman of Needham, a Macintosh consultant, says what happened to Sentance sounds more like a hard-drive ``crash'' than a virus - something she said is potentially far more destructive.

A document that disappears when the user tries to save it onto the hard drive usually means there is something physically wrong with the computer's hard drive, not that it is under viral attack, Hoffman said.

Hoffman, who keeps three or four infected disks in a safe so that she can test new anti-viral software, said the software that runs TOPS networks is written in such a way that it can show up as a ``virus'' in programs that check for viruses. She said a ``Type 003'' virus is one of these phantom ``sneak'' viruses.

Hoffman said Macintosh users are often more lax about maintaining their computer's hard drives than users of IBM compatible machines, because Macintoshes are aimed at people who do not want to have anything to do with the hardware of their machines. The Macintoshes were installed during the Dukakis administration.

But even Mac hard drives require regular maintenance, she said. She said she often gets calls from clients who blame disappearing data or strange things on their screens on viruses, but that almost always the problem is caused by a mechanical hard-drive problem.

She added that the particular version of anti-viral software Sentance used is two years out of date. Since new viruses are created all the time, this means the software might not be able to detect one even if the machine were infected, she said.

Reinterpretation of term "Computer Security"

Frank Dixon, fdixon@hq.dla.mil <fhi0011@hq.dla.mil>
Wed Feb 6 09:01:17 1991

One of the moguls in our business has publically taken the position that computer security, as a concern, should be interpreted to include _all_ data not just data perceived to be "at risk." He suggests--at his most extreme pole--that the term "sensitive data" should be stricken from the lexicon of security practitioners.

Given that those charged with protected the information judged to be sensitive are more or less plowing an uphill furrow, I am concerned that this movement toward a broadening of the coverage of the concern will have either of two deleterious effects: (1) It may weaken the already feeble attempts to protect the truly sensitive, or (2) be used pragmatically as a justification for "protecting" all communications.

I don't like the implications.

Frank Dixon, Alexandria, VA

SSN and Schwab Telebroker RISKS

Curtis Jackson <!jackson@adobe.UUCP>
7 Feb 91 20:46:02 GMT

This morning my girlfriend decided to sell some stock in her Charles Schwab (a popular U.S. discount stock brokerage firm) account. Schwab has a 24-hour automated telephone quote and order service called Telebroker, and since I know that stock orders placed through Telebroker qualify for a 10% discount on commission fees, I suggested she place her order over the telephone with the automated system.

All of her records (including her account number) were at work, but she glibly called up the local Schwab office and was able to obtain her account number simply by giving her social security number and her address. She then called up Telebroker for the first time ever, entered her account number, and it asked for *the last four digits of her social security number as her default password*. "This is easy," she said. And indeed it is! It then had her pick a new password, and dropped her into the standard interface. I do not know if it would have balked if the "new" password she entered was the old one -- the last four digits of her SSN.

Telebroker is a relatively new and somewhat unknown feature offered by Charles Schwab. As easy as it is to obtain social security numbers of people in the U.S., it would be very easy to find someone who has a Schwab account but has never used Telebroker. If you couldn't get their Schwab account number on your own, you could simply call up Schwab and get their account number, then call Telebroker and have a good deal of fun at their expense. Certainly you couldn't get your hands on the proceeds from a stock sale, but if you wanted to wreak havoc on their life you could sell valuable stocks they are holding, or find a climbing stock and margin them into it to the hilt. Schwab allows you to purchase 1.5 times your equity on margin. Schwab further has a [somewhat lax] policy of not leaving completed transaction confirmation messages on answering machines for privacy reasons, so if you do it while Mr. X is out of town he won't find out what you've done until the margin call.

Even without the human-induced risk of giving out account numbers on the telephone, the risk of using the last four digits of the SSN as the default password is a great one.

Curtis Jackson @ Adobe Systems in Mountain View, CA (415-962-4905)
Internet: jackson@adobe.com uucp: ...!{apple|decwrl|sun}!adobe!jackson

---

Re: Inquiry into cash machine fraud (RISKS-11.03)

John Sloan <jsloan@niwot.scd.ucar.EDU>
Thu, 7 Feb 91 12:21:35 MST

> A bank engineer is being interviewed by police investigating unauthorized
>withdrawals from cash machines. It is alleged that money was withdrawn from
>customers' accounts through information gained during the servicing of machines
>operated by Clydesdale Bank.

This reminds me of a personal anecdote that illustrates how computers can play passive partners in "low-tech" cash machine ripoffs. In 1975 I worked for a national bank which was among the first to introduce cash machines to the region. Normally the cash machines were online and continuously monitored by a DEC PDP-11 front-ending an IBM 370/135 (I should mention that the cash machines were not manufactured by either of these two firms). The machines had offline capabilities in the case that the host systems went down and thus an account could not be verified.

One weekend we were converting from a 370/135 to a 370/145 during which time there was a short period in which the machines were left in offline mode. While the machines were acting independently a large theft occurred from the cash cassettes of several machines. There was no record of transactions on the internal audit paper tape on any of the victimized machines. It was clearly an inside job, since the thief knew precisely when the host system would be unavailable.

Since I was on duty that weekend during the conversion I was among the personnel interviewed by the FBI. Nearly a year later, after changing jobs, I read where the FBI had arrested one of two of the cash machine vendor's service people, who had confessed. His crime involved some special knowledge -- if a cash machine were to be opened while online that would be time stamped on the host system console -- but required no more technology than the key to open the vault in the rear of the machine.

John Sloan, NCAR/SCD, POB 3000, Boulder CO 80307 +1 303 497 1243
jsloan@ncar.ucar.edu ...!ncar!jsloan jsloan%ncar@ncario.BITNET

Re: the new California licenses

<mjackson.wbst147@xerox.com>
Wed, 6 Feb 1991 14:33:00 PST

That's "coercivity" rather than "corrosivity"; it's a measure of how "stiff" the system is in the sense of resisting changes in magnetization. (Differences in coercivity between DD and HD diskettes in both 3 1/2 and 5 1/4" formats have a lot to do with the inadvisability / impossibility of using DD disks at the higher densities.)

The oersted is the unit of magnetic field strength in the CGS system.

Mark <MJackson.Wbst147@Xerox.COM>

[Also noted by Fred Gilham <gilham@csl.sri.com>, Steve Bellovin <smb@ulysses.att.com>, Ron Fox <fox@rudolf.nscl.msu.edu>, and Mark Gabriele (gabriele@hub.toronto.edu). Even PGN noticed it, but did not get around to fixing it. I try, but I do not always fix everything that needs it. If I did, I would probably be Chorusively Orst(ed) on my own Peterd. PGN]

Re: the new California licenses

Mark Gabriele <gabriele@riverdale.toronto.edu>
Thu, 7 Feb 91 11:13:43 EST

>... The other two tracks will be in a format that is incompatible
>with current commercial readers, and will contain the rest of the
>information that is printed on the front: birth date, eye color, hair
>color, height, weight etc.

The author then goes on to point out the issues of loss of privacy from this new system, and how all shopkeepers will soon inevitably upgrade their card readers to capture this important and private information.

I don't see what the privacy problem is here, provided that the only data which is encoded magnetically on the back of the cards is currently available in human-readable format on the front of the card. If you'll give your driver's license to a clerk, you should be prepared to have the clerk copy down all of the information on that license (I've had clerks meticulously copy my height, weight, and eye color off of the driver's license while I and the customers behind me waited).

=Mark Gabriele (gabriele@hub.toronto.edu)

No more quick n' easy account info from Fidelity

Carol Springs <carols@drilex.dri.mgh.com>
Wed, 6 Feb 91 13:18:42 EDT

In today's Boston Herald (Febrary 6), Robert Powell has a followup to his article on Fidelity that appeared yesterday. Basically, Fidelity has "slammed the door shut" on Fidelity Telephone Connection. Tracey Gordon at Fidelity says, "We changed it in response to concerns by some of our shareholders who called because of reports in the press."

People who called the toll-free number on February 5 got a real human person asking for SSN and Fidelity account number.

According to Gordon, a system is being set up wherein callers will enter their account number along with their SSN. And a few weeks later, a PIN system will be put into place.

Carol Springs carols@drilex.dri.mgh.com

Discontinued: Quick n' easy access to Fidelity account info

"B.J. 07-Feb-1991 1021" <herbison@ultra.enet.dec.com>
Thu, 7 Feb 91 07:46:47 PST

In a message in RISKS-11.03, Carol Springs described a system that allowed access to Fidelity Investments account information using an 800 number and a social security number. The message said it was possible to call Fidelity and request blocking for your accounts. When I called Fidelity and asked about the service, the response was:

`No, we discontinued that service.'

I thanked the representative, told her I was pleased that the service was dead, and hung up. A small victory for privacy.

On a related note, when you call 1-800-DISCOVER you are given the opportunity to check your Discover credit balance automatically. When this service first started, only the card number was needed. Because of complaints, the system now require your zip code as well. Another reason to refuse to write your address on your credit card receipt.

Quick n' easy access to Fidelity account info

"Carl M. Kadie" <kadie@cs.uiuc.edu>
Thu, 7 Feb 91 11:27:52 -0600

I just called Fidelity. The representative say that the Telepeople system has been taken down until they can add PIN protection.

[O PIN, O SESAME? PGN]

Re: Electronic cash completely replacing cash

"Lee S. Ridgway" <RIDGWAY@mitvma.mit.edu>
Thu, 07 Feb 91 10:46:55 EST

No one seems to have proposed the most obvious, simple solution to the risks of americards and mastercards: cash! I find that for my normal purchasing habits,

I can pay cash. I can go to my bank machine two or three times a week [I know some people who visit theirs daily!], get cash to cover known purchases for several days, and not have to bother waiting for clerks to fill out charge slips, get verifications, and other time-consuming procedures. Thus, I pay for groceries, gas, meals, recordings, books, concerts, etc., etc.

I do have credit cards, but I use them only for large or very specific purchases. That means few databases have records of my purchasing habits. I also don't carry balances, or incur interest, and don't have to write several big checks to credit card companies each month.

For those who are now going to say that cards are safer: I live in a city where street robbery is not unknown, but I don't carry very much cash at one time - and I don't carry my cards unless I know I will use them. Yes, I've been robbed a few times (in about 20 years), but never lost much cash, and lost much more in time and aggravation over stolen credit and ID cards than the cash.

For those who say cards are more convenient: Carry more than two, and they are as bulky as bills. They require more time to complete a transaction (compare the time it takes to pay a restaurant bill in cash vs. credit card!). Compare the amount of time needed for a verification, especially if the phone or computer connection is down or slow, or the manager is not around. Compare the amount of time needed once a month to sit down and check store receipts against bills, write checks, etc.

One other possible blessing of cash and not cards: I find that I am on the mailing list of only one or two mail-order houses, from whom I receive catalogs maybe once a month, while my housemate, who uses credit cards for just about everything, receives at least six or more catalogs per day! Cause and effect?

[NO MORE RESPONSES on this topic for a while. We are badly backlogged. PGN]

Re: Re: Predicting System Reliability...

Brad L. Knowles <blknowle@frodo.jdssc.dca.mil>
Wed, 6 Feb 91 19:16:41 EST

In reference to Richard P. Taylor's point in 11.03, namely that to show "sufficient" reliability for a system requires that the entire system in question run in a production environment for longer than the required time, I must agree. In fact, with the things about quality that we are learning from the Japanese (who learned it from Dr. Deming), I would claim that the entire system in question run in a production environment for a six-sigma period of time.

For those of you who might not have been accustomed to the term six-sigma, I will attempt my best explanation (poor 'tho it will be):

In statistics, we can call sigma the Standard Deviation of the Probability of Failure of the system in question. The term x-bar (a lower-case x with a bar above it) is the Mean Probability of Failure of the system in question. X-bar plus six-sigma is the value we want to prove is

lower than some given criterion, to a certain level of confidence.

We then compose what is called a "Null Hypothesis" that is the exact opposite of what we are trying to prove (namely, that our system will last at least x amount of time). We then try to prove our Null Hypothesis wrong, to a probability of 95% or better. If we prove to 95%, then we have proven to a two-sigma level of confidence that are system will last at least as long as desired. If we prove to a 99%, then we have proven to a three-sigma level of confidence. If we prove to a 99.997%, then we say we have a six-sigma level of confidence. The test used to show the level of confidence is usually "Student's T Test", for historical reasons (I know, there are oodles of other tests, this just happens to be the first taught in most University Senior-level Stat courses, and probably the best known).

One thing to keep in mind, as we get to higher levels of confidence, we must test our system for exponentially long periods of time, assuming that all else is equal (which, we all know, never happens). That is, unless you test hundreds or even thousands of units, all in parallel. This is how a disk drive manufacturer can say something like "50,000 Hours Mean Time Between Failures" -- you didn't think they actually had a single drive that they tested for 50K+ hours, did you? I would go so far as to say that no well known drive manufacturer today has a single drive with 50K hours on it -- they'll get junked and replaced long before that happens. Still, the drives fail.

The exact numbers of units that you would have to test to prove a certain level of confidence can also be calculated by well known statistical methods, so that you might have to test only 53 units to get the level of confidence desired.

Basically, this is what the Japanese are hitting us over the head with. Most Japanese companies have been using six-sigma Statistical Quality Control for years now, and many of the front runners are now going to nine-sigma (and even twelve-sigma)!

Now, the problem we've got is when we try to test a system like a Nuclear Power plant. We certainly can't afford to build a single plant to try to prove our system will last at least x number of years without failure, much less build *MULTIPLE* identical plants to do so. Thus, all we can really do is unit-test as many parts as we can, and forgo the system testing. I can point out to one very well known system where this has led to many heartaches, if not outright system failure before it was ever put on line -- the Hubble Space Telescope. Everything was completely unit-tested, but system testing was deemed too expensive and time-consuming. Still, in some cases, system testing just is not possible.

Oh well, this is an interesting discussion of an ages-old problem -- it is non-trivial to prove even trivial systems correct (or when they will fail), not to mention how hard it is to prove non-trivial systems correct!

Brad Knowles, Sun System Administrator, DCA/JDSSC/JNSL, The Pentagon BE685, Washington, D.C. 20301-7010 (703) 693-5849 | Autovon: 223-5849

Disclaimer: Nothing I have done or said in the above should be construed as an official position or policy of the Defense Communications Agency or the United States federal government. The author is the sole person responsible for the content of this message.

Re: Predicting system reliability (RISKS 11.02)

Jeff Johnson <jjohnson@hpljaj.hpl.hp.com>
Thu, 07 Feb 91 10:32:49 PST

This discussion is muddied by a failure to distinguish between reliability and functional sufficiency. I believe that there is a tradeoff in systems engineering between reliability and sufficiency. If a problem exists that is to be solved by a system, the system designers are often faced with the choice of designing a system that solves the problem or one that is reliable and maintainable. The reliable design usually solves some sub-problem.

Many system designers don't realize that they are faced with this tradeoff: they design a system to solve the full problem and only after it is built do they discover that it is so complex and bug-ridden that it cannot be relied upon or maintained. Or, perhaps seeing the tradeoff, perhaps not, they aim low and deliver a reliable, maintainable system that doesn't do what was desired. Either way, the resulting system doesn't solve the customer's problem.

Often, as a system designer, I've had programmers respond to design specifications by saying: "Providing functional capability X would require me to write a non-modular program. I won't make it non-modular, so you can't have feature X." This argument is of course false -- any thing that can be done "non-modularly" can also be done "modularly" -- but it illustrates the programmer's tendency to sacrifice functional sufficiency for reliability and maintainability. Customers, salespeople, and those who write functional specifications typically exhibit the opposite tendency: requesting or promising functionality that would exceed developers' ability to produce a reliable system.

An example from SDI: Initially, the plan was to design a system in which there was a great deal of inter-component communication in order to coordinate the defense. Critics correctly shot down this plan as hopelessly unreliable. The SDIO responded by advocating a decentralized design involving significantly less inter-component communication. Under further criticism, control was further decentralized until we ended up with "Brilliant Pebbles", in which at least the "business-end" components are supposedly autonomous, and which managed to win over a few SDI critics.

My reaction to Brilliant Pebbles and some of the other decentralized plans that preceded it was that even if they are more reliable than centralized designs (and this is debatable), they wouldn't solve the problem from a functional point of view: massive inter-component communication may well be *necessary* for the system to accomplish its task. Unfortunately, massive inter-component communication also implies a level of unreliablility that, for SDI, is unacceptable.

If handed a functional specification for SDI, I could write a ten-line C/unix program that would be (I assert) highly reliable. But it wouldn't meet the functional specification. Some SDI proposals (and some proposals for other ambitious projects) are simply schemes to develop slightly-larger "ten-line" programs that won't do the job.

Computer Science has partially addressed the issue of reliability and maintainability by developing: 1) formalisms for proving correctness of programs, 2) programming languages and tools providing more support for program correctness (e.g., modularity, strong-typing), 3) improved methodologies for software engineering. These don't insure reliable systems, but they help. Has Computer Science developed anything analogous for analyzing functional sufficiency of programs (beyond a few proofs that certain extremely ambitious functional specifications can't be met)? Might such an analysis be useful here?

JJ, HP Labs

Electronic telephone directory

<MFMISTAL@HMARL5.BITNET>
Wed, 6 Feb 91 22:19 N

In the Netherlands, printed telephone directories provide telephone numbers by using the name as an index. Currently, there is also an electronic version of those directories available by means of a VIDITEL service. Here it is also possible to ask for a telephone number by providing the street name, the house number and the city. This involves an inherent risk. When one observes that there are apparently no people in a house, one can ask for the phone number, dial that number and when no one replies.... it may be safe for burglars to go in. It seems also to be an invasion of one's privacy, since one need not to know a name in order to place haressing/obscene phone calls.

The only thing one needs is a PC and a modem. The costs: 35 cents (20 $cents) a minute.

Jan Talmon, Dept of Medical Informatics, University of Limburg, Maastricht, The Netherlands

---

Search RISKS using swish-e

THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

ACM Committee on Computers and Public Policy, Peter G. Neumann, moderator

Volume 11: Issue 5

Thursday 7 February 1991

Contents

Re: Enterprising Vending Machines (Allan Meers, Risks 11.01)

"Jay Schmidgall" <shmdgljd@rchvmw3.iinus1.ibm.com>
Thu, 7 Feb 91 12:37:24 CST

In RISKS DIGEST 11.03, mjackson.wbst147@xerox.com writes:

> It seems the programmers did anticipate this problem (credit stuck
> in the machine with no means of recovery).

Well, I got to witness a incident quite similar here at my onsite stamp machine. A person had put in $5 and tried to buy a book of 20 stamps. Unfortunately, the price was now $5.80 because of the price per stamp increase and the machine flashed an message "Use exact change" (as an aside, not quite the response I would have expected, which would have been more like "Insert additional funds" or some such.) Also unfortunately, the person did not have an additional 80 with them -- apparently he had just grabbed a fiver to buy the stamps. Fortunately, someone he knew was around so he asked them if they had 80. Unfortunately they did not.

When he got back to the machine, I suggested he just buy a book of the old 25 stamps, since it was posted that a purchase was required to get back change. In fact, it was also posted that a minimum $7 purchase was required to get back change -- this was a bit unclear as someone had just written it in red ink over the operating instructions, which were on a roughly 3x5 sticker in small type on the upper right corner of the machine.

When he tried to get the stamps, the "Use exact change" message flashed again. He was pretty confused but, having read my RISKS this morning, I had an idea what was happening. I put in my money to get my stamps (exact change, BTW) and sure enough, his $5 credit was gone. I got my stamps, explained to him what I thought had happened and suggested he contact Vending Services to get his money back. I also fired a note off to the vending person myself, suggesting that this "feechur" be disabled if at all possible. No response as yet.

Jay Schmidgall RSCS:shmdgljd@rchvmw3 shmdgljd@rchvmw3.iinus1.ibm.com

---

Re: Enterprising Vending Machines (RISKS-11.03)

<mattd@apple.com>
Thu, 7 Feb 91 13:51:54 -0800

The hotbeds of American technology are not immune to this horrid machine. I went to the main post office right here in Cupertino, CA yesterday, having already read the article in Risks 11.01 (happy anniversary!) warning of this nasty machine. I *intended* to purchase stamps at the window, but made the mistake of arriving at 4:58 PM -- the service area was already locked, and only those already inside were being let out. So I went to the vending machine.

Just for fun, I pressed the button for an item without any money in the machine, and the "SOLD OUT" light *did* illuminate. I didn't take this at face value, but I decided to risk that there was a roll of 29 cent stamps or two still in the machine.

Problem: All I had were $20 bills. OK, I thought, even though this machine had a label on it clearly saying that it will not deliver more than $3.00 in change, I can put in 3 $20-bills and buy two rolls of 100 $0.29 stamps. Right?

Wrong. It cheerfully accepted my first $20, but rejected the second one with "CAUTION: USE SMALLER BILLS." Apparently the machine knew that it's most expensive item was $29 and wouldn't let me insert $40! I had no smaller bills, and the helpful postal employee in the lobby had a vocabulary limited to the words "we're closed". Finally, after about 5 minutes of trying to figure a way out of this mess without having to purchase the entire machine, a postal supervisor came out and gave me two $10 bills for a $20, enabling me to finish and be on my way.

(The supervisor, by the way, had only come out to investigate a report that the machine was not accepting coins, but gave change when he noticed that the problem I'd encountered had stopped approximately 8 other potentional income sources from taking their chances with this demonic mechanical contraption.)

--Matt Deatherage, Apple Computer, Inc.

[THIS SERIES OF HORROR TALES IS BROUGHT TO YOU IN THE PUBLIC INTEREST, ALTHOUGH PUBLIC DISINTEREST IS LIKELY TO ENSUE RAPIDLY. BEWARE. PGN]

Re: A risky gas pump

Donald Lehman <dlehman@cyclonic.sw.stratus.com>
Wed, 6 Feb 91 21:20:14 EST

I remember a setup, similar to what Mr. Grumbine describes, in Sacramento around 1985 or so. I wish we had something like that around here. I think this is a case where the benifits outweigh the risks. Unlike voting, buying gas is something I do relatively often and I want the process to be optimized. I consider the increased risks (relative to the risks already associated with credit card puchases) to be minimal.

I respond:

> What verification is there that the card that is authorized is really mine?
None. But my other credit card purchases are not usually validated either. I think the fair credit acts protect you somewhat.

> What happens if the receipt disagrees with the amount pumped?
Complain. Same as if the human attendant tried to overcharge you. I would assume that these stations have a human attendant or at least a telephone available.

> How about if my number is not cleared from the pump's memory and I get
> billed for the entire day's gas from that pump?
This is a risk of any system. The same thing could happen with the computer at an attended pump. I'm not sure, but I believe that with modern systems the slips you sign are only looked at if there is a discrepancy.

> How do I get that receipt if the machine is out of paper? Will is _always_
> know that it can't print _before_ I pump the gas?
I assume these things would be similar to an ATM in telling you if it can't print receipts, but even if it doesn't, I don't consider it a big deal. It may mess up your records, but, except for expense accounts, I can't think of a reason I need to prove that I bought gas. What I would want is proof that I didn't buy something, but that is practically impossible.

>Perhaps this gas pump is a harbinger of the 'Americard'. I hope not.
There is a major distinction between the issue of 'Americard' and credit cards, and that is credit. As I understand it, the 'Americard' is like a debit card in that you don't need to 'agree' to the charges by paying a bill. Unless you blindly pay what the credit card company asks, you are protected to some extent. I've never had to go to arbitration or litigation over credit card items,

so I don't know how powerful the companies may be, but you need to weigh the risks with the benefits.

Don Lehman | Donald_Lehman@es.stratus.com
Stratus Computer Inc. | Standard Disclaimers Apply
Marlboro, Mass | I speak for myself...

Re: A risky gas pump (RISKS-11.03)

James Helman <jim@baroque.stanford.edu>
Wed, 6 Feb 91 21:39:45 -0800

A similar system is in use in at least one Chevron station on the SF Peninsula (Belmont). The only difference is that a receipt is always printed, so no interaction beyond running the card through and pumping the gas is necessary.

Initially, the station attendants were running all around checking things and said they were having problems. But now it has settled down and is one of the quicker places to get gasoline.

Personally, I find the convenience to be worth the additional risk. The danger does not appear to be substantially higher than other electronically entered transactions, probably less since gasoline purchases are usually modest in amount and frequency. Perhaps, it's just another good reason to only carry cards from reputable and responsive banks, just in case of problems.

Jim Helman, Department of Applied Physics, Stanford University, Durand 012
(jim@baroque.stanford.edu) (415) 723-9127

---

re: risky gas pumps

Jonathan Clark <jhc@ulysses.att.com>
Thu, 7 Feb 91 09:54:29 EST

Completely unmanned petrol (gas) stations have been around in Europe for at least the last ten years. When I lived in Brussels I used to patronize them all the time, because:

1) They were open 24 hours a day, 7 days a week; and
2) They were significantly cheaper.

They worked on a bank debit card system (like a money machine card), and so were just as (in)secure as those. I believe that there was a maximum amount of fuel that one was allowed to charge in one pass, this would occasionally lead to drivers of cars with large tanks (V12 Jaguars spring to mind) having to go through the ritual twice, in order to fill up completely. As far as I recall one *always* got a receipt.

One of the risks they *reduced* was the possibility of driving away with the hose still attached to the car. When it's one's own money one is very careful about closing off the transaction properly...

Perhaps some of our readers currently living in Europe would contribute
some horror stories?

Jonathan Clark jhc@ulysses.att.com, attmail!jonathan

Re: A risky gas pump (RISKS-11.03)

Paul S. Sawyer <paul@unhtel.unh.edu>
7 Feb 91 10:20:08 EST (Thu)

> [Gas pumps which read credit cards directly] ...
>
>I did not try this 'convenience' out. Just in the time I was pumping gas
>I came up with several _risky_ questions about the process:
> What verification is there that the card that is authorized is really mine?
> What happens if the receipt disagrees with the amount pumped?
> How about if my number is not cleared from the pump's memory and I get
> billed for the entire day's gas from that pump?
> How do I get that receipt if the machine is out of paper? Will is _always_
> know that it can't print _before_ I pump the gas?
>
> There are quite a few that risks readers could come up with. This situation
>does start to merge in to the 'Americard' type of risks as well. Perhaps
>this gas pump is a harbinger of the 'Americard'. I hope not.
> Bob Grumbine

Mobil has been doing this for some time, and it usually seems to work [I only
use my Mobil card on the turnpikes, since they like to charge their regular
customers extra....] They also take debit cards, including some bank teller
cards. The problem is, during the authorization phase, they go for something
like $30-$35. Then, you get $5-$10 worth of gas, and the difference is not
credited until later. [possibly end of day batching?] A local news item told
of a woman who could not get cash from an ATM to buy groceries because she
had just used the card to get gas....

Paul S. Sawyer {uunet,attmail}!unhtel!paul paul@unhtel.unh.edu
UNH CIS - - Telecommunications and Network Services VOX: +1 603 862 3262
Durham, New Hampshire 03824-3523 FAX: +1 603 862 2030

Re: auto gas pumps

Christopher Lott <cml@cs.UMD.EDU>
Thu, 7 Feb 91 08:49:33 -0500

I am responding to the article about gas pumps that take payment;
the author encountered these on the Ohio Tpke.

Maryland has these pumps, and I for one love them. Around here, you
have to pay in advance for non-auto pumps, which in my case means walking
in and handing the attendant my credit card and then leaving it with

him/her for the 5-10 minutes it takes me to fill the truck tank (big tank!).

I feel that the purely human risks of leaving my cc with some joker far outweigh the tech. risks of trusting the implementor of the pump to have done the right thing.

Of course I could always use cash! ;-)

chris...

Re: A Risky Gas Pump (devil's advocate)

NSIL LCM <0004222127@mcimail.com>
Thu, 7 Feb 91 15:34 GMT

[comments & disclaimers]
I am not a lawyer, and I do not work at a bank. I am somewhat disheartened that people simply do not take time to read credit agreements and learn how to protect themselves. Credit, while not really a friend, can be something of a robber or "banker in your pocket." I have never appeared in a published article (and probably won't anytime soon).

[begin response]

It may come as a surprise to our international friends, but it should be noted that on perhaps the rarest of occasions, proper identification may be required to complete any transaction with a credit card. The laws governing commerce and use of demand consumer credit do not place a compulsion before the seller of any good or service to identify the holder of a credit card as the authorized user. I personally know of no place, other than a hotel or motel, where the seller is compelled to discover or validate your identity. Also, in some hotels, credit issuers agree in advance to a floor limit, which allows the innkeeper to authorize charges without calling for an authorization (used to be significant, but has probably decreased with automation). I know these limits exist because one of my cards was stolen and AFTER it was known to be stolen, it was presented and accepted for a room (the billing was, I believe, over $200).

Secondly, on the point of agreement between the receipt and the delivery of any good or service purchased with credit cards, it should be pointed out that every consumer (in the United States) has the right to dispute any transaction appearing on his account within 60 days of that charge's first appearance (most grantors will afford some leeway in this). In fact, the grantor of credit risks the possibility that the authorized user will dispute valid charges and claim that the card was lost or stolen. Goodwill and plain honesty go a long way in the relationship.

Thirdly, given the protection basically held above, receipt failures are not serious faults. The receipt for expendables like gasoline and food can be written by hand and used for proof of a transaction (naturally, there is some penalty for fraudulent receipts which should curb their creation), even to the point that it is valid for an audit of one's income tax returns. This question is answered also by the power of a dispute.

Finally, the possibility that a single person might be charged with all the transactions at one gas pump over a given period is that also where a single person's bank account should become the target of an ATM gone silly. There is always that risk, but then there is always a limitation on spending as well. Banks impose a limit upon an account's daily withdrawls, and upon borrowing with a credit card.

The real risks of pumping gas are more substantive than economics. Gasoline is a volatile high explosive. The average car with a full tank has at least the equivalent explosive potential of 140 sticks of dynamite. A sufficient discharge of static electricity anywhere on the fragile connection from pump to filler neck could loose an explosion of no mean displacement (not to mention during rush hour on a crowded city street).

[end response]

I wish I had something more substantial and helpful to say than "this is a good list, and I wish I had been reading it before." I don't have, and for that, I am committing the rest of my life to the pursuit of the Oxford English Dictionary, if she will have me.

Yours truly,

Guy Sherr, MCI, 12369 Sunrise Valley Drive, Reston, VA 22091 Dept 1076/637

Re: A risky gas pump

Michael C. Tanner <mtanner@gmuvax2.gmu.edu>
Thu, 7 Feb 91 14:54:33 -0500

Bob Grumbine <RMG3@PSUVM.PSU.EDU>, writes about gas pumps that take your credit card, and don't require signatures, etc.

I've been using pumps like this for some time now. I know there are certain risks involved, but they are not that great. I accept them in exchange for the increased convenience.

Some of the issues he raises are easy to address. If it doesn't print a receipt, you go inside and ask for one and after suitable checking they give it to you (that's how it works around here, anyway). If the amount is different, you go inside and talk about it. Etc. Having bought gas this way 50-75 times in the last 6 months, I have failed to receive a receipt once and had the pump fail to turn on once. Otherwise, no problems. Not a large sample, I know, and one bad experience is all it takes, but it looks pretty good.

Another possible risk is that my number gets stuck in there somehow, and everybody's gas is charged to my card at that pump/station/throughout northern Virginia/USA for some period of time. But I don't think I'd have much trouble convincing anyone that I didn't really buy a million dollars worth of gas on Friday. I'm not convinced this is a real danger.

The only real problem, I think, is that 2 or 3 extra charges per month could appear on my bill. Since I check carefully before I pay any bill, it's not likely this would get by me. If it happens once, I can probably get the charges removed. If it happens regularly it may be more of a problem. So the real risk is that I get overcharged $20-30 per month, get into a hassle with the company, and ultimately have a blot on my credit record. My total exposure is to maybe a $100 or so loss (I can cancel the card and pay it off after 4 or 5 months and have no credit problems). The way I look at it, I run this risk in simply having the card, whether I accept the credit pump, or have a person enter the same data into the same computer.

So the way I look at it, I get greater convenience at little or no increased risk. A nice application of technology, I say.

Michael C. Tanner, Assistant Professor, CS Dept, AI Center, George Mason Univ., Fairfax, VA 22030 tanner@gmuvax2.gmu.edu (703) 764-6487

Re: A risky gas pump (RISKS DIGEST 11.03)

Michael Van Norman (2) <EGC4MV2@MVS.OAC.UCLA.EDU>
Wed, 06 Feb 91 15:11 PST

Here in Los Angeles, ARCO has had the same type of service for years. I have used it for years without any problem. Now in LA you can even get a hamburger at Carl's Jr. with your ATM card!

> What verification is there that the card that is authorized is really mine?

You enter your PIN after sliding your card through the reader. I believe that what the authorization entails is a check to see if you sufficient funds to make a purchase.

> What happens if the receipt disagrees with the amount pumped?

Complain to the cashier.

> How about if my number is not cleared from the pump's memory and I get
> billed for the entire day's gas from that pump?

I have never had this happen (or have heard of it happening) but i have also wondered about it.

> How do I get that receipt if the machine is out of paper? Will is _always_
> know that it can't print _before_ I pump the gas?

Probably not :)

Michael Van Norman, Library Administrative Computing, 11334 University Research Library, 405 Hilgard Avenue, Los Angeles, CA 90024-1575 (213)825-1206

Re: A risky gas pump (from RISKS DIGEST 11.03)

Barry Margolin <barmar@think.UUCP>
Thu, 7 Feb 91 00:40:29 GMT

Your tone suggests that this is a new risk. The risks of these gas pumps are precisely the same as many other uses of credit cards. What makes the gas pumps any different from credit card telephones? The phones don't even *try* to print a receipt. And what about giving your credit card number over the phone to a mail order house? In general, the risk with all these is that most credit cards don't have a PIN, even though they're being used more and more for such automatic transfers. But even a PIN won't solve the "reuse" problems that you identified; to solve these, you generally need a challenge/response authentication system, probably involving a smartcard rather than a simple credit card.

> What verification is there that the card that is authorized is really mine?

None. However, if you dispute a charge, the bank will generally remove it. Your liability is only $50 for charges made on a stolen credit card, and I think you have no liability for purchases made after reporting the card lost or stolen.

> What happens if the receipt disagrees with the amount pumped?

I'd go to the attendant and get a refund of the excess charge.

What happens if the pump claims to have delivered more gas than it actually has? How would you even know, so long as the claim was within a gallon of your expectation? This relates to a misc.invest discussion I recently participated in, regarding balancing one's checkbook; someone asked whether I really trust greedy banks to properly maintain my balance. I didn't reply, but I was thinking: if they wanted to screw me, they'd be much less likely to get caught if they skimmed from my interest payments rather than play games with my deposits and withdrawals, as I'm unlikely to verify their interest calculations. So I *must* trust them.

> How about if my number is not cleared from the pump's memory and I get
> billed for the entire day's gas from that pump?

Complain and have the charge removed. I don't think any bank would give you a hard time if you were to dispute a charge for thousands of dollars of gas from an ordinary gas station.

> How do I get that receipt if the machine is out of paper? Will is _always_
> know that it can't print _before_ I pump the gas?

Who knows? I think my bank's ATM warns about not being able to print receipts.

Barry Margolin, Thinking Machines Corp. {uunet,harvard}!think!barmar

Search RISKS using swish-e

Report problems with the web pages to the maintainer

Search RISKS using swish-e

THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

ACM Committee on Computers and Public Policy, Peter G. Neumann, moderator

Volume 11: Issue 6

Friday 8 February 1991

Contents

Mailing lists are, indeed, cheaply and easily available (RISKS-10.81)

"CONTR HERRICK, DAN" <herrickd%iccgcc.DNET@abvax.UUCP>
29 Jan 91 09:56:00 EDT

Samuel Bates asked where you can get names of companies that produce the Lotus-style information.

Look in your local Yellow Pages. Possibly Madison is too much a one industry town, so you may need to look in the Milwaukee Yellow Pages. Use the Business to Business Yellow Pages if they make that distinction out there.

The Cleveland Business to Business Yellow Pages have about 3 1/2 columns of entries under Advertising, Direct Mail. Both national and local firms. More

than a third of those Yellow Pages advertisers will sell or rent the same kind of information as Esmark and Lotus were offering.

dan herrick herrickd@iccgcc.decnet.ab.com

U.S. Mailing List Business

"Mary Culnan" <mculnan@guvax.georgetown.edu>
30 Jan 91 20:30:00 EST

This is in response to the posting in RISKS 10.81 asking for the names of companies that sell mailing lists based on personal information. The list business in the US is more than a $1 Billion dollar/year industry. To put it briefly, if it moves, it will be for sale in a list. If you use a credit card, call an 800 #, subscribe to any publications, order from a catalog, contribute to a political party or a charity, or return a warranty card, you are on somebody's list.

Of most concern to me is that the two large credit bureaus, TRW and Equifax, are both also in the list business. Data from your credit record are summarized and moved into the marketing databases. This was the source of the data for the Lotus MarketPlace (plus census data). I don't believe that most people knew this.

There is nothing illegal about this, and because the marketing databases do not include an individual's *credit report*, these lists are not covered by the Fair Credit Reporting Act.

If you are interested in seeing examples of actual lists, I suggest you consult the following 3 trade publications:

1) Standard Rate & Data Services (SRDS) volume on Direct Mail List Rates & Data. (A multi-volume reference source available in many libraries--other volumes include names and addresses for radio stations, etc.)

2) DM News, a weekly newspaper

3) Direct Marketing, a monthly magazine.

I will send a short handout with more information on specific list vendors as well as general information on the list industry to anyone who sends me a business-size stamped self-addressed envelope:

Mary Culnan, School of Business Administration,
Georgetown University, Washington, D.C. 20057

---

cashless society

Jolly C. Pancakes <jcp@islay.dco.dec.com>
Wed, 30 Jan 91 14:49:25 -0500

Margaret Atwood's book _The Handmaid's Tale_ makes an excellent case against a cashless, plastic dependent society (doubtless there are other books which deal with the subject but Atwood's is the one most familiar to a wide segment of the population).

At some time prior to the action in the book, everyone in the US has converted to an "Americard"-type system. The legitimate government is then overthrown and taken over by a fundamentalist Christian sect which then revokes all bank accounts owned by women. At a single stroke, half of the adult population can be immediately disenfranchised (and you can imagine for yourself all the implications, etc.)

-J.C.Patilla

Cashless Society

"Jay Schmidgall Rochester MN" <shmdgljd@rchvmw3.iinus1.ibm.com>
Wed, 30 Jan 91 14:04:16 CST

Pointer to Roger Zelazny's "My Name is Legion", a collection of three tales concerning a detective using/making cash in a cashless society.

In this case, it is a world-wide electronic credit card, not just USA.
Also, the detective was a compsci guy who was in on the organization of the database from the beginnning and was eventually presented with the decision to enter/not enter into that database.

Very interesting reading, especially as relating to the realization of the detective that this might not be a good thing and how he got around it.

Jay Schmidgall RSCS:shmdgljd@rchvmw3

Re: Electronic cash completely

Frank Wales <frank@grep.co.uk>
Wed, 30 Jan 91 19:46:25 GMT

If someone can invent a cash-replacement scheme that lets me give money to a homeless busker, give the equivalent of a post-dated cheque as a deposit to be destroyed if I don't mess up, and allows my friends from abroad to buy things while they visit me, then maybe I'll think about it.

Frank Wales, Grep Limited, [frank@grep.co.uk<->uunet!grep!frank]
Kirkfields Business Centre, Kirk Lane, LEEDS, UK, LS19 7LX. (+44) 532 500303

Re: Electronic Cash Cards (RISKS-10.82)

Alex Bangs <abg@mars.EPM.ORNL.GOV>

Wed, 30 Jan 91 15:32:54 EST

The primary motivation behind these cards seems to be the potential to eliminate crime. Yet I don't think we can say that all crime involves cash and individuals. Banks have been caught laundering money for drug dealers before; who says they couldn't find a way to do it with cash cards?

Alex Bangs, ORNL

Abolish Cash, and destabilize the nation.

Pink <prince@pebbles.tcs.uh.edu>
Wed, 30 Jan 91 17:24:19 CST

The social changes that would be brought about by the proposals in the article "Abolish Cash" by Harvey F. Wachsman are almost prophetic in their similarities to Margret Atwood's _The Handmaid's Tale_. The idea of a cashless society has been around much longer than this book, but the dangers Atwood illustrates are still just as real.

In her book, a group of fundamentalists perform a bloodless coup on this country, primarily by taking over the central computers that control every citizens monetary accounts. The first thing they do is freeze all of the accounts whose holders are women or whom the consider to be the opposition. Literally overnight they are able to seize control of the country. If this were to happen in reality, a hostile group could concievably freeze our entire economy with a reletively small amount of military or political effort.

If this country "goes cashless" I'm sure the control of the system would be distributed with multiple backup computers to come online if an important one failed or started acting "outside of norms." The danger still remains that hostile countries or organizations could place agents in whatever agency would control this program.

In short, we would be putting our economy in the hands of computers and by extention the (probably) small number of people who control them, rather than in the hands of the entire government, where change is slow and relatively visible.

Cashless society

Jerry Leichter <leichter@lrw.com>
Wed, 30 Jan 91 23:31:40 EDT

Those interested in this issue might want to look up the December, 1979 CACM (V22 #12). This was a special issue on Electronic Funds Transfer.

Some interesting data (from Lipis's article on Costs of ... Payment Systems): For 1976, it is estimated that the cost of a cash transaction is about $.012, which is actually a DECREASE from the cost in the early '70's. The cost for a credit card transaction is $.52; for a check, $.53. In 1976, cash represented

88% of all transactions, but only 3% of all money changing hands. (96% of the money moved as checks, though only 11% of the transactions were by check).

-- Jerry

Re: Electronic cash

Geoff Kuenning <geoff@devnet.la.locus.com>
Wed, 30 Jan 91 18:23:34 -0800

Somebody said they hardly use cash any more, even using a Visa at 7-11. That's them. Me, I do a *lot* of cash business; it takes much less time to hand the clerk a fiver and get change than any alternative -- and the bank doesn't charge me 10 cents a transaction.

One other small point, pointed out by John D. McDonald in one of his Travis McGee books:

Suppose you are a black marketeer with a large nest egg in the mattress. You learn that on June 1, your money is going to be useless unless it's orange, and there's a complicated system that will keep you from swapping your green for orange. Are you really going to sit quietly while your money becomes worthless? Or are you going to go visit your local car, boat, and art dealers? When you find out that the BMW's are out of stock because your neighbor beat you to it, are you perhaps going to be willing to pay double for a Honda (getting 50% out of your money being obviously better than 0%)? The obvious result is a spurt of demand-pull inflation; how much depends on the true size of the underground economy, but the more you believe the proponents of this idiotic idea, the worse it will be.

Geoff Kuenning geoff@la.locus.com geoff@ITcorp.com

Cashless society

Rob Aitken <aitken@hpdtlra.ctgsc.hp.com>
Thu, 31 Jan 91 12:09:00 pst

Yet another problem with the Americard proposal is that a number of small countries, particularly in the Caribbean, use the U.S. dollar as their official currency. Instantly eliminating a country's money supply could be damaging to international relations.

Rob Aitken

---

cashless banking

Daniel B Dobkin <dbd@marbury.gba.nyu.edu>
Mon, 4 Feb 91 14:06:05 EST

The recent discussion of the New York Times op-ed proposal for a cashless

society reminded me of Robert Ellis Smith's book on "Privacy," published in 1979. I don't have the book in front of me, but I'll paraphrase the passage that really struck me:

> A number of years ago a group of academics was asked to consider how a government could best keep track of what all its citizens were up to. After a day's discussion, their proposal was remarkably similar to what the banking industry wants to establish in this country: real-time electronic funds transfers.

Remember, that was 1979. We've come a long way since then!

Unfortunately, Smith doesn't attribute the source of this story; does anyone out there have any clues? Enquiring minds want to know.....

\dbd

Electronic Cash

<yamauchi@cs.rochester.edu>
Thu, 31 Jan 91 18:25:25 -0500

I'm in favor of replacing the various pieces of paper and bits of metal we currently use for money with a more convenient electronic system, but I think this should and will be done via the free market rather than as mandated by the central government.

Already, I tend to use my VISA debit card for most purchases over $10-$20, and it would be convenient to be able to avoid carrying any cash and use a debit card for all purchases (including vending machines, etc). Transfers of money from one individual to another might be a little more complicated, but one could have a terminal which accepted two cards (with appropriate passwords) and transferred funds between the two accounts. Granted, this is less convenient than just handing someone a few bills, however, on the whole, this system should be more efficient than having to run down to the ATM whenever you get low on cash (hard to imagine how people dealt with bankers' hours before ATM's...).

Another vast improvement would be an LCD display on the card which indicates your current balance. Thus no more need to either balance a checkbook or worry about bouncing checks. (For the paranoid, this feature could be disabled so that others can't see the balance.)

Bill payment would also be easier. Just dial the access number for your electric/phone/credit company, insert your card, and key in your password and the amount you are paying.

I'm not extremely enthusiastic about giving the government too much information. It is true that they could abuse this. On the other hand, the real solution is to enact pro-freedom measures legislatively to limit the government's power. If either (1) the government ceases to become democratic,

or (2) the majority wants to allow government oppression, then there's not a lot you can do -- short of armed rebellion -- the tanks can always roll through the streets.

Electronic cash would have both positive and negative effects on crime. On the positive side, violent crimes would drop substantially -- no longer would you have to worry about being knifed for your wallet in a dark alley. On the negative side, the potential for computer crime would be increased. At least in theory, this could create the potential for truly huge sums of money to be stolen, not by stealing large chunks, but by stealing minute amounts from large numbers. For example, stealing 1 cent from every transaction made in the U.S. would probably result in a take in the $million/day range.

Still, given a choice, I would rather have some hacker breaking into my checking account than some mugger slitting my throat...

Brian Yamauchi University of Rochester
yamauchi@cs.rochester.edu Department of Computer Science

Re: Electronic cash completely replacing cash

Joe Keane <jgk@osc.UUCP>
Fri, 1 Feb 91 18:40:24 PST

The article on electronic cash worries me. It's so full of vague reasoning and outright contradictions that it seems like a joke, but evidently it's quite serious. It's hard to figure out where to start criticizing it.

The stated goal is to reduce the Federal deficit. But the plan includes the government giving away, to every home and business, machines which evidently read not just magnetic cards but also hand and retina prints. Even ignoring the feasibility and risks of this technology, it's clear that such machines would not be cheap. The article assures us that `regardless' the goverment would come out ahead, but i don't see any basis for this belief.

I'll just point out the obvious irony in saying banks would be `delighted' to open new accounts, and then also saying they will be required to do so.

Most of the article talks about the benefits of the proposed `Americard'. I agree with much of this, and in fact we are seeing more use of credit cards and bank cards to replace cash. But i would prefer the American way, having many banks to choose from rather than one government-mandated plan. This leads us to the obvious question: if the Americard is such a hot idea, then why do we need to outlaw its competition?

In any case, talking about these benefits is deceptive, since it implies that the plan is giving us something we don't have, when really it's taking away something we do have. This is a common ploy; everyone knows the sarcasm in the phrase `for your own good'. And it's not just taking our greenbacks, but quite a bit of personal freedom too. This alone should make this plan unacceptable to any reasonable person.

Finally, the argument that eliminating cash will also eliminate black market activity is ridiculous and goes against all common sense. Apparently we are to believe that black marketeers will simply throw up their hands and give up. A child could tell you that they will simply switch to using yen, Deutsch marks, drugs, diamonds, or whatever else is convenient. Most likely they will also accept the `obsolete' American dollars at some reduced rate. The only way to actually accomplish the stated objective is to eliminate everything of value smaller than a cow. I leave it to the reader to evaluate this option.

Re: RISKS DIGEST 10.81

Richard A. O'Keefe <ok@goanna.cs.rmit.OZ.AU>
4 Feb 91 09:24:32 GMT

In Risks v.10 no 81, 28-Jan-91, David 'Witt' wrote about
> Subject: Electronic cash completely replacing cash

The article he transcribed said, amongst other things:

> If all the people who do business in cash were forced to report their
> incomes accurately - if the under-ground economy were forced to the surface -
> the Government could collect an additional $100 billion a year for the nationl
> treasury - without raising taxes.

This is simply false. It's every bit as blatant a lie as the one that says television advertising saves consumers money. The bottom line is SOMEONE HAS TO PAY. The underground economy having been forced to the surface, where do they get the money to pay the taxes? From people who use their services. The nett result is that all around the economy, prices go up. If the underground economy didn't have a major part to play in the national economy, there wouldn't be any point in making them pay taxes, no? People who find themselves spending lots more money, and who notice that the government's income has gone up, may possibly be stupid enough to believe that "taxes haven't been raised", but surely not all of them.

This is the part of the proposal that really bothers me, that there are people who are prepared to believe that huge chunks of money can be extracted from part of the economy without any other effect.

> How do we create a system to keep cash businesses honest ?? Eliminate
> cash. That may sound revolutionary, but the exchange of cash for electronic
> currency is already used in nearly all legitimate international business
> transactions.

EFT is also used in a heck of a lot of dishonest and fraudulent transactions. New Zealand recently created a "Serious Fraud Office" because it finally dawned on the police and the government that the depradations of thieves and muggers were *dwarfed* by white-collar crime. I sometimes wonder whether it might be a good idea to outlaw EFT in order to slow white-collar crime down. (Half (:-), but only half.) People who steal millions of dollars at a time do _not_ walk around with pockets full of $1 notes...

> Think about it. Drug deals, muggings, corruption, businesses
> concealing their income - they all require cash and secrecy. A monetary system
> bases solely on electronic currency would leave a trail that would cripple such
> enterprises.

Don't people read science fiction any more? Has Mack Reynolds gone completely out of favour? Many science fiction writers have published schemes for doing all these things in a cashless society. (Example: your hand- and eye-print scanners had better check for temperature and pulse...) (One elementary principle: having X buy something for you with his money is quite as good as having X give you the money and then you buy it, and in some respects better.)

> In place of paper money, we would receive new cards - let's call them
> Americards - each bio-mechanically impregnated with the owner's hand and retina
> prints to insure virtually foolproof identification.

If one person can make something, another can forge it. Is this really so obscure? If the handprint is only on the card, that doesn't ensure foolproof identification, it makes forgery all the easier. (To quote Edgar Wallace's Mr J.G.Reeder, "I fear I have a criminal mind". Evidently the author of the article David Witt quoted is very honest.)

> The Government would supply all homes and businesses, free of charge,
> with machines, to read the card, certify the holder's identity, and make
> instantaneous electronic debits and credits. Regardless of what such machines
> would cost, the Government, with $100 billion in new revenues and no more
> printing and mining costs, would come out ahead.

Eh? These machines are going to be *at least* as expensive as VCRs, and we're talking about distributing > 500 million of them (ALL homes and businesses, remember, and businesses will need as many of these gadgets as they have cash registers). Then think about maintenance.

> And think of the benefits to the average American.

I have a couple of US bank accounts, but no longer live or work there. Would the US government give *me* a magic reader and a network connection, or would they just steal the money?

> No one would have to write a check again.

What's so hard about writing cheques? The last supermarket I was in would print the cheque for you, all you had to fill in was the signature.

> Muggers and
> buglars would be out of business: no one would be carrying cash and stolen
> property would be difficult to sell because there would be records of all
> transactions.

Cars are registered now, aren't they. There's a change of registration form you have to fill out when ownership changes. Has this done anything to stop car theft? Where has this guy been living?

> The Federal Reserve would be better able to follow the economy, helping

> to stabilize the financial markets.

Here we have someone who does not believe in the Free Market, and has
a wonderful child-like faith that because there is an outfit whose task
is to manage the economy that it is able to do it. I have a bridge for him.

> And besides, I'd like to ask every parent whose child walks to school
> through a gauntlet of drug dealers, everyone whose home has been robbed,
> whether they think that their rights have been jeopardized by a system that
> could solve all these problems ??

If drug dealers can't get cash, I'm sure they'll be happy to take services.
I note that two of the most dangerous drugs around (as measured by the
amount of social damage demonstrably related to them) are legal...
Abolishing cash isn't going to do one little thing to the burglar who steals
your TV set because he *wants* a TV set, or because he just feels like
trashing your home. This is *unbelievably* naive.

The thing that is really evil about the suggestion is that it is a
technological fix to a social problem; the basic attitude is that
human "misbehaviour" is best cured by making people behave like good
little cogs. "Forget trying to build a humane society so that fewer
people *want* to buy drugs, let's build electronic cages so they're
found out." How do we educate people like this?

---

re: cashless society

<jeffj@synsys.UUCP>
Mon, 4 Feb 91 06:10:55 -0500

Gee, this discussion had elements from
misc.consumers (discussions about credit cards, supermarkets
tracking people's purchases with Point Of Sale (POS) terminals)
comp.dcom.telecom (discussions of Japan's telephone cards that
are purchased for cash and the calls are deducted,
quite different from a credit card because there's no billing
and it's anonymous).
misc.legal, and other groups.

I can safely say that this CANNOT happen for a loooong time
considering the current state of affairs:
1) ALL credit card companies charge fees.
Even if the cardholder pays no annual fee, there's a fee
the merchant pays PER TRANSACTION (usually 1-3 percent).
Dealing with cash is cheaper and immediate.
(gas stations cannot legally charge more for credit cards,
but can offer a discount for cash)
You'll have to abolish this before progressing.
2) Cash is very negotiable and its authenticity is easily checked.
I can buy a pretzel and the vender can check the dollar's
authenticity with no special instruments.
3) cash is anonymous. I usually buy my groceries with cash because

that way nobody can track my purchases and build up a database
about me.
4) most banks won't even provide checking for free.

The Washington DC subway system has a nice arrangement where vending machines dispense magnetically striped tickets with the amount on the stripe. The fare is automatically deducted from the ticket as you exit the station (putting the ticket through the turnstile's reader). Not enough fare? Vending machines allow you to pay cash and add the value to the card. Since cards are anonymous, they're transferrable and can't be used to track my whereabouts.

The Japanese phone cards are similar. I believe that ANY 'money card' should allow anonymous cash deposits to establish the accounts. This prevents companies like Lotus from collecting data about me and then selling it on CD-ROM (a product that was happily withdrawn).

This also allows non-residents/non-citizens to use the system because establishing an account depends ONLY on paying cash (which could have been converted from whatever currency to the native currency by any of several ways). [This has been discussed in the telecom group because non U.S. citizens have problems establishing calling card accounts with U.S. phone companies because that requires international banking.]

Jeffrey Jonas, jeffj@synsys.uucp, synsys!jeffj@uunet.uu.net

Epilogue on cashless society

"Peter G. Neumann" <neumann@csl.sri.com>
Thu, 7 Feb 1991 14:43:27 PST

Believe it or not, this issue is brought to you by popular demand. Several people were urgently clamoring for it, requesting even the raw text if I couldn't get around to moderating it. Quite a sociological exercise! For those of you who have read this issue all the way to the end, I hope you can eschew further discussion unless it really adds something substantive. I've been unusually permissive on this one, but after all one of the main purposes of RISKS is to foster intelligent discussion on important issues. PGN

[Knock, knock!
Who's there?
Cash.
Cash-who?
... {Your choice: (1) Sorry, no credit.
(2) Gesundheit!
(3) Nuts to you, too.
(4) ... }

Report problems with the web pages to the maintainer

Search RISKS using swish-e

THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

ACM Committee on Computers and Public Policy, Peter G. Neumann, moderator

Volume 11: Issue 7

Saturday 9 February 1991

Contents

"Study links leukemia to power lines, TV's"

"Martin Minow, ML3-5/U26 09-Feb-1991 0946" <minow@bolt.enet.dec.com>
Sat, 9 Feb 91 06:56:52 PST

>From the Boston Globe, Sat. Feb 9, 1991 (page 21, under the obituaries):

Study links leukemia to power lines, TVs (Lee Siegel, Asociated Press)

Los Angeles - Children may face twice the risk of getting leukemia if they live near power lines, frequntly use hair dryers or watch black-and-white television, says a study sponsored by electric utilities. The findings offer

"considerable support for a relationship between children's electrical applicance use and leukemia risk," said a summary of the study by the University of Southern California.

The University of Sourthern California study of 464 Los Angeles County children age 10 and younger is considered important because it was financed by the Electric Power Research Institute, which had been skeptical of earlier studies linking cancer to magnetic fields. The study found children who lived closest to neighborhood power lines were up to 2 1/2 times more likely to suffer leukemia. Frequent use of hair dryers and black-and-white televisions also increased leukemia risk.

That's the entire article -- does anyone have more information?
Martin Minow minow@bolt.enet.dec.com

A note on electromagnetic fields (and an epilog on cashless society)

"Martin Minow, ML3-5/U26 08-Feb-1991 1429" <minow@bolt.enet.dec.com>
Fri, 8 Feb 91 11:36:03 PST

The "risks of electromagnetic radiation" has a new, interesting, champion: Wayne Greene, publisher of 73 magazine (and the founder of Byte Magazine). He points out that amateur radio transmitters (especially when used by Morse code enthusiasts) generate electromagnetic fields that seem to match some of the more biologically active fields under study. While Greene isn't a scientist, he appears to be a reasonably competent electrical engineer. His editorial is in the current issue of 73 magazine.

If it hasn't been mentioned already, the "cashless society reading list" ought to include John Bruner's "The Shockwave Rider."

Martin Minow minow@bolt.enet.dec.com

City in Turmoil

Pete Mellor <pm@cs.city.ac.uk>
Fri, 8 Feb 91 18:37:00 PST

Infrastructure Collapses - 1000s of civilian casualties.

Is it Baghdad under Tomahawks and laser-guided bombs?

Is it Tel Aviv under SCUDs with nerve gas warheads?

NO! It's London under 6 inches of snow!

If Saddam Hussein could have delivered this lot, he'd be well pleased!

Once again, the Dunkirk spirit is to the fore, as the courageous inhabitants of this plucky little island, once one of the bastions of civilisation, leaders of the industrialised west [That's enough nauseating cliches! Get on with it! -

PM.], cope with a disaster the scale and magnitude of which is unparalleled in the history of mankind, or even in the history of Network South-East, since at least 1984.

The unsuspecting British were caught completely unawares by the sudden drop in temperature last night, to the previously unheard of level of -2 degrees C. The only warning that the authorities had was a brief announcement from the Met. Office a mere 5 days ago that things were going to get "...as cold as a Polar Bear's packed lunch".

Taken by surprise, all the major services collapsed one by one. Trains ground to a halt as they ploughed into snow drifts, which, in places, reached depths of almost 2 inches. Traffic skidded on the roads as gritting and salting services, with no practice in dealing with such a major catastrophe for at least 2 years, were stretched to the limit.

Telephone services were jammed by businessmen ringing up City University to say that they could not make it to urgent appointments with software reliability lecturers because it was impossible to get from Stevenage to London. In the city itself, those who had not fled at the first sign of snow, got tanked up at the Pheasant and Firkin and tried to get what sleep they could across two chairs in their offices, expecting any moment to be hit by one of the "Snowball" missiles raining down outside.

Normal life seems to have disappeared for ever. Today, students sat in classrooms with no lecturers. The few lecturers who didn't get home last night found their classrooms empty, because the students had assumed that lectures would be cancelled and gone out to build snowmen in Northampton Square.

The fearsome dictator of the regime, John el Major, appeared on television to rouse the population to new frenzies of resistance. In one speech, he went so far as to declare: "Yes, it is a bit chilly. I advise everyone to wrap up warmly."

Defence analyst Brig. Gen. (Ret'd) Sid Spotty said in interview:
"Of course, the apparent total devastation does not mean that the British haven't got a lot still in reserve. There must be a lot of logic bombs still hidden in bunkers. It's amazing how a technologically unsophisticated nation can still keep their software going in the face of overwhelming bombardment. I could illustrate what I mean, but the last power cut ****ed my fixed disk."

[This is Pete Mellor, RISKS network, London, Friday. (The last lecturer left in City University before the central heating goes off.)]

Re: the new California licenses (RISKS-11.04)

David Redell <redell@src.dec.com>
Fri, 8 Feb 91 10:48:06 PST

In RISKS 11.04. Mark Gabriel writes:

> I don't see what the privacy problem is here... If you'll give your

> driver's license to a clerk, you should be prepared to have the clerk
> copy down all of the information on that license.

As I understand his argument, it boils down to:

There's no reason to distinguish between:
what a clerk may see,
what a clerk may write down,
what a clerk may enter in a computer

Two observations:

1) There can be good reasons for distinguishing between what is seen and what is recorded. Often this principle is applied to mechanical recording (e.g. there are many situations in which you may listen to a phone conversation but may not record it) but even if the recording is manual, there can be good reasons for making the distinction. For example, recent California legislation (effective 1/1/91) prohibits the practice of writing down credit card numbers on checks as ID verification. A clerk can still ask for a credit card as ID, but is not allowed to copy down the information from the card.

2) There is an important difference in effort between manually copying down information and swiping it through a magstripe reader. (After all, if there weren't, the state wouldn't be going to all this trouble to issue magstripe licenses.) Currently, if you pay by check, you greatly reduce the likelihood of your purchasing habits ending up in the kind of database described by Mary Culnan in RISKS 11.06. Using a magstripe driver's license for check ID will make it significantly easier for the merchant to pull together online information about you and your purchases. (Of course, it would be possible for the clerk to type in the information manually, but the extra effort is enough to represent a qualitative change in practicality.)

Dave Redell, DEC Systems Research Center

Re: automatic flight and seasickness

Charles Bryant <ch@dce.ie>
Wed, 6 Feb 91 18:40:08 GMT

In risks 10.83 "Olivier M.J. Crepin-Leblond" <UMEEB37@vaxa.cc.imperial.ac.uk> quotes from "Le Figaro" concerning computer-controlled low level flight:

> Unfortunately, the actual pilots cannot stand this type of passive flight.
>Not because by vanity, but because they tend to get sick...

Surely this is not because the plane is not controlled by the pilot, since there are two-seater aircraft in use where both crewmembers are expected to be alert when they reach the target. It must be some characteristic of the motion

which is different when a human is in control.

Charles Bryant (ch@dce.ie)

Building very reliable systems

Jerry Leichter <leichter@lrw.com>
Fri, 8 Feb 91 10:28:45 EDT

There have been a couple of notes on RISKS of late on the problem of building very reliable systems - say, for the sake of discussion, those for which we have some good reason to believe that the probablity of failure is less that 1 in 10^8. The general problem is hardly new to computer systems, and really there are only two techniques in existence that can give you this kind of assurance:

1. Testing (whether by explicit test in a lab or by actual use in the field) of very large numbers of copies of the system at issues. This is the approach that most of the previous notes have mentioned. That such an approach is being used is often clear when you see people talking about things like "aggregate experience hours". The theory here is that running 100 units for 100 hours apiece gives you the same information as running one unit for 10,000 hours. Reliability of reactors is often argued in these terms; for items in mass production, where there may be hundreds of thousands if not millions of copies, "aggregate experience hours" mount very rapidly.

2. Functional decomposition of the system into a number of modules such that failure can occur only when ALL the modules fail. If there are three modules each of which has a probability of failure of 1 in 10^3, the system as a whole has a probability of failure of 1 in 10^9 - extremely reliable. Making modules that assured failure probabilities in the 1 in 10^3 range is relatively easy. SDIO always uses arguments of this form - "defense in depth" is an informal notion of the same thing. An article in the New York Times this Tuesday talked about missile defense systems, and showed five successive layers. Even if each layer misses 10% of the incoming targets, after five layers only one target in 10,000 makes it through - reliable enough to stop almost any conceivable attack. This technique is, of course, also used in reactors in the form of multiple redundant safety systems.

Now, the criticism of technique 2 is that the multiplication of failure probabilities is only valid when the failures of the different modules are known to be uncorrelated. There are many classic examples of lack of independence, as for example in the fire that destroyed all the cables for several "independent" reactor safety systems (at Brown's Ferry?). In the software community, technique 2, under the name of "n-version programming", has been sold as a way to build reliable software: Just run multiple independently-written versions of the same software in parallel. Unfortunately, Nancy Levenson and

others have shown that the "independently-written" versions cannot be assumed to have independent failure modes.

So, is technique 2 worthless? By no means: It's just often misapplied. To use it, you need to establish (by formal techniques, testing, experience in the field) not just the failure rates for the individual modules, but an upper bound on failure correlation among modules. This is by no means impossible to accomplish. For physical systems, it is often assumed (with little real "proof") if the modules involved are physically far apart, and especially if they are based on different physical mechanisms - e.g., a gasoline motor-generator set as a backup for the main power grid, which in turn is driven by multiple power sources scattered over the countryside, using a variety of very different energy sources. Things get much harder when the modules have to be packed closely - correlated failures are much more of an issue in an airplane than on the overall road system of a city. The "different physical mechanisms" idea doesn't translate easily to software (though the fifth shuttle computer, using different hardware, is pretty close). n-version programming was a good idea, though it neglected this piece of the technique. That's not to say that some still-unknown variant of n-version programming can't be made to work. In fact, I'd guess that it can be, though it won't be easy - and I certainly wouldn't want to propose a mechanism. If so, then software systems to which we can reasonably ascribe "1 in 10^9" failure probabilities should be quite buildable.

It's also worth pointing out that technique 1 ALSO relies on an assumption - often unstated, rarely proven in any sense - that failures across copies of a system are uncorrelated. The fact that 100,000,000 digital watches have calculated the date correctly for the last 5 years tells us nothing at all about the probability that they will all decided incorrectly whether 2000 is a leap year. In general, technique 1 can let you make predictions about reliability in the presence of external circumstances that occur fairly frequently (e.g., wear over time); they can tell you nothing about design flaws dealing with extremely rare circumstances. Ten thousand "reactor years" of experience in and of itself tells us nothing about what will happen if a plane crashes into a containment dome. (On the other hand, we have hundreds of thousands of "experience years" with steel-reinforced concrete shells.)

In fact, techniques 1 and 2 are fundamentally the same thing: One cuts the world "vertically" between many complete copies of the same system; the other cuts the system itself "horizontally" across its components. The same two issues - reliablity of the individual slices; independence of failure modes - occurs in both cases. Either technique can be used to get believable failure estimates in the 1 in 10^8 (or even better) range. Such estimates are never easy to obtain - but they ARE possible. Rejecting them out of hand is as much a risk as accepting them at face value.

-- Jerry

Re: Predicting System Reliability...

<bruce_hamilton.osbu_south@xerox.com>
Fri, 8 Feb 1991 10:23:01 PST

Re: "...you test hundreds or even thousands of units, all in parallel. This is how a disk drive manufacturer can say something like "50,000 Hours Mean Time Between Failures" -- you didn't think they actually had a single drive that they tested for 50K+ hours, did you? I would go so far as to say that no well known drive manufacturer today has a single drive with 50K hours on it"

I'm no M.E., but it's absurd to suggest that any mechanical system can be meaningfully tested in parallel. Fatigue, friction, dust accumulations, etc. occur as a result of cumulative loads on a single system.

I can't speak for disk drives, but Aviation Week often talks about how one airframe of each new type is used for fatigue testing, undergoing thousands of repeated pressurize/depressurize cycles.

--Bruce BHamilton.OSBU_South@Xerox.COM 213/333-8075

Electronic traffic signs endanger motorists...

Lars Henrik Mathiesen <thorinn@diku.dk>
Fri, 8 Feb 91 19:33:45 +0100

>I can only
>imagine what we are going to see happen when they start displaying things like
>"LEFT LANE BLOCKED, USE COLLECTORS AHEAD" and 700 motorists first slow down to
>read this and then try and pull over to the two rightmost lanes in order to
>exit off that section of the highway.

I have seen a similar system in use in Belgium or the Netherlands; there, however, they know enough to limit the information to a few bits. Each lane has a square display that can show symbols for "go ahead", "don't use this lane", lane changes (to warn of upcoming closed lanes) and speed limits; the first two are color-coded (green and red, of course).

The displays stand at intervals of 1/2 to two miles, closest around exits etc.. Since they are visible at a distance of at least 1/2 mile, nobody has to slow down or think. There were a fair amount of roadworks at the time I was there, and the system really helped the traffic flow.

>From what pictures I've seen, the amount of text on North American traffic signs would strike a European traffic engineer with horror. I'd think that it all only works because most drivers are commuters who don't really need to read the signs.

The RISK of the Toronto system is that the computer system can confuse everybody in a new way every day.

Lars Mathiesen, DIKU, U of Copenhagen, Denmark [uunet!]mcsun!diku!thorinn
Institute of Datalogy -- we're scientists, not engineers. thorinn@diku.dk

---

Newborn security system

"Always mount a scratch monkey. 08-Feb-1991 0832" <edp@jareth.enet.dec.com>
Fri, 8 Feb 91 07:36:21 PST

The following is from the Nashua, New Hampshire, _Telegraph_, by Denise Lavoie of Associated Press, entitled "Hospitals using electronic security to protect newborns":

> Retailers use them to keep shoplifters from walking off with their merchandise. Now hospitals are using electronic security devices to protect a more precious commodity: newborns. ...
>
> St. Francis Hospital and Medical Center in Hartford quietly installed an electronic surveillance system after a woman kidnapped a 16-hour-old baby from a maternity ward two years ago. The girl was found unharmed 12 hours later.
>
> Abington Memorial Hospital in Abington, Pa., has one of the more elaborate systems. There, the infant bracelets trigger an alarm and automatically turn on a video camera that records an abduction.
>
> St. Joseph's Medical Center in Wichita, Kan., normally uses the sensitized wrist bracelets, but has experimented with sensitized tags that are sewn into babies' clothing, and sometimes, their diapers. ...
>
> The costs of the systems vary, depending on how sophisticated a hospital wants to get. Some hospitals want a system that triggers an alarm, turns on a video camera, and even locks the doors and elevators, [Sam] Shirley [of Sensormatic Electronic Corp.] said. ...

Automatic door locks is obviously a disaster waiting to happen -- imagine the plight of people in a fire who realize they can leave but they cannot take the babies with them.

-- edp (Eric Postpischil)

---

request for info on UNIX viruses

Tom Brendza <tomb@bellhow.UUCP>
Thu, 7 Feb 91 15:49:06 EST

I am requesting the following information as part of a research project involving computer viruses, prophylactic software, and recovery procedures. When the research is completed, I will gladly make available any information that I am able to release to any interested RISKS readers.

Has there ever been a documented occurence of a computer virus attacking the UNIX operating system outside of laboratory conditions? I refer to the strict definition of "computer virus" (i.e. reproducing by attaching itself to existing code), and not the standard media definition of computer virus (i.e. just about anything).

Personal anecdotes are also welcome.

Any information regarding this matter (including other places to request information) would be greatly appreciated. Please contact me at:

Tom Brendza, Bell & Howell, PSC, 5700 Lombardo Center #220
Cleveland, OH 44131-2531 (216) 642-9060 x288 (voice)
..!usenet.ins.cwru.edu!ncoast!ushiva!bellhow!tomb

Search RISKS using swish-e

THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

ACM Committee on Computers and Public Policy, Peter G. Neumann, moderator

Volume 11: Issue 8

Wednesday 13 February 1991

Contents

News of His Death Much Exaggerated

Jeff Johnson <jjohnson@hpljaj.hpl.hp.com>
Tue, 12 Feb 91 14:15:18 PST

The San Francisco Chronicle (11 Feb 91) has on the second page a photo of a man pointing to the Vietnam War Memorial wall in Washington, D.C. The caption reads:

> "Vietnam veteran Eugene J. Toni of suburban Virginia pointed to his name on the Vietnam Memorial in Washington yesterday. Toni, a 41-year-old former Army sergeant, is one of 14 Americans who can find their own names carved in black granite among the 58,175 dead and missing in the war. Toni was listed because a wrong number was typed into a computer."

JJ, HP Labs

Prison terms for airline computer ticketing fraud

Rodney Hoffman <Hoffman.El_Segundo@Xerox.com>
Wed, 13 Feb 1991 09:50:06 PST

In RISKS 7.72, I summarized a 'Wall Street Journal' article about a travel agency employee charged with breaking into American Airline's computer reservations system for fraud.

I believe this recent item is the conclusion of that case:

'Los Angeles Times', 11 Feb. '91: TRAVEL AGENTS SENTENCED: Their federal terms ranged from nearly two years to four years in prison for running a scheme to defraud American Airlines of frequent-flier tickets totaling $1.3 million between 1986 and 1987. Through a computer reservation terminal at North Ranch Travel Agency in Woodland Hills (CA), the three men changed American Airlines' records on frequent fliers, crediting fictitious accounts with miles flown by legitimate passengers not enrolled in the frequent-flier program. The defendants then used the miles to apply for free flights, sold them for profit or gave them to friends and family. They were convicted after a trial last year. (Case No. 90-409. Sentencing Feb. 5)

PWR system "abandoned owing to technical problems"

Martyn Thomas <mct@praxis.co.uk>
Wed, 13 Feb 91 13:25:04 GMT

The following story is from Nucleonics Week (pubs: McGraw-Hill) Vol 32 No 1 (Jan 3 1991) and No 2 (Jan 10 1991).

Electricite de France (EDF) has decided in principle to abandon the Controbloc P20 decentralised plant supervisory computer system developed by Cegelec for EDF's new N4 Pressurised Water Reactor (PWR) series, because of major difficulties in perfecting the new product, according to EDF officials.

EDF does not yet know [as of Jan 3rd] what it can use in place of the P20 to control the N4 reactors, the first of which is nearly completed. [They were meeting to decide the way forward on January 25th. Options include trying to salvage parts of the P20, or reverting to the N20 system used to control the earlier P4 series of reactors {the numbering seems maximally confusing}. Unfortunately, the P20 data acquisition and control uses dual LANs, called Controbus, whereas the N20 uses cables. If they fall back to the N20, they will have to design miles of cables into the reactor to replace the LANs.]

A Cegelec official described the P20 as "the most ambitious system you could imagine". It has distributed control and monitoring, programmable logic controllers, and 32-bit microprocessors. The N20 used 8-bit microprocessors.

Cegelec blame EDF reorganisations for the cancellation, but EDF's engineering

and construction division say that the problems were strictly technical. According to Pierre Bacher, the division's president, the failure to achieve sufficient capacity to process the mass of acquired reactor data with the original P20 architecture had led to "increasingly complex software programs" with "increasingly numerous interactions between subsystems". The complexity apparently grew to the point where modification became difficult and there was fear that the system could never be qualified [which I take to mean certified for use].

According to the report, "Ontario Hydro faced a similar situation at its Darlington station, in which proving the safety effectiveness of a sophisticated computerized shutdown system delayed startup of the first unit through much of 1989. Last year, faced with regulatory complaints that the software was too difficult to adapt to operating changes, Hydro decided to replace it altogether". [I hope that Dave Parnas or Nancy Leveson can fill in the details here.]

Of particular interest to UK RISKS readers is the fact that the P20 system is on order for the Sizewell B PWR (due to load fuel in November 1993, and the only remaining scheduled PWR in the UK nuclear power programme). The P20 "is to be applied less to safety systems at Sizewell than was planned on the N4", the report says. [Sizewell has a separate shutdown system, although there are rumours that all is not well with it.]

There is a fully computerised N4 control room designed to go with the P20 system. If the P20 cannot be salvaged, presumably this will be abandoned too.

[There is more detail in the two reports, which I recommend interested readers acquire].

Martyn Thomas, Praxis plc, 20 Manvers Street, Bath BA1 1PX UK.
Tel: +44-225-444700. Email: mct@praxis.co.uk

Risks of having a sister

Robyn A Grunberg <rag@yarra.oz.au>
12 Feb 91 02:32:26 GMT

On Thursday 7th February, I arrived home from an interstate trip to find a letter in the mail stating that my driver's license had been cancelled for 6 months. The cancellation took effect from January 15th, 1991 and was to continue until July 15th 1991. The cancellation was due to my driving a car while exceeding the state limit of .05% alcohol in my bloodstream. This interested me greatly as I had not been breathalised nor blood tested on (or even near) the day in question, stated on the notice as December 17th 1990.

The following day I approached VICROADS who had sent me the notice. I explained to them that I was not the offender of the crime and the clerk called up the details of the charge. My name was listed, as well as my license number, however the registration number of the car involved in the incident was not the registration number of my car. The clerk suggested I fill out a Statuary Declaration and file that (along with the notice) with them so that

the department could place the matter under investigation.

I then went to the Police Station where I obtained a Statuary Declaration and had it witnessed. I also asked if the officer could check and see whose car was involved, as it wasn't mine. The officer checked out the records and returned to tell me that the car belonged to my sister, who is unlicensed. He also explained that I was able to drive as long as I carried the Stat Dec with me at all times.

Unfortunately, my licensed expired *that day*, so I then had to approach VICROADS and try and get them to reissue my license. The clerk would not reissue my license as it was currently under cancellation. I showed him the Stat Dec, which was no use to him (or me) at all, he could not reissue the license until the matter is resolved. He suggested I continue driving with the Stat Dec. I would not accept this statement from him and asked he put in writing the fact that I had attempted to renew my license and he had refused to reissue it. He would not put it in writing, and suggested I speak to his supervisor.

So here I am without a license, and waiting for the matter to be heard. It would appear that my sister was breathalised and gave my details when asked who she was. The car, she explained, she had borrowed from her sister Michealle, which the police accepted in good faith. As far as the police are concered, all you need do is state your name, address and birthdate (which she did) and the police will accept this and demand that you show your license at a later date. Unfortunately, they also went ahead and cancelled my license without any proof that she was who she stated being, as she hasn't produced the license at any stage.

Re: Risks of having a sister

Charles Meo <cm@yarra.oz.au>
13 Feb 91 04:17:20 GMT

For non-Australians it is worth pointing out that under unique (and unsuccessfully opposed) legislation, the burden of proof has been reversed and police are empowered to record a conviction _without_ any judicial process whatever and the driver is then obliged to prove his or her _innocence_ in the matter.

This has enabled local police to generate enormous government revenues as many traffic infringements are now handled in this way.

I do not know of any other civilised country that would allow this (the spirits of the old prison governors are alive and well in our seats of government!) and of course, when this law is translated into computer systems with _no_ safe guards the situation Robyn has described can happen easily.

C. Meo #6512441/L (Turn to the right!)

Re: Study links leukemia to power lines, TV's

<smb@ulysses.att.com>
Sat, 09 Feb 91 23:46:22 EST

The original AP story was considerably longer, and included many more qualifiers. As noted in the excerpt your paper ran, this study will receive very careful scrutiny because it was sponsored by an industry group.

The methodology has been described as somewhat suspect by the Electric Power Research Institute, though the University describes the findings as significant. The parents of children being treated for leukemia were quizzed about their child's activities; their responses were compared with those of a control group. (The article did not say how the control group was selected.) Unfortunately, memory plays funny tricks; in an era where newspapers often seem to feature the carcinogen of the week, parents of such children may -- and I stress the word ``may'' -- be more likely to recall suspect behavior patterns. (For example, the article noted a correlation to home use of pesticides, and to paternal exposure to spray paint at work during the pregnancy.)

More troubling, the objective measurements taken don't seem to agree with the incidence of disease. For example, bedroom electric field strength measurements did not differ between the two groups, though since the measurements used were 24 hour averages, there may have been differing peaks. Similarly, there is no particularly obvious reason to suspect black-and-white TVs; according to the article, the researchers ``speculated'' that such sets might be older, and hence might not meet current standards. (If we're guessing, I'd guess that such TVs are smaller, and hence would be watched from a closer distance.)

No statistically significant correlation was found with use of electric blankets or hair curlers; the former, at least, would (as I recall) contradict other studies.

The study itself has not been released, and will not be, pending peer review and publication in a refereed journal. But a precis was released by the university and by the sponsors.

--Steve Bellovin

Re: Predicting System Reliability...

"Jay Elinsky" <ELINSKY@IBM.COM>
Sun, 10 Feb 91 00:16:56 EST

Re Brad Knowles' statement that disk drives are tested in parallel, and Bruce Hamilton's rejoinder that mechanical systems can't be tested in parallel: Just as the airframes in Bruce's example are presumably pressurized and depressurized at a much higher rate than occurs in actual takeoff-landing cycles, disk drives can presumably be tested at a higher duty cycle than they see in actual use. That is, the manufacturer can keep the heads thrashing around continually, unlike the typical drive on a desktop computer. I don't

know how one would accelerate a test on a mainframe disk drive that perhaps does thrash around 24 hours a day, nor do I know if it's possible to accelerate the testing of the platter bearings, which are spinning 24 hours a day even on powered-up but otherwise idle machines.

So, I assume (and I'm no M.E. either) that parallel testing is combined with tests that tend to accelerate wear of components where possible.

Jay Elinsky, IBM T.J. Watson Research Center, Yorktown Heights, NY

Re: Building very reliable systems

Dr. Tanner Andrews <tanner@ki4pv.compu.com>
Sun, 10 Feb 91 9:51:25 EST

) The theory here is that running 100 units for 100 hours gives you
) the same information as running one unit for 10000 hours.
The theory is crocked. It builds heat slowly. The actual behavior:
100 hours: a little warm
200 hours: case is softening
250 hours: case melts
257 hours: catches fire
The times and failure modes will vary, depending on the type of device in question.

...!{bikini.cis.ufl.edu allegra uunet!cdin-1}!ki4pv!tanner

Re: building very reliable systems

Martyn Thomas <mct@praxis.co.uk>
Mon, 11 Feb 91 11:47:59 GMT

Jerry Leichter <leichter@lrw.com> writes:
.....
: 2. Functional decomposition of the system into a number of modules
: such that failure can occur only when ALL the modules fail.

: Now, the criticism of technique 2 is that the multiplication of failure proba-
: bilities is only valid when the failures of the different modules are known
: to be uncorrelated.
.....
: So, is technique 2 worthless? By no means: It's just often misapplied. To
: use it, you need to establish (by formal techniques, testing, experience in
: the field) not just the failure rates for the individual modules, but an
: upper bound on failure correlation among modules. This is by no means impos-
: sible to accomplish.
.....
: That's not to say that some still-unknown variant of n-version programming
: can't be made to work. In fact, I'd guess that it can be, though it won't
: be easy - and I certainly wouldn't want to propose a mechanism. If so, then
: software systems to which we can reasonably ascribe "1 in 10^9" failure

: probabilities should be quite buildable.

[I have extracted the elements from Jerry's article that I want to disagree with. I thought the articles as a whole was a very valuable contribution to the discussion. I apologise in advance if I have distorted his argument by selective quotation.]

How can we have confidence that the means by which we have combined the n-versions (for example, the voting logic) has a failure probability below 1 in 10^9?

How can we be sure that our analysis of the upper bound on failure correlation among modules is accurate? How accurate does it need to be - does it need to have a probability of less than 1 in 10^9 that it is grossly wrong? (By "grossly wrong" I mean wrong enough to invalidate the calculation that the overall system meets the "1 in 10^9" figure). This would seem impossible. Consider, for example, the probability that the common specification is wrong.

I also have a question for statisticians: if we are attempting to build a system "to which we can reasonably ascribe a 1 in 10^9 failure probability", what *confidence level* should we aim for, if we are using statistical methods? Does it make sense to be satisfied with 99% confidence of 1 in 10^9? Or should we aim for 99.9999999%? (I hope the answer isn't simply "it depends what you mean by "reasonably". I am looking for guidance on how the failure probability and the confidence levels interact in practical use).

(I suspect that I am missing some contributions to this discussion. I would be grateful if anyone following-up would also copy me by email).

Martyn Thomas, Praxis plc, 20 Manvers Street, Bath BA1 1PX UK.
Tel: +44-225-444700. Email: mct@praxis.co.uk

Re: Predicting System Reliability...

"Jay Elinsky" <ELINSKY@YKTVMZ.BITNET>
Sun, 10 Feb 91 00:11:17 EST

Re Brad Knowles' statement that disk drives are tested in parallel, and Bruce Hamilton's rejoinder that mechanical systems can't be tested in parallel: Just as the airframes in Bruce's example are presumably pressurized and depressurized at a much higher rate than occurs in actual takeoff-landing cycles, disk drives can presumably be tested at a higher duty cycle than they see in actual use. That is, the manufacturer can keep the heads thrashing around continually, unlike the typical drive on a desktop computer. I don't know how one would accelerate a test on a mainframe disk drive that perhaps does thrash around 24 hours a day, nor do I know if it's possible to accelerate the testing of the platter bearings, which are spinning 24 hours a day even on powered-up but otherwise idle machines.

So, I assume (and I'm no M.E. either) that parallel testing is combined with tests that tend to accelerate wear of components where possible.

Jay Elinsky, IBM T.J. Watson Research Center, Yorktown Heights, NY

Re: Building very reliable systems (Jerry Leichter, RISKS-11.07)

Paul Ammann <pammann@gmuvax2.gmu.edu>
Mon, 11 Feb 91 13:22:03 -0500

> 1. Testing (whether by explicit test in a lab or by actual use in
> the field) of very large numbers of copies of the system
> 2. Functional decomposition of the system into a number of modules
> such that failure can occur only when ALL the modules fail.

The first technique assesses performance directly, and can be applied to any system, regardless of its construction. As Jerry points out, various assumptions must be made about the environment in which the testing takes place. The second technique estimates performance from a predictive model.

> [...] To
>use [NVP], you need to establish (by formal techniques, testing, experience in
>the field) not just the failure rates for the individual modules, but an
>upper bound on failure correlation among modules.

The Eckhardt and Lee model (TSE Dec 1985) makes it clear that performance prediction is much more difficult. To evaluate a particular type of system, one must know what fraction of the components are expected to fail over the entire distribution of inputs. The exact data is, from a practical point of view, impossible to collect. Unfortunately, minor variations in the data result in radically different estimates of performance. For a specific system, it is not clear (to me, anyway) what an appropriate "upper bound of failure correlation among modules" would be, let alone how one would obtain it.

>In fact, techniques 1 and 2 are fundamentally the same thing: One cuts the
>world "vertically" between many complete copies of the same system; the other
>cuts the system itself "horizontally" across its components. The same two
>issues - reliability of the individual slices; independence of failure modes -
>occurs in both cases.

I am uncomfortable with merging the issues of direct measurement with those of indirect estimation. The difficulties in 1 are primarily system issues; details of the various components are by and large irrelevant. In technique 2 the major issue is the failure relationship between components.

> Either technique can be used to get believable failure
>estimates in the 1 in 10^8 (or even better) range. Such estimates are never
>easy to obtain - but they ARE possible. Rejecting them out of hand is as much
>a risk as accepting them at face value.

I am unaware of any application of NVP in which it has been (believably) demonstrated that components of modest failure probability (say 1 in 10^4) can been used to generate a system with a very low failure probability (say 1 in 10^8). The relatively scant empirical evidence indicates that NVP

might be good for an order of magnitude or so (which may be great, depending upon the system). However, there are no guarantees; in certain circumstances, NVP may well be worse than the use of a single component. The real issue is economic: could better systems be built by applying development resources to other technique(s). There are strong views on both sides of the question.

(As a final aside, there are random algorithms that, for certain well behaved problems, *can* justifiably employ an independence model to obtain very low system failure probabilities. However, these techniques are not in the domain of NVP).

-- Paul Ammann: pammann@gmuvax2.gmu.edu (703) 764-4664
-- George Mason University, Fairfax VA

Search RISKS using swish-e

THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

ACM Committee on Computers and Public Policy, Peter G. Neumann, moderator

Volume 11: Issue 9

Thursday 14 February 1991

Contents

Vote-by-fax plan before Legislature

<clarinews@clarinet.com>
6 Feb 91 02:49:14 GMT

mit.edu!hsdndev!wuarchive!uwm.edu!lll-winken!looking!clarinews

[Provided for USENET readers by ClariNet Communications Corp. This copyrighted material is for one-time USENET distribution only.] [SEE END OF MESSAGE!]

SACRAMENTO (UPI) -- Troops fighting in the Persian Gulf could vote in California elections by using fax machines to cast their ballots under

legislation announced Tuesday.

The measure, SB293, would amend the state Elections Code to allow members of the military and other California voters temporarily living outside the United States to fax absentee ballot applications to county election officials.

County officials would then use fax machines to send absentee ballots to overseas voters, who could return the completed ballots by fax.

``Even when applications for overseas absentee ballots are received early in the process, ballots sent halfway around the world sometimes arrive too late to be returned by mail before the close of polls on Election Day,'' Secretary of State March Fong Eu said.

``This legislation would allow overseas voters, such as those members of the armed forces stationed in the Middle East as part of Operation Desert Storm, to fax their voted ballots back in time to be counted,'' she said.

The bill is coauthored by state Sen. Milton Marks, D-San Francisco, and Assemblyman Peter Chacon, D-San Diego.

Only a few people stationed at U.S. embassies, working at projects overseas, and members of the military would be expected to take advantage of the vote-by-fax program, Eu's spokeswoman Melissa Warren said.

``The numbers aren't huge. We aren't expecting large numbers of people to participate,'' she said.

Several states accepted vote-by-fax ballots during last November's elections, Warren said. If the measure is quickly passed by the Legislature and signed by Gov. Pete Wilson, the first California election with fax voting would be the March 19 special elections for two state Senate seats and one Assembly seat.

Marks said he would rush the measure through the Legislature. ``It seems only fitting that at a time when we are engaged in a military struggle with a ruthless despot, we make this effort to provide our servicemen and women with the most important franchise of our democratic system -- the right to vote,'' he said.

[This item submitted to RISKS by Eric Postpischil <edp@jareth.enet.dec.com>.
THE RESPONSE FROM clarinews@clarinet.com TO PGN's REQUEST FOR PERMISSION TO REUSE THE ABOVE IN RISKS IS From: Brad Templeton <brad@looking.on.ca>:
"The one time statement indicates you have to ask for more. You did, so I'll grant permission for RISKS in electronic form. (We are unable to grant permission for print forms). Brad"]

[Nice phrase, "take advantage" of it!!! Nice opportunities for voter fraud? I hope some sort of authentication is planned... PGN]

Douglas goes fly-by-wire

Martyn Thomas <mct@praxis.co.uk>
Thu, 14 Feb 91 13:19:09 GMT

McDonnell Douglas has switched to a full fly-by-wire flight control system for its MD-12X, reports Flight International (13-19 Feb 1991, p4).

"With fly-by-wire we are able to retain the flying qualities of the aircraft and more easily resemble MD-11 [handling]". "The benefit is predominately in

the area of cross-crew training". "A fly-by-wire aircraft should also be cheaper to produce". [quotes from MD-12X management].

The control system will be modelled on that developed by GE aerospace for the USAF C-17 airlifter.

Martyn Thomas, Praxis plc, 20 Manvers Street, Bath BA1 1PX UK.
Tel: +44-225-444700. Email: mct@praxis.co.uk

Vietnam Vet's Memorial article ambiguous (Johnson, RISKS-11.08)

Go Mossad! 14-Feb-1991 0938 <levitin@cadsys.enet.dec.com>
Thu, 14 Feb 91 06:39:12 PST

RE: Jeff Johnson's article in RISKS 11.08 about the Vietnam Vets' memorial and a photo in the SF Chronicle, I didn't see the photo, but I do know that there is a possibility that this situation is *not* due to a typo. On the Vietnam Veterans' Memorial in DC, there is a set of symbols: one to denote "Killed" (a cross?), one for "Missing in Action", and "Formerly MIA but now known to have survived" (a circle?). The symbol used for MIA can be further carved in one way to become the symbol for Killed in Action, and can be further carved in a different way to become the symbol for "Formerly MIA".

Because I don't know which symbol appeared next to Eugene J. Toni's name on the monument, I won't comment on the possibility of a typographical error, as reported by the Chronicle. However, the language in the caption (or perhaps the title of Johnson's RISKS article) makes it too easy for the reader to believe that Toni was formerly believed killed.

Sam Levitin Digital Equipment Corporation

Tax Preparation

Peter Jones <MAINT@UQAM.bitnet>
Thu, 14 Feb 91 12:12:12 EST

Today, I saw an advertisement in the mail about a new service on Bell's ALEX service offering income tax preparation assistance. Customers can supply income tax information and then order completed forms by mail. The RISKS I see are:

1) Transmitting confidential data in the clear over public phone lines.

2) Giving the service provider potential access to a lot of confidential information: SIN (SSN in the US), income, address, credit card number,... I found no mention of safeguards of confidential information when I browsed the literature.

3) Possible loss of all data entered if the phone connection is broken (unless the system provides a checkpoint facility. I don't want to spend $$$ to find out.

4) Underestimation of costs. The literature quotes about $12 for mailing, and this ALEX service costs $0.15/min. The literature estimates connect time to be 30 minutes for a couple. So we're talking about $35 or so here, and this may be optimistic (see 3, especially if the phone has Call Waiting.)

5) The system only covers certain basic forms (this is stated in the literature. So you have to be fairly knowledgeable about income tax to decide if the system is worth using.

Peter Jones (514)-987-3542 UUCP: ...psuvax1!uqam.bitnet!maint
Internet:Peter Jones <MAINT%UQAM.bitnet@ugw.utcs.utoronto.ca>

Collection of Evaded Taxes

Cameron Laird <news@lgc.com>
Mon, 11 Feb 91 09:47:17 CST

Comp.risks supports continuing discussions on advantages and disadvantages of automation of financial transactions; most recent was a proposal for an AmeriCard, which would facilitate or enforce movement of all purchases to equipment which would record those purchases. One of the advantages claimed for such schemes, including Mr. Gorbachev's latest "monetary reform", is that they'll flush not-fully-taxed activities into the spotlight of tax enforcement agencies. For example, if you rebuild your neighbor's carburetor in exchange for him removing the dying tree in your backyard, the Internal Revenue Service expects you both to declare those (imputed) incomes and pay corresponding taxes on them. Thus, as an article in the 21 January 1991 *Forbes* asks, "Politicians of all stripes love to claim the federal deficit can be cut by cracking down on tax cheats. Why cut spending when the IRS has $78 billion in total accounts receivable and is losing $100 billion a year to tax evasion?"

The article's conclusion: "The argument ... grossly exaggerates the IRS' ability to raise more money through tougher enforcement." Note that the Agency has strong institutional pressures to overestimate its capabilities. Most interesting from the point of view of economic science is the (unsupported) assertion that, "As for outright cheating, even the IRS' toughest audits find less than half the evasion it claims goes on." In the midst of tendentious estimates and murkiness, there's a real value in looking at the actual operating experience of, for example, the IRS.

I've marked the distribution of this note for "world" because it's at least as great an issue outside the USA. France, for example, sometimes prides itself on the vigor with which its citizens fail to co-operate with tax agencies; from my little experience there, though, I can report that people were generally more law-abiding than they should have to be, given the confusion those agencies generate.

The article does make one incomplete reference to a scholarly study. The reporter might be willing to help someone pursue the subject; I've known some who do, and some who don't.

I summarize: for the reasons others have already stated in comp.risks, tax enforcement does *not* yield the windfalls some expect of it; in particular, the IRS' own records suggest much lower returns than they estimate in their reports to Congress.

Cameron Laird USA 713-579-4613 USA 713-996-8546

Singacard anyone?

Bill J Biesty <wjb@edsr.UUCP>
Thu, 14 Feb 91 09:33:35 CST

>From the Wall Street Journal Wednesday, February 13, 1991, p.A7 c.1

"Singapore Equals Push Buttons"
From cashless shopping to electronic paperwork and even a computerized pig auction, Singapore is plugging its 2.6 million people into electronic grids linking the entire island nation. It plans to build grids for shopping, booking tickets, checking data and sending documents.
Singapore's small size and centralized bureaucracy simplified establishing the electronic groundwork. All citizens carry a numbered identification card, allowing cross-indexing of data. "The purpose ... is to turn Singapore into an intelligent island in which IT [information technology] will be fully exploited to improve business competiveness and, more importantly, to enhance the quality of life," and education ministry official said. A master plan, IT 2000, will be unveiled at year end.
Already, TRadeNet lets companies submit data electronically to the state and accounts for 90% of all trade documents. The Network for Electronic Transfers, a cashless shopping system, has been operating for five years and is used by more than one-third of the population.
Other networks include StarNet for air cargo, MedNet for Medical claims, and LawNet for company registry. Coming next: "Smart Town," linking households.

I think it was mentioned in Risks, but was mentioned in WSJ that Singapore plans to install sensors in cars and roads and start taxing vehicle owners based on usage rather than an average fee to cover maintenance costs of roads.

Considering Singapore's government, widely considered autocratic, though it is democratically elected, this will probably be less than beneficial to the entire populace. (The Editorial and Letters pages of the WSJ recently had a debate on this. Nepotism seems to be one indicator. Sorry no dates.)

The risk envolved is for those people whose idea of "quality of life" has nothing to do with feeding the commercial/consumer dynamo. Then again they probably don't live in Singapore.

Another is as long as you're a good little consumer and a good little entrepreneur you're ok. The ability to catch laggards and other non-productive types cannot be underestimated. You've heard of sin taxes, Lazy Tax anyone?

What the article doesn't mention is how much independence exists for the

businesses that use the Nets. Are the Nets a government service or control of all players using them? Will the Nets provide a situation similar to the national airline reservation system(s) or will they nationalize industries under monarchical control.

Bill Biesty, Electronic Data Systems Corp., Research and Advanced Dev., 7223 Forest Lane, Dallas, TX 75230 edsr.eds.com!wjb wjb@edsr.eds.com 214-661-6058

The new CA driver license (RISKS-11.07)

Ian Clements <ian@lassen.wpd.sgi.com>
Mon, 11 Feb 91 8:00:32 PST

In RISKS 11.04 Mark Gabriel writes about privacy issues concerning the new CA drivers license. In issue 11.07 David Redell responds with two points concerning recent privacy legislation and the clerks right to certain parts of the information.

Like many modern marvels, the magnetic strip is easily defeated. If you're concerned about what a clerk may or may not record or know about you, run a magnet down the stripe. This will render the stripe useless and the clerk (or police officer) will once again have to rely on mechanical recording.

I would be more concerned about the possibilities for abuse of this new technology. Insurance companies will surely ask potential customers for a drivers license to check the driving record (given CA's new insurance rules, there is much incentive to bit twiddle)--how long will it be before someone figures out how to rearrange bits on the stripe?

--ian Ian Clements ian@sgi.com 415/962-3410

Re: The new California licenses (Hibbert, RISKS-11.03)

Curt Sampson <curt@cynic.wimsey.bc.ca>
Sat, 09 Feb 91 10:40:56 PST

> This track will only contain 40 bytes of information, and will only
> contain the name, driver' license number, and expiration date.

This would not likely leave more than 32 bytes for the person's name.
Yet another problem. <Sigh>

Coercivity is a measure of how much magnetic energy it takes to imprint or erase a magnetic medium, and it is measured in oersteds. The typical coercivity of a cassette tape would be in the 280-380 oersted range. The typical coercivity of a high-coercivity tape (such as DAT or 8 mm video) would be 1000-1400 oersteds.

30 orsteds is quite low (surprisingly low, in fact). That may explain why my bank card has been "zapped" twice in the past year. 3600 is quite high, but a standard videotape eraser might be able to affect it if you put the stripe

right up against the surface. (An audiotape eraser would not affect it.)

I have little doubt that a dedicated hardware hacker would be able to come up with a unit to read from and write to the cards with little difficulty. The hardest part would probably be machining a head to read the stripe. I wonder if the data is going to be encrypted in any way?

cjs curt@cynic.wimsey.bc.ca curt@cynic.uucp {uunet|ubc-cs}!van-bc!cynic!curt

---

Re: automatic flight and seasickness (Bryant, RISKS-11.07)

Lars-Henrik Eriksson <lhe@sics.se>
Sun, 10 Feb 91 11:33:17 GMT

> [Re: Bryant on Olivier M.J. Crepin-Leblond" <UMEEB37@vaxa.cc.imperial.ac.uk> in RISKS-10.83]

I believe the original poster is right. I am a private pilot, and I have noticed numerous times, that I do have a tendency to get sick when I go along a a passenger. I have even noticed this tendency when flying the aircraft myself with an instructor who tells me what to do. When a fly as the pilot-in-command, I have *no* problems with airsickness even on extended flights in rough weather.

Lars-Henrik Eriksson, Swedish Institute of Computer Science, Box 1263, S-164 28 KISTA, SWEDEN +46 8 752 15 09

---

follow-up to wireless network

frank letts <letts@ficc.ferranti.com>
Sun Feb 10 13:16:10 1991

There seems to be some question regarding the legality of the radio telemetry testing I described in an earlier post. The story was presented with a bent toward the (objectively) humorous and the obvious risks presented by the wireless network. Left out was some information that, by its absence, led some to believe the the operation was an illegal one carried out by "sickos" and technically incompetent bozos.

The oil company held a valid FCC license for data transmission over the frequency in its normal operation mode, and a temporary permit for same at low power in the Houston facility. While looking for the source of the interference we did find some bad dummy loads which we replaced, but, following that, our installation was on spec and fully legal. We did determine that the delivery driver(s) were running linear amps and were bleeding over onto adjacent frequencies when transmitting. That would explain their interfering with our operation, but not our interfering with them. Odds were that the driver(s) only heard the buzzing while driving directly past our building. They should have had no problem receiving or transmitting.

As far as the personnel are concerned, the engineer and technicians all held

FCC tickets, were highly qualified for the work, and had been in the business for many years. I have been doing data acquisition and communications software for about twenty years and consider myself somewhat competent in the area. None of us are necessarily sickos. One of the techs probably qualifies as a bozo, but he's a nice enough fellow and a decent tech.

I hope that this quiets any unrest out there.

Frank Letts, Ferranti International Controls Corp., Sugar Land, Texas
(713)274-5509

4th Annual Ides-of-March Virus & Security Conference

Judy S. Brand <jsb@well.sf.ca.us>
Fri, 8 Feb 91 08:54:37 -0500

Who SHOULD attend this year's Ides-of-March
Fourth Annual Computer VIRUS & SECURITY Conference
at the New York World Trade Center?

MIS Directors, Security Analysts, Software Engineers, Operations Managers, Academic Researchers, Technical Writers, Criminal Investigators, Hardware Manufacturers, Lead Programmers who are interested in:

WORLD-RENOWNED SECURITY EXPERTS:	CRIMINAL JUSTICE LEADERS:
Dorothy Denning - DEC	Bill Cook - US Justice Dept
Harold Highland - Comp & Security	Donn Parker - SRI Intl
Bill Murray - Deloitte & Touche	Steve Purdy - US Secret Service
Dennis Steinauer - NIST	Gail Thackeray - AZ Attorney

UNIVERSITY RESEARCH LEADERS:	LEGAL/SOCIAL ISSUES EXPERTS:
Klaus Brunnstein - Hamburg	Mike Godwin & Mitch Kapor - EFF
Lance Hoffman - GWU	Emmanuel Goldstein - 2600 Magazine
Eugene Spafford - SERC/Purdue	Tom Guidoboni - (R.Morris' lawyer)
Ken van Wyk - CERT/CMU	Marc Rotenberg - CPSR

PLUS Fred Cohen, Ross (FluShot) Greenberg, Andy (DrPanda) Hopkins, and over 40 MORE!

Over 35 PRODUCT DEMOS including: include Candle's Deltamon, HJC's Virex, McAfeeSCAN, Symantec's SAM, ASP 3.0, DDI's Physician, Gilmore's FICHEK, Certus, FluShot Plus, Iris's Virus Free, 5D/Mace's Vaccine, Norton Utilities, PC Tools, Quarantine, Viruscan, Panda's Bear Trap, Disk Defender, Top Secret, Omni, ACF2, RACF and OTHERS AS REGISTRANTS REQUEST.

FIFTY PRESENTATIONS INCLUDE:
Security on UNIX Platforms, Tips for Investigators, HURRICANE Recovery, Dissecting/Disassembling Viruses, 6 Bytes for Detection, LAN Recovery, ISDN/X.25/VOICE Security, Encryption, Apple's Security, EARTHQUAKE Recovery, IBM's High-Integrity Computing Lab, US/Export Issues, 22-ALARM Fire Recovery,

Publicly Available Help, Adding 66% More Security, NETWARE VIRUS Recovery,
Next Generation of Computer Creatures, THE WALL STREET BLACKOUT Recovery,
Mini Course in Computer Crime, Great Hacker Debate, REDUCING Recovery Costs,
S&L Crisis: Missing DP Controls, OSI and the Security Standard, Virus Myths,
Viruses in Electronic Warfare, US Armed Forces Contracts for New Ideas....

INTERESTED? ONLY $275 one day (Thurs 3/14 - Fri 3/15) or $375 both days:
* Bound, 600-page Proceedings containing ALL materials - no loose paper!
* Eight meal breaks, including Meet-the-Experts cocktail party 107th Floor
* 2-day track of product demo's * 2-day course for ICCP Security exam
* Full-day Legal & Justice Track * Full-day disaster Recoveries Track
There is a $25 discount for ACM/IEEE/DPMA members.
Fourth member in each group gets in for no charge!

To register by mail, send check payable to DPMA, credit card number
(VISA/MC/AMEX), or purchase order to:

Virus Conference
DPMA
Financial Industries Chapter
Box 894
New York, NY 10268

or FAX to (202) 728-0884. Be sure to include your member number if
requesting the discounted rate. Registrations received after 2/28/91
are $375/$395, so register now!

For registration information/assistance, call (202) 371-1013

Discounted rates available at the Penta Hotel. $89 per night. Call
(212) 736-5000, code "VIRUS"
Discounted airfares on Continental Airlines, call (800) 468-7022, code EZ3P71

Sponsored by DPMA Financial Industries Chapter, in cooperation with
ACM SIGSAC and IEEE-CS.

Search RISKS using swish-e

Report problems with the web pages to the maintainer

Search RISKS using swish-e

THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

ACM Committee on Computers and Public Policy, Peter G. Neumann, moderator

Volume 11: Issue 10

Thursday 14 February 1991

Contents

On-line in Saudi Arabia

"Martin Minow, ML3-5/U26 14-Feb-1991 1444" <minow@bolt.enet.dec.com>
Thu, 14 Feb 91 11:47:35 PST

Date: Fri, 08 Feb 91 16:06:19 -0500
From: Steve Elias <eli@pws.bull.com>
Subject: funny sco unix story

[...] at sco last week, they told me that their customer service line had received a call from a US Army dude who was calling from inside his M1 tank in the Saudi desert. apparently, SCO Unix runs on one of the computers in the tank. the customer service person pointed him to the SCO BBS system and he dialed it and downloaded the bug fix.

Steve Elias, eli@spdcc.com; 617 932 5598 (voicemail), 508 294 7556 (work phone)

[Hmm. I wonder if someone could dial up the tank's Unix? PGN]

serious bug in SVR3.2 gives root access easily

Patrick Wolfe <pwolfe@kailand.kai.com>
Wed, 13 Feb 1991 12:19:18 CST

I learned last night that the Esix operating system (really AT&T Unix System V/386 Release 3.2) which I run on my PC at home suffers from the serious security bug recently reported in comp.unix.sysv386. Someone posted a 51 line (commented) program which shows how any user with access to a shell and C compiler can obtain root priviledges with no effort at all.

I'm not familiar with all the details, but apparently it has something to do with a bug in the numeric coprocessor emulation library and the os which makes the user page (where uid information is stored) writable to the process. The posted program changes it's own effective uid and gid to zero (becoming root), and changes the permissions on /etc/{passwd,shadow} to 666 (world writable).

Apparently the bug exists in Esix 3.2, Interactive Unix version 2.02 and 2.2, and possibly others, but not in SCO Xenix or Unix, nor Intel's Unix 3.2 (these give memory faults). Interactive V2.2 users (and possibly some others - not Esix) can fix the problem by installing a 387, changing the value of one kernel variable (UAREARW) and rebuilding the kernel.

In my opinion, the rest of us are probably screwed. I seriously doubt any of these OS vendors will stop working on SVR4 to fix this bug in SVR3.2, except possibly for customers who pay for software maintenance. Many vendors are just about ready to ship their SVR4 release. I suspect most will tell those of us who don't pay for maintenance that we must upgrade to fix the bug.

It just goes to show that it was a good idea when I set my bbs up to run in a "chroot" filesystem, where even if a user could break out of the bbs program into a shell, there is no compiler (in fact, there are hardly any useful commands at all) to mess around with.

Patrick Wolfe, System Programmer/Operations Manager, Kuck & Associates, 1906 Fox Drive, Champaign IL USA 61820-7334, voice 217-356-2288, kailand!pat

Risks of large disk drives

"Roger H. Goun 12-Feb-1991 1602" <goun@ddif.enet.dec.com>
Wed, 13 Feb 91 02:03:05 PST

>From an article in the USENET newsgroup clari.nb.general, announcing a new large-capacity Winchester disk drive from Fujitsu:

"You used to have to rely on 8 inch drives for capacity, performance and

reliability," added [Mike] Gluck [senior vice president of Fujitsu America's Computer Products Group]. "Now we have put mainframe reliability into a 5.25 inch disk drive. Our MTBF (mean time between failure) is 200,000 hours and the advantage to using one large capacity drive like ours over three smaller drives is that even if the smaller drives have an equal MTBF, there are three chances to have a problem."

I see two risks here:

- As has recently been beaten to death in RISKS, the proffered MTBF figure is suspect, unless Fujitsu has actually withheld this product from market long enough to test a statistically significant number of samples for nearly 23 years;

- Mr. Gluck seems to think that having a single point of failure is less risky than having three separate (though of course not entirely decoupled) points of failure.

Roger H. Goun, Digital Equipment Corporation, 110 Spit Brook Road, ZKO2-2/O23, Nashua, NH 03062 USA, +1 603 881 0022, goun@ddif.enet.dec.com or goun%ddif.enet@decwrl.dec.com, {uunet,sun,pyramid}!decwrl!ddif.enet!goun

---

The Risks of Having a Sister (Any well informed sibling will do)

David Ruderman <ruderman@sbcs.sunysb.edu>
Thu, 14 Feb 91 16:54:12 EST

A few years ago, I encountered virtually the same problem with my driving record. I went to motor vehicles for my routine license renewal (every three years), when I noticed on the bottom line a small comment that read "Last Conviction Speed In Zone $50".

I was directed to the violations department, where they quickly consulted my records on a terminal. They told me that one year earlier I had gotten a speeding ticket and evidently paid it. They told me that I had other tickets as well. I was told that if I wanted a list of 'my' violations I would have to send $5 or so to Albany (NY) and they would send me a printout.

I discovered that my brother had simply told the police that he was me, and he did not have his license with him (his was nearly suspended). He then paid the tickets.

The Risks are clear:
- There was no confirmation of my brother's identity.
- He was able to plead me guilty by mail.
- I was not provided with a routine way to review my driving record for possible errors.
- The last risk is that I was not able to clean up my record, since the only way would be to turn in my brother to the authorities.

David Ruderman, Department of Computer Science, SUNY at Stony Brook,

Stony Brook, NY 11794-4400 ruderman@sbcs.sunysb.edu (516) 632-7675

Re: risks of having a sister

<sullivan@poincare.geom.umn.edu>
Thu, 14 Feb 91 04:02:13 CST

In the states of the USA with which I'm familiar, one must be a licensed driver to register a car. This allows a driver's license number to be associated with, say, unpaid parking tickets. I don't think that moving violations (say in the case of a hit&run driver whose plates are observed) can be ascribed to the owner of the car without other evidence. But it does seem that such a rule might be useful in Australia to discourage unlicensed drivers.

John Sullivan sullivan@geom.umn.edu

Re: Risks of having a sister

Charles Meo <cm@yarra.oz.au>
13 Feb 91 04:17:20 GMT

For non-Australians it is worth pointing out that under unique (and unsuccessfully opposed) legislation, the burden of proof has been reversed and police are empowered to record a conviction _without_ any judicial process whatever and the driver is then obliged to prove his or her _innocence_ in the matter.

This has enabled local police to generate enormous government revenues as many traffic infringements are now handled in this way.

I do not know of any other civilised country that would allow this (the spirits of the old prison governors are alive and well in our seats of government!) and of course, when this law is translated into computer systems with _no_ safe guards the situation Robyn has described can happen easily.

C. Meo

---

guilty until proven innocent

<ark@research.att.com>
Thu, 14 Feb 91 16:46:32 EST

C. Meo says he `does not know of any other civilised country' that would allow the burden of proof to be reversed in the event of traffic violations. Unfortunately, that is becoming more common here as well -- several states have empowered police to seize licenses of people tho fail breath alcohol tests. It then becomes the problem of the accursed -- um, accused, to prove innocence. Yeah, right.

I know a guy who was stopped for speeding once. They looked him up and discovered his license had been revoked, so they carted him off to the police

station and booked him for driving while on the revoked list. He protested that (a) he had never been informed that his licence had been revoked, and (b) he had not done anything that should have caused his license to be revoked.

When his case came to trial, the state readily admitted that both (a) and (b) above were true. However, his name was indeed on the revoked list, albeit erroneously, and he was accused of driving while his name was on the revoked list, so he should be found guilty. The judge agreed and found him guilty. Afterwards, he asked what he might have done to avoid this. The answer was that it was his responsibility to check the revoked list to see if his name turns up there. He left the state shortly thereafter, and I don't suppose he has been back since.

Parking Ticket Notice

Robert McClenon <76476.337@compuserve.com>
14 Feb 91 00:46:16 EST

I received from the District of Columbia Government Bureau of Traffic Adjudication a Notice of Delinquent Parking Tickets today for three tickets issued in December 1990. The tickets were all issued to a Volkswagen with plate number 457-143 in a section of Washington that I have not visited. I do not own a Volkswagen.

Prior to October 1987 I owned a Ford Fiesta with plate 457- 143. Shortly before October 1987 I lost the front plate. Since I was preparing to trade it in for a new van I did not replace the plate, and did not report it as lost. I simply requested a new plate rather than transferring an old plate. The plate expired in March 1988.

Either the plate number was reissued, or someone found the lost plate and is using it illegally. If it was reissued, the problem is that the database shows the wrong name as the owner. If it was lost and found and is being used illegally, then the system should have shown that the registration is no longer valid. Besides, if that old plate is being used, tickets should also have been issued for using an expired license plate without renewal stickers.

The specific RISK here is: "D.C. motor vehicle registration will not be renewed if you have outstanding parking tickets." The notice doesn't say that it only restricts the renewal of this Volkswagen with plate 457-143. They also have my name, and presumably know that I now own a 1988 van. A more serious risk could arise with a system with this vulnerability in a state where parking tickets are considered to be petty crimes, in that an arrest warrant could be issued. (Parking tickets in the District of Columbia are civil rather than criminal. That reduces the risk but doesn't eliminate it.)

Robert McClenon

Reinterpretation of the term "Computer Security"

Barry Schrager <71370.2466@compuserve.com>

08 Feb 91 23:02:59 EST

Mr Dixon seems to be perturbed that one of the moguls in his business has determined that all data should be protected rather than just "sensitive data." Just who is going to be so totally aware of what the implications of all data are to make an absolutely correct decision so that all company sensitive information will be protected. It is obviously much more secure and definitely safer to assume that all data has some importance and therefore should has some measure of protection. If this is the case then the data creator/owner or security manager can determine who should have access to share this data.

If all data is protected by default then the error of omission is just an inconvenience -- if only "sensitive data" is protected then the error of omission is disclosure of sensitive data and presumably some corporate harm.

The security product I designed for large IBM Computer Systems -- ACF2 -- was the first product in that arena to protect all data by default and it was done with less overhead than the products that presumably protected only sensitive data. Given this, there exists no reason to not protect all data and determine who to share it with rather than guess which data should be protected or not protected. Thousands and thousands of computer sites licensed this package so therefore they also felt that this was the correct way to do this.

The SHARE Security Project Requirements for future data security in IBM Operating Systems also called for all data to be protected as a default in 1974. Obviously, Mr Dixon's business mogel is not alone with his presumptions -- in fact, I think he's right.

COMPUTING & VALUES CONFERENCE, N C C V / 91, Aug 12-16 1991

Walter Maner <maner@bgsuvax.UUCP>
9 Feb 91 17:35:09 GMT

NCCV/91 THE NATIONAL CONFERENCE ON COMPUTING AND VALUES,
AUGUST 12-16, 1991, NEW HAVEN, CONNECTICUT FIRST CALL FOR PARTICIPATION

The National Conference on Computing and Values will address the broad topic of Computing and Values by focusing attention on six specific areas, each with its own working groups.

- Computer Privacy & Confidentiality
- Computer Security & Crime
- Ownership of Software & Intellectual Property
- Equity & Access to Computing Resources
- Teaching Computing & Values
- Policy Issues in the Campus Computing Environment

CONFERENCE HIGHLIGHTS -- Details follow

o Active role for all attendees

- o Free associate membership in the Research Center on Computing and Society
- o Valuable take-home materials
- o A user-friendly conference
- o A family-friendly conference
- o Unique aspects
- o Members of the Planning Committee
- o Partial list of confirmed speakers
- o Modest cost
- o Further information and registration

ACTIVE ROLE FOR ALL ATTENDEES

A special feature of the National Conference on Computing and Values will be the active role of all attendees. Each attendee will belong to a small working group which will "brainstorm" a topic for two mornings, then recommend future research. On the third morning, each group will report the results of its activities to the assembled conference. (Group reports will be incorporated into the published proceedings of the conference.)

In addition, each person will be able to attend five keynote addresses, three track addresses, three track panels, two evening kick-off events, two evening enrichment events, and four days of exhibits and demonstrations.

FREE ASSOCIATE MEMBERSHIP IN THE RESEARCH CENTER ON COMPUTING AND SOCIETY

Every attendee can become an Associate of the Research Center on Computing and Society for two years free of charge. Associates receive the Center newsletter, announcements of Center projects, lower registration fees at Center sponsored events, and access to the Center's research library on computing and values.

VALUABLE TAKE-HOME MATERIALS

The conference will provide a wealth of materials on computing and values, including articles, government documents, flyers about organizations and publications, a special "Resource Directory on Computing and Society," and a "track portfolio" of materials for each of the six tracks. Every attendee will receive a copy of the resource directory, the track portfolios, plus many other useful materials.

A USER-FRIENDLY CONFERENCE

The conference will be held on a residential campus at a quiet time between semesters. Adequate time for meals, conversations, and relaxation is scheduled. There will be social events, such as an ice cream social and a conference barbecue. In addition, various lounges will have coffee, tea, juice, and snacks all day to encourage conversation among participants. The conference will include individuals from six different professional groups: Computer Professionals, Philosophers, Social Scientists, Public Policy Makers, Business Leaders, and Academic Computing Administrators.

A FAMILY-FRIENDLY CONFERENCE

Family members of attendees will be able to use university facilities, such as

the swimming pool, playing fields, tennis courts, and TV lounges. In addition, a day-care center, baby sitting service, and bus trips to local tourist attractions will be available. Attendees' spouses will be welcome at conference social events; and both spouses and children may attend the conference barbecue.

UNIQUE ASPECTS

The National Conference on Computing and Values will be one of most significant assemblies of thinkers on computing and values ever to gather in one place.

Among the nearly 50 speakers who will address the 500 conference attendees are philosophers, computer scientists, lawyers, judges, social scientists, researchers in artificial intelligence, and experts in computer security.

The conference also will feature one of the most comprehensive exhibits of materials ever assembled on computing and values. The exhibit will including books, journals, articles, government documents, films, videos, software, curriculum materials, etc.

Hosted by Southern Connecticut State University, including the Research Center on Computing and Society, Philosophy Department, Computer Science Department, Adaptive Technology Laboratory, and the journal Metaphilosophy.

Planned in cooperation with: The American Association of Philosophy Teachers, the American Philosophical Association, the Association for Computing Machinery, the Canadian Philosophical Association, Computer Professionals for Social Responsibility, and the Institute of Electrical and Electronics Engineers.

Funded, in part, by grants from the National Science Foundation (DIR-8820595 and DIR-9012492).

MEMBERS OF THE PLANNING COMMITTEE

Terrell Ward Bynum, Co-chair, Walter Maner, Co-chair

Ronald E. Anderson, Gary Chapman, Preston Covey, Gerald Engel, Deborah G. Johnson, John Ladd, Marianne LaFrance, Daniel McCracken, Michael McDonald, James H. Moor, Peter Neumann, John Snapper, Eugene Spafford, Richard A. Wright

PARTIAL LIST OF CONFIRMED SPEAKERS

Ronald E. Anderson, Chair, A C M Special Interest Group on Computing and Society; Co-Editor, SOCIAL SCIENCE COMPUTER REVIEW

Daniel Appelman, Lawyer for the USENIX Association, Specialist in Computer and Telecommunications Law

Leslie Burkholder, Staff Member of the Center for the Design of Educational Computing, Carnegie-Mellon University; Editor, COMPUTERS AND PHILOSOPHY

David Carey, Author and Speaker on Software Ownership; Doctoral Dissertation on Software Ownership; Assistant Professor, Whitman College, WA

Gary Chapman, Executive Director, Computer Professionals for Social Responsibility; Editor, JOURNAL OF COMPUTING AND SOCIETY

Marvin Croy, Author and Researcher on Ethical Issues in Academic Computing; Associate Professor of Philosophy, University of North Carolina at Charlotte

Gerald Engel, Vice-President of Education, Computer Society of the I E E E; Member, Computing Sciences Accreditation Board; Editor, COMPUTER SCIENCE EDUCATION

Batya Friedman, Co-Editor of Computer Professionals for Social Responsibility Anthology of Computer Ethics Syllabi; Teacher of Computer Ethics at Mills College, CA

Don Gotterbarn, Researcher and Speaker on Computer Ethics; Associate Professor of Computer and Information Sciences, East Tennessee State University

Barbara Heinisch, Co-Director, Adaptive Technology Computer Laboratory, Southern Connecticut State University; Associate Professor of Special Education

Deborah G. Johnson, Chair, Committee on Computers and Philosophy of the American Philosophical Association; Author of the textbook COMPUTER ETHICS

John Ladd, Professor Emeritus of Philosophy, Brown University; Author of articles on Ethics and Technology

Marianne LaFrance, Project Director, "Expert Systems: Social Values and Ethical Issues Posed by Advanced Computer Technology"; Associate Professor of Psychology, Boston College

Doris Lidtke, Editorial Staff, Communications of the A C M; Professor of Computer and Information Sciences, Towson State University

Walter Maner, Director of the Artificial Intelligence Project, Bowling Green State University; Author of Articles on Computer Ethics

Dianne Martin, Researcher and Curriculum Developer in Computers and Society; Co-Chair of "Computers and the Quality of Life 1990", A C M / S I G C A S conference

Keith Miller, Computer Science, the College of William and Mary; Author and Speaker on Integrating Values into the Computer Science Curriculum

James H. Moor, Member, Subcommittee on Computer Technology and Ethics, American Philosophical Association, Author of Articles on Computer Ethics

William Hugh Murray, Consultant and Management Trainer in Information Systems Security; Past Fellow on Information Security with Ernst & Young Accountants

Peter Neumann, Senior Researcher in Computer Science, S R I International; Chair, A C M Committee on Computers and Public Police; Editor, Software Engineering Notes; Moderator of COMP.RISKS

George Nicholson, Judge of the California Superior Court, Head of the "Courthouse of the Future" Project

Judith Perolle, Researcher on "Ethical Reasoning about Computers and Society"; Associate Professor of Sociology, Northeastern University

John Snapper, Illinois Institute of Technology; Author and Editor in COMPUTER ETHICS; Member of the Center for the Study of Ethics and the Professions

Eugene Spafford, Member A C M - I E E E Joint Task Force on Computer Science Curriculum; Author of Articles and Reports on Computer Viruses and Security

Willis Ware, Researcher, Author and Speaker on Computers and Privacy

Terry Winograd, Past President of Computer Professionals for Social Responsibility; Author and Researcher in Artificial Intelligence

Richard A. Wright, Executive Director, American Association of Philosophy Teachers; Director, Biomedical and Healthcare Ethics Program, University of Oklahoma

Bryant York, Professor of Computer Science, Boston University; Director of the Programming by Ear Project for visually handicapped individuals

MODEST COST

Registration Fee

	Before 7/1/91	After 7/1/91
regular	$175.00	$225.00
student	$ 50.00	$100.00

Food (entire conference)
$90.00 (adult) $50.00 (child)

Dormitory Room (entire conference)

	Before 7/1/91	After 7/1/91
adult (double occupancy)	$100.00	$110.00
adult (single occupancy)	$150.00	$175.00
child	$40.00	$50.00

There are a limited number of single occupancy rooms available.
A few Room & Board Scholarships are available.

FURTHER INFORMATION AND REGISTRATION

Registration for the National Conference on Computing and Values is limited to 500 people (about 85 from each professional group). It is highly recommended that you pre-register well in advance to ensure a place in the conference. To receive a set of registration materials, please supply the requested information (see "coupon" below) to Professor Walter Maner, the conference co-chair:

By E-Mail:
BITNet MANER@BGSUOPIE.BITNET
InterNet maner@andy.bgsu.edu (129.1.1.2)
CompuServe [73157,247]
By Fax:
(419) 372-8061
By Phone:
(419) 372-8719 (answering machine)
(419) 372-2337 (secretary)
By Regular Mail:
Professor Walter Maner
Dept. of Computer Science
Bowling Green State University
Bowling Green, OH 43403 USA

/---------- COUPON ----------\
First Name:
Last Name:
Job Title:
Phone:
Institution or Company:
Department:
Building:
Street Address:

City:
State:
Zip:
Country:
Email Address(s):

All attendees will be part of a working group that "brainstorms" a topic and suggests further research for the next five years. PLEASE INDICATE YOUR PREFERENCES BELOW (1 = first choice, 2 = second choice, 3 = third choice):

[ ] Privacy & Confidentiality
[ ] Equity & Access
[ ] Ownership & Intellectual Property
[ ] Security & Crime
[ ] Teaching Computing & Values
[ ] Campus Computing Policies

PLEASE MARK *ONE* OF THE FOLLOWING:

[ ] Send me registration information ONLY. I'll decide later whether or not to register.

[ ] Register me NOW. Enclosed is my check (made payable to "B G S U") for $ to cover all of the following (PLEASE ITEMIZE):

Quantity
[ ] regular registration(s)
[ ] student registration(s)
[ ] meal ticket(s) for adult
[ ] meal ticket(s) for child
[ ] room(s) for adult (double occupancy)
[ ] room(s) for adult (single occupancy)
[ ] room(s) for child

Note that rates change on July 1, 1991.

\---------- END OF COUPON ----------/

InterNet maner@andy.bgsu.edu (129.1.1.2) | BGSU, Comp Science Dept
UUCP ... ! osu-cis ! bgsuvax ! maner | Bowling Green, OH 43403
BITNet MANER@BGSUOPIE | 419/372-2337 Secretary
Relays @relay.cs.net, @nsfnet-relay.ac.uk | FAX is available - call

Search RISKS using swish-e

THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

ACM Committee on Computers and Public Policy, Peter G. Neumann, moderator

Volume 11: Issue 11

Friday 15 February 1991

Contents

Re: Enterprising Vending Machines (Risks 11.03)

Jeff Johnson <jjohnson@hpljaj.hpl.hp.com>
Mon, 11 Feb 91 15:26:14 PST

Just had my own run-in with a postal vending machine. Was expecting trouble because of what I'd read in RISKS, but got bitten anyway. If not interested in the details, skip to Summary.

Entered a post office to buy some new stamps. Long line waiting. Vending machines (3) all flashing the "Use exact change" light. Line backed up into narrow hallway containing both vending machines and post boxes. Hallway very crowded; people angry because they must wait in line or because they can't get through the crowd to their post box. Several people standing in front of the

vending machines, trying to figure out how to coerce stamps from them, adding to the crowd. Purchase-pooling deals being suggested, mentally tested ("Let's see, if I buy two books of stamps and you get 1 book of post-card stamps..."), and tried.

One machine offered ten 29-cent stamps for $2.90, but wanted exact change. I had 3 ones and a twenty. I decided to put in $3, get ten stamps, and forget about the extra dime. Put in first dollar: amount-display showed $1.00. Tried to put second bill in, but machine rejected it repeatedly. Ditto other bill. Pressed "change return" to get first dollar back. Machine made four "ka-chunk" noises, but no money actually appeared. The amount-display now read $0.00, but I didn't notice this at the time. I put in the other 2 bills (this time the machine accepted them); now the display said $2.00. Hadn't notice that it had gone to zero, so wondered where my other dollar had gone. Figured that it must have timed me out as reported in RISKS. Had no more one-dollar bills, so was stuck. Pressed "change return" in frustration: eight "ka-chunks" but no money. Noticed amount decreasing $.25 for each "ka-chunk" this time, so figured out what happened to first dollar.

Asked to see station manager. Told him what happened. He didn't understand. Invited him out into lobby to put bills into machine. He did. Told him to press "change return". He didn't want to: didn't want to lose his money. I said, "You've already lost your money since there's no way to get it back; you might as well press 'change return' so you can see what happens." He did, heard the "ka-chunks", then said: "This machine is out of order; I need to put a sign on it". I said, "It's out of order, but not because it's malfunctioning; this is what it is designed to do when out of change." He didn't think so.

I also tried to explain to him that new stamp price *means* that vending machines must be refilled with change much more often. By now he was beginning to feel some of the stress and exasperation that filled the hallway. He said, "The guy who services these machines isn't here today," gave me my money back, and put an "Out of Service" sign on the machine. This ended the interaction, because now several other people who had been having trouble with the machines pounced upon him.

Summary: The new stamp-price ($.29) has side-effects that clearly were not anticipated by the Postal Service. The new price was calculated to increase revenue to cover operating costs, but some of its ramifications weren't anticipated. One is that the vending machines will be dispensing much more change and therefore must be re-filled more frequently if they are to serve their purpose. The change-making apparatus also will require more frequent repair. This increased servicing of machines will consume some of the expected revenue gain. Second, increased demand for change from the machines has increased user-exposure to various design flaws in the change-making functionality of the machines. The Postal Service should either keep the machines full of change or change the stamp-price to $.30. Simply fixing the machines to behave "correctly" when out of money won't solve the real problem: long lines in post offices.

Jeff Johnson, HP Labs

<jerbil@cobalt.cco.caltech.edu>
Fri, 8 Feb 91 10:26:55 PST

In comp.risks you (Brian Yamauchi <yamauchi@cs.rochester.edu>) write:

>I'm in favor of replacing the various pieces of paper and bits of metal we
>currently use for money with a more convenient electronic system, but I think
>this should and will be done via the free market rather than as mandated by the
>central government.

Agreed. This is what the growing trend for payroll electronic automatic deposit, and Social Security "direct deposit", are all about. Agreed, that for payments over $20 a credit card is handy. But I'd rather have the option, thanks, to handle my finances more flexibly.

My big disagreement with you comes with the transfer scenario -- if that's the only method of transfer. Checks of many sorts handle the large transfers, as do wire transfers, and cash handles the small stuff.

Want to absolutely ruin a cashless society? Turn off the power to the clearinghouses. I wonder how commerce fared during the New York black-out of several years ago, when no one had power. Shopkeepers which didn't have to depend on credit-card sales didn't see the same dip in sales for the month that the others would, I'd wager....

>I'm not extremely enthusiastic about giving the government too much
>information. It is true that they could abuse this. On the other hand, the
>real solution is to enact pro-freedom measures legislatively to limit the
>government's power. If either (1) the government ceases to become democratic,
>or (2) the majority wants to allow government oppression, then there's not a
>lot you can do -- short of armed rebellion -- the tanks can always roll through
>the streets.

If the government ceases to be democratic, or the majority wants government oppressions, then those will be fought by citizens who do not want to see the US Constitution circumvented. The Constitution came out of the efforts of citizens trying to weld together thirteen States in a failing Confederation after a bloody armed rebellion. The tanks can roll through the streets, but unless there's valid authority behind it, it's unconstitutional. The bystanders might be just as dead, but the following reactions would bring the balance back.

>Electronic cash would have both positive and negative effects on crime. On the
>positive side, violent crimes would drop substantially -- no longer would you
>have to worry about being knifed for your wallet in a dark alley. On the
>negative side, the potential for computer crime would be increased. At least
>in theory, this could create the potential for truly huge sums of money to be
>stolen, not by stealing large chunks, but by stealing minute amounts from large
>numbers. For example, stealing 1 cent from every transaction made in the U.S.
>would probably result in a take in the $million/day range.

Depends on the method of 'cashlessness'. If the cards are truly personal, stealing them would be a better method of tying him up than beating

himn into hospital. If not personal, then anyone wishing more money would simply mug for the cards, just as they currently mug for coins and paper and cards. (I thought most muggings were non-violent.)

Several cases have already meandered though RISKS' attention about computer money-skimming schemes at banks, including the 'take the round-off balance account and assign it to me' scam. And the 1-cent per transaction fraud would be noticed somewhere, since it's simply a variation of how banks get paid for their services.

>Still, given a choice, I would rather have some hacker breaking into
>my checking account than some mugger slitting my throat...

I'd rather have the mugger. Most of them don't go for the strong, the active, or those who look like they know what they're doing. The others tend to be caught not long after. With hackers, no one could be the wiser, it's not clear what laws are applicable and to what extent, and the damage potential is orders of magnitude higher.

Joseph Beckenbach

Re: Electronic cash completely replacing cash

Joseph R. Beckenbach <jerbil@cobalt.cco.caltech.edu>
Fri, 8 Feb 91 10:40:39 PST

In RISKS-11.06 Richard A. O'Keefe writes regarding David Witt in RISKS-10.81:

>Eh? These machines are going to be *at least* as expensive as VCRs, and we're
>talking about distributing > 500 million of them (ALL homes and businesses,
>remember, and businesses will need as many of these gadgets as they have cash
>registers). Then think about maintenance.

Let's see, that's running $150.00 x 200 x 10^6 as a low estimate. $30 G-bucks. That's over 1% of the current deficit. GACK!

<> The Federal Reserve would be better able to follow the economy, helping
<> to stabilize the financial markets.

It ain't broke, don't fix it. At least, that part ain't broke.

>Here we have someone who does not believe in the Free Market, and has
>a wonderful child-like faith that because there is an outfit whose task
>is to manage the economy that it is able to do it. I have a bridge for him.

See below....

>The thing that is really evil about the suggestion is that it is a
>technological fix to a social problem; the basic attitude is that
>human "misbehaviour" is best cured by making people behave like good
>little cogs. "Forget trying to build a humane society so that fewer
>people *want* to buy drugs, let's build electronic cages so they're
>found out." How do we educate people like this?

I think it's as simple as saying "Eastern Bloc during the Cold War". Reasonable minds can, and _should_, take it from there.

Joseph Beckenbach

RE: cashless society, a post-mortem

<34AEJ7D@CMUVM.BITNET>
Mon, 11 Feb 91 09:35:36 EST

Two points militate more strongly against this scheme than any others I can think of:

1. The "barter" economy is already well-entrenched in the underground economy. This proposal would immeasurably swell the ranks of those trading by this method,

2. The "hand print and retina pattern" scanners would, I am rather certain, run afoul of the recently-enacted ADA (Americans with Disabilities Act) as illegally discriminatory. There are, boys and girls, people in the good ol' US of A with neither hands nor eyes who are nevertheless productive citizens.

Re: Electronic cash (post dated cheques)

M P Evans <evansmp@uhura.aston.ac.uk>
Mon, 11 Feb 91 19:17:11 GMT

With referance to Frank Wales article (RISKS-11.06) Post dated cheques (at least in Britain) have no validity. If someone were to write me a cheque with next month's (or next year's) date on it I could immediately present it at my bank, and they would accept it without question. This has happened with a cheque I wrote, which I was able to have returned to me, which clearly shows that the date it was paid it (by to bank's stamp) was before the date which I wrote on the cheque. The only thing which can stop such a cheque being processed is the staff at the bank, they do not check the date. The only information known to the automatic processing system is the cheque number, sort code (bank), account number and the value of the cheque. The first 3 are preprinted on the cheque, the latter typed in at the bank.

Mark Evans, Univ. of Aston in Birmingham, Aston Triangle, Brimingham, England.

Cashless Banking and Privacy

<jake@mars.bony.com>
Mon, 11 Feb 91 21:23:35 EST

[Internally-From: Jake Livni <JAKE@DBCLUA>]

Daniel B Dobkin <dbd@marbury.gba.nyu.edu> describes the ultimate government

surveillance tool:

>Unfortunately, Smith doesn't attribute the source of this story; does
>anyone out there have any clues? Enquiring minds want to know.....

Try the Nova show called "Computers, Spies and Secret Lives" which first aired on PBS on Sept. 27, 1981. Excerpts from the transcripts for that show follow:

> PAUL ARMER
> Several years ago, I was a member of a workshop of computer people [and] law enforcement people who were gathered together and asked to pretend that we were consultants to the Russian Secret Police...given the task of designing for them a system which would keep track of all the Soviet citizens, plus all the foreigners who happened to be within the boundaries of the USSR. After considerable study, the workshop concluded that the best system to build for the KGB, the secret police, was an electronic funds transfer system, for the reason that electronic funds transfer systems not only know what you're buying, but where you are in real time at the time you're making your financial transaction.
>
> NARRATOR
> Some privacy experts acknowledge these threats and consider them beyond existing computer capacities.
>
> [This is followed by a bank vice-president who says that ATM usage produces too much information to sort through with then-current computers, except in a serial manner.]

Jake Livni jake@bony1.bony.com

Cashless gas pumps; alternative to credit card use

Jeff Helgesen <jmh@morgana.pubserv.com>
Fri, 8 Feb 91 14:29:15 -0600

The risks inherent in automated charging to credit cards are easily avoided by use of a system like the one(s) used by phone companies in many European countries; that is, the user purchases a card of a particular denomination via a vending machine [or human vendor, if the stories regarding post office machines put you off]. This card has an mag strip encoded with a value which can be read and written to by the automated pump. The card remains in the machine and decrements the value available until the transaction is completed (either the user stops the pump, or the value of the card is dropped to $0, and the pump shuts off automatically), whereby it is ejected. Used-up cards may then be discarded; cards with value remaining may be kept until the next time the user needs petrol.

Benefits versus credit card system include:

- Difficult system to defraud; only risk to petrol vendor is that a wily consumer will figure out the encoding scheme.

o Validation of identity is no longer required. Too bad if you lose your card, though I'd rather lose one of these than my AmEx.

o Handling costs are reduced, presumably reducing the pump price of gas.

o Big brother is not watching.

Jeff Helgesen jmh@morgana.pubserv.com

Re: A risky gas pump (Grumbine, RISKS-11.03)

Dick Smith <dick@smith.UUCP>
9 Feb 91 06:11:20 GMT

I worked on such a system at a previous employer, and think that the concerns expressed are overdone.

Here are my thoughts on the worries expressed about this auto-approving gas pump:

Is card mine: Well, it's probably checked as well as the typical human attendent checks it... I am surprised when someone looks at the back of mine to verify my signature. I try to remember to thank them for doing it!

Receipt disagrees: Complain to the attendent immediately... (in the US, there WILL be an attendent, if only to shut the pumps off if there is a fire) just as you would if the receipt that you got inside was wrong. It's a requirement that the amount pumped stay displayed on the pump until the next person uses it, so you'll have something to compare against if you hurry.

It remembers my card number: Again, I don't know why this is any more likely than the human attendent copying down your number and reusing it. Certainly not on purpose, anyway. When I worked in this industry, I recall that the credit card network had its own validation organization which served as an independent check for credit equipment vendors. I remember their testing as being fairly comprehensive, followed by a month long beta test at a single site with the paper logs checked. We felt pretty good when we got through with it.

The receipt printer doesn't work: Well, the cutter kept jamming in ours... you'll have to go inside in that case, and get the guy to write one by hand. He can copy the info off the paper tape log.

Actually, I worried more when I used a gas pump of a kind that wouldn't be allowed in the U.S. (because of that fire law). I was in Holland last fall, and had occasion to buy gas on the AutoRoute late one night. The station I pulled into has no attendent, just a bill reader for (I

think) 20 & 50 guilder bills. What I worried about was what I was going to do if I put in too much money, since there was no change return at all. I managed to buy 2/3 of a tank for my rental car, though, with no trouble.

Dick Smith, R.H.E Smith Corp ...ast!smith!dick dick%smith@ast.dsd.northrop.com

---

Re: risky gas pumps (Clark, RISKS-11.05)

Lars-Henrik Eriksson <lhe@sics.se>
Sat, 9 Feb 91 15:34:40 GMT

I've been buying gas from automatic gas pumps (both manned and unmanned) in Sweden for several years. I have not yet had a single case of incorrect charging or any other problem that is worse than not getting gas out of the machine.

However, at about 20% of all occations I use these machines, I do *not* get a reciept. Usually because the machines are out of paper.

Lars-Henrik Eriksson Internet: lhe@sics.se
Swedish Institute of Computer Science Phone (intn'l): +46 8 752 15 09
Box 1263 Telefon (nat'l): 08 - 752 15 09
S-164 28 KISTA, SWEDEN

Re: A risky gas pump

K. M. Sandberg <sandberg@ipla01.hac.com>
11 Feb 91 18:08:23 GMT

(Re: Lehman, RISKS-11.05)

> None. But my other credit card purchases are not usually validated
>either. I think the fair credit acts protect you somewhat.

The difference is that with regular credit card transactions you have to sign the slip, with ATM transactions you have to enter a pin code, either of which indicates that you are the owner of the card or in the case of the signature, you can show it is not your signature, with the readers there is no such protection, but one question I have is what happens if you dispute a charge. Since they have no proof of who charged it, except an electronic card number.

Normally a lot of the disputes can be resolved by looking at the signed charge slip, in this case there is none, nor was there any pin code entered as an electronic psuedo-signature, so is there really an agreement?

(Re Margolin, RISKS-11.03)

>From: barmar@think.UUCP (Barry Margolin)
>Subject: Re: A risky gas pump (from RISKS DIGEST 11.03)
>

>Your tone suggests that this is a new risk. ...

This is a new risk, allowing the use of a credit card with no trace back on who used the card, no signature to forge, no pin code to break, nothing. There is no license plate recorded or anything else. You could take a valid charge and say that it was not valid, how do they prove it was? They take a charge that is invalid, how do you prove it was not? Normally you can request the charge slip and so it can be shown that it was not your signature, but in this case anyone who has access to the card can use it. If someone borrowed your card, you at least stand a chance of detecting who it was based on the signature.

As far as the phone credit calls, there is a record of the phone numbers and where the call was placed from, along with a history which can be checked to see if you ever called that number before, so it is quite different.

With mail order house they are supposed to have your signature on file and if they don't you can dispute the charge, but in any case they have a record of where the stuff was sent, and a way to track the person because of that.

I used such gas pumps, but I also write down all the information in a book to watch the gas mileage, so if there was a problem I could show that the gas was not put into one of my cars, unless I forged other entries. Personally I think the gas stations are taking a large risk unless they have something to track the cards better than it appears (ie. some information to ensure that the card number really belongs to the person, like the name. ATM cards have this information). Also if the card is lost or stolen it is generally the case that the person could not keep reusing the car because a person might notice and might also recognize them. In this case the card holder is not seen. Maybe there is a check to make sure that the card is not used too many times, I don't know. What I do know is that if your card is lost and returned, you better be very careful in knowing what you had charged to make sure that a charge was not made before it was returned.

Kemasa.

Re: Burned by a gas pump (was Re: A risky gas pump, RISKS-11.05)

Sean Malloy <malloy@nprdc.navy.mil>
Mon, 11 Feb 1991 13:12:21 PST

> How about if my number is not cleared from the pump's memory and I get
> billed for the entire day's gas from that pump?

Your number can be cleared from the pump's memory and still try to take you, as long as the programmers for the billing software don't pay attention to wierd-case transactions.

Some months ago, I received a bank statement showing that I'd been billed twice for the same transaction at an ARCO PayPoint gas station using my ATM card. The circumstances were that I was returning home _late_ at night, and had stopped to fill my tank. Between the time I'd opened the transaction and shut off the pump after filling my tank, the time had rolled across midnight to the next day. The billing software ARCO was using billed me for each end of the

transaction, since there was a transaction start record for an amount of $9.56 on day X, and a transaction end record for an amount of $9.56 on day Z+1.

The reason I noticed the error was that there were two transactions listed on consecutive days with the same transaction number and amount. When I called the customer service number for my bank and talked to the representative, they said that they'd take the duplicate charge off my account and inform ARCO of the problem; I got the notification of the credit to my account about a week later. Since then, when I've had to fill my tank close to midnight, I always wait for the date to change if there's a chance that it would roll over while I was pumping gas.

Sean Malloy, Navy Personnel Research & Development Center, San Diego, CA 92152-6800 malloy@nprdc.navy.mil

---

Risky gas pumps

Peter da Silva <peter@taronga.hackercorp.com>
Fri, 8 Feb 1991 14:01:30 GMT

These pumps appeared a couple of years ago here in Houston, then most of them promptly vanished. Why? Simple... people buying gas this way didn't tend to make impulse purchases of the overpriced soft drinks, candy, motor oil, and other things they pile up around the regular payment window and revenue actually went down.

The risks aren't just one-way.

(peter@taronga.uucp.ferranti.com)

---

gasoline

<34AEJ7D@CMUVM.BITNET>
Fri, 08 Feb 91 08:31:26 EST

Guy Sherr writes:

>Gasoline is a volatile high explosive.

Wrong. Gasoline is incapable of true "detonation", as required by the definition of a "high" explosive.

Re: Electronic telephone directory

<rmoonen@hvlpa.att.com>
Fri, 8 Feb 91 09:18 MET

MFMISTAL@HMARL5.BITNET (Jan Talmon) writes:

->In the Netherlands, printed telephone directories provide telephone numbers

->by using the name as an index. Currently, there is also an electronic
->version of those directories available by means of a VIDITEL service.
->Here it is also possible to ask for a telephone number by providing the
->street name, the house number and the city. This involves an inherent risk.
->When one observes that there are apparently no people in a house, one can
->ask for the phone number, dial that number and when no one replies....
->it may be safe for burglars to go in.

So what's the big deal here? The Dutch PTT has a directory assistance number (dial 008) that gives exactly the same service, but cheaper. And it's a voice number, so it's probably faster too. The computer number is only good when wanting to look up a lot of numbers, as directory assistance only gives you two informations per call. Another thing that the computer service does, but the voice number not, is give you the name & address, when you supply only the telephone number. I don't consider this a COMPUTER risk as:
1) the service was available all along, only voice.
2) Unlisted number are not in the computer
3) Burglars don't tend to pre-select their victim, but rather go out to a 'nice' neighbourhood, and find a suitable house there and then.
4) Burglars don't tend to have computers & modems unless they stole it from a previous victim :-)

->It seems also to be an invasion of one's privacy, since one need not to
->know a name in order to place haressing/obscene phone calls.

No. I definetely disagree with this statement. One NEVER needs to know a name in order to find the telephone number. If this was an invasion of ones privacy, then get your name-tag off your frontdoor too! Furthermore, if you don't want _any_ unsollicited phonecalls, just change your number to an unlisted one. This costs nothing if you do it at the initial request for a telephone line, and it costs F35.00 ($20.00) if you want it changed to an unlisted number later. (BTW: I live in The Netherlands too, and have an unlisted number)

--Ralph Moonen --rmoonen@hvlpa.att.com

Search RISKS using swish-e

THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

ACM Committee on Computers and Public Policy, Peter G. Neumann, moderator

Volume 11: Issue 12

Sunday 17 February 1991

Contents

Re: PWR system "abandoned..." [Darlington nuclear plant]

<Richard.P.Taylor@nve.crl.aecl.ca>
Fri, 15 Feb 91 12:16:49 EST

Some of the details of the situation regarding the Darlington nuclear power plant's computerized shutdown systems referred to in the Nucleonics Week article quoted by M. Thomas (RISKS 11.08) are given in a previous Nucleonics Week article of May 24, 1990. I will try to summarize that article and include some further details from the Atomic Energy Control Board's (AECB) review process and licensing decision.

That article correctly indicates that the problems with these shutdown systems were that the software is difficult to verify and difficult to modify. These difficulties caused both delays and extra cost. The article also mentions briefly that the software "will have to be rewritten because it is not designed so changes can be easily incorporated." This requirement was placed on Ontario Hydro by the AECB as part of the licensing decision. To quote that AECB licence: "The Board ... has concluded that the existing shutdown system

software, while acceptable for the present, is unsuitable in the longer term, and that it should be redesigned. Before redesign is undertaken, however, an appropriate standard must be defined."

What led to this conclusion was an extensive and thorough analysis of the software. The original software submitted by Ontario Hydro for AECB review was obviously very complex and convoluted. The introduction of digital computers had been taken as an opportunity to add additional complexity and new monitoring functions to the shutdown systems over and above previous analog and hybrid systems. The AECB was concerned about how such software could be reviewed and demonstrated to be safe. Dave Parnas was contracted to advise the AECB, and Nancy Leveson was contracted to advise Ontario Hydro. Nancy Leveson's advice resulted in a hazard analysis by Ontario Hydro and some revisions to the code for better fault detection and safety. The review method eventually chosen by the AECB was strongly based on Dave Parnas' work and involved rewriting the software requirements in "A-7 style" event and condition tables, deriving similar format "program-function tables" from the source code, and comparing the two sets of tables.

It should be pointed out that the software was not designed with such a verification process in mind. When Ontario Hydro safety analysts and AECB reviewers (myself included) tried to verify this software, we encountered many problems simply because the designers and programmers had not expected to have their work verified by mathematical techniques. Nor could they have; the decision to do such a verification was made after the software was designed and coded. Nevertheless, the techniques were successfully applied to the software for the two shutdown systems. Since automated tools were not available, most of the work had to by done manually, and to compensate for human error, all verifications were independently reviewed. The AECB's audit of this process constituted a second independent review of the most critical 30-40% of the software.

Despite the difficulties, the AECB did eventually license the Darlington reactor. The NW article of May 24 quotes Zygmond Domaratzki of the AECB: "At the end of the long tedious process we went through to review the software....(W)e don't have any reservations about its ability to shut down the reactor in an emergency." The other result of this process was considerable assurance that the software would not perform any unintended, unsafe actions. Every part of the code was analyzed, some unintended actions were discovered, but all actions were determined to be safe.

The current situation is that Ontario Hydro and Atomic Energy Canada Limited (AECL) are developing methods for specifying, designing and verifying safety critical software. These methods will be applied to the development and verification of some prototype systems before they are adopted for general use, and for the redesign of the Darlington shutdown systems. The goal of these methods is to make software easier to modify and easier to verify and review. The AECB is monitoring this process closely.

The AECB also is working (with the help of Dave Parnas and Wolfgang Ehrenberger of GRS in Germany) to develop Canadian standards for safety critical software in nuclear power plants. We are monitoring international developments in this area to ensure that Canadian standards are on par with the rest of the world.

A separate, but related issue is to find a method of predicting the reliability of the software. I hope to join that RISKS discussion again shortly.

Richard P. Taylor, AECB, Canada taylorrp@nve.crl.aecl.ca

*I have tried to be brief and informative rather than simply quoting published material. Any misquotes or additional material are strictly my own interpretation and should not be taken as the position of the AECB. All the usual disclaimers apply. Please also note that the AECB is distinct and separate from AECL even though I get my e-mail via an AECL address.

Re: PWR system "abandoned..."

Nancy Leveson <nancy@murphy.ICS.UCI.EDU>
Sun, 17 Feb 91 16:00:18 -0800

> According to the report, "Ontario Hydro faced a similar situation at its
> Darlington station, in which proving the safety effectiveness of a
> sophisticated computerized shutdown system delayed startup of the first
> unit through much of 1989. Last year, faced with regulatory complaints
> that the software was too difficult to adapt to operating changes, Hydro
> decided to replace it altogether". [I hope that Dave Parnas or Nancy
> Leveson can fill in the details here.]

This is not exactly the situation as I understand it. Although I have not been directly involved for a while, I do have contact with people at Ontario Hydro.

It is true that granting of a low-power testing license for the reactor was delayed due to questions about how to certify the software. Both Dave and I were consulting on this -- Dave for the Atomic Energy Control Board (the government agency) and me for Ontario Hydro. Dave and I disagreed about what OH had to do to ensure the safety of the shutdown software, and they ended up having to satisfy both of us.

Very briefly, my major requirements were that the software be subjected to a hazard analysis, including a software fault tree analysis. A few other minor suggestions involved such things as rewriting the code slightly so that it was easier to read and review.

A paper on the results of the software hazard analysis (using Software Fault Tree Analysis) was just presented at the PSAM (Probabilistic Safety Assessment and Management) Conference in L.A. two weeks ago. The Software Fault Tree Analysis took 2 man months. There were no "errors" found, but they did make 42 changes to the code as a result of what they learned by doing it (e.g., changed the order of some statements to make it more naturally fault tolerant and added assertions to detect hazardous states at various points in the code). They reported to me (and in the PSAM presentation) that they liked the software fault tree analysis technique, have used it on some other control system software, and are planning to use it again in the future. A little more about this can be found in my current CACM paper on how to build safety-critical software.

Dave required that they rewrite their requirements specification in the A-7 style and that they do a "handproof" of the code using functional abstraction from the code (called Program Function (PF) Tables). This was quite costly and painful in comparison with the fault tree analysis (at PSAM I was told that the PF tables took 30 man years), but it is also more complete. I heard that a few errors were found in the specification (not in the code) as a result -- but this may not be correct. I have also heard from several people at Ontario Hydro that they are not happy with the prospect of having to repeat the PF analysis when changes are made in the code (which the AECB has decreed), and some have suggested getting rid of the software altogether to avoid having to go through this type of PF table analysis again.

nancy

More on very reliable systems

Jerry Leichter <leichter@lrw.com>
Fri, 15 Feb 91 11:46:08 EDT

Dr. Tanner Andrews writes:

>) The theory here is that running 100 units for 100 hours gives you
>) the same information as running one unit for 10000 hours.
> The theory is crocked. It builds heat slowly. The actual behavior:
> 100 hours: a little warm
> 200 hours: case is softening
> 250 hours: case melts
> 257 hours: catches fire
> The times and failure modes will vary, depending on the type of device in question.

He's just re-discovered the problem of correlated failures, which was what my whole article was about. I gave a very similar example concerning digital watches.

Martyn Thomas asks:

> How can we have confidence that the means by which we have combined the n-versions [of an n-version program] (for example, the voting logic) has a failure probability below 1 in 10^9?

Clearly, we can't. If your view of an n-version program is that it just produces some numbers that you somehow combine to get some other number, you've got a problem. But the real issue is how you build reliable systems that somehow affect the real world.

Consider the brake system in an automobile. It is divided into independent halves from the master cylinder on; the halves control diagonally opposite pairs of wheels. Either half can stop the car, and failures that affect both are "unlikely". Now suppose we wished to build a computer-controlled brake. We might try to get reliable operation by having redundant computers and a voter which then applied all four brakes. But it would make much more sense to have a pair of independent computers controlling diagonally opposite pairs

of wheels. The "voter" is then the car itself, and physical laws guarantee that if either vote says "stop", the car stops. (This actually comes full circle to a comment I made a number of months back about the significance of physical laws in mechanical systems, and the lack of such "enforced by the universe" laws in digital systems.)

This is a HARD problem, there's no denying that!

> How can we be sure that our analysis of the upper bound on failure correlation among modules is accurate? How accurate does it need to be - does it need to have a probability of less than 1 in 10^9 that it is grossly wrong? (By "grossly wrong" I mean wrong enough to invalidate the calculation that the overall system meets the "1 in 10^9" figure). This would seem impossible. Consider, for example, the probability that the common specification is wrong.

We can never be SURE. Try and come up with any analysis that makes you SURE (with high probability) that your car will stop when you hit the brakes - or, for that matter, that the sun will rise tomorrow. The language of mathematics is very misleading here: Mathematics deals with models of the world, not the world itself. There is no certainty, even of probabilistic estimates, in the world. But we have to muddle on.

I'm not knowledgeable enough in statistical theory to comment on how one even measures the correlation, much less what the appropriate tests and sample sizes are. On the other hand, fairly small experiments showed the FAILURE of the independence hypothesis for naive n-version programming.

Also, it's worth commenting on an assumption about testing that many people make implicitly: That only tests that do NOT use special knowledge about the system being tested are acceptable. In fact, hardly anything is ever tested that way - it's just not practical. It requires too many tests and takes too long, often longer than the useful lifetime of the object under test.

Consider, for example, computing MTBF for disks. People ask how a manufacturer can come up with an estimate of 100,000 hours on a fairly new product. The answer is two-fold: For failures that occur essentially at random during the lifetime of a disk, testing a number of disks in parallel gives you a valid estimate. For failures related to aging - i.e., those whose probability goes up as time in service goes up - there are a variety of "accelerated aging" techniques. Almost anything that's the result of a chemical reaction (e.g., deterioration of lubricants) will proceed faster if you run the device at higher temperatures. Similarly, Dr. Andrews's slow heating will occur much faster in a higher temperature environment. Many kinds of mechanical failures are due to CHANGE in temperature; a common test environment cycles the temperature repeatedly. Similar considerations apply to humidity. Vibration stresses can be easily applied. Someone asked about bearing failure after many thousands of hours. It may take a bearing thousands of hours to fail, but the failure process doesn't suddenly happen - subtle changes are going on in the bearing and the lubricants over that period of time. A close examination - much more than a "yes, it's still turning" determination - will find chemical and physical changes: Breakdown of the lubricant, migration of metal into the lubricant (whether in macroscopic (chips of metal) or micro-

scopic (disolved metal) quantities), scoring of the bearing races, changes in metal crystal structure. We have a huge amount of experience with these kinds of systems, and know what their plausible failure modes are. Are we always right? No, of course not - but again, we have to muddle through.

Paul Ammann writes:

> 1. Testing (whether by explicit test in a lab or by actual
> use in the field) of very large numbers of copies of
> the system
> 2. Functional decomposition of the system into a number of
> modules such that failure can occur only when ALL the
> modules fail.

> The first technique assesses performance directly, and can be applied to any system, regardless of its construction. As Jerry points out, various assumptions must be made about the environment in which the testing takes place. The second technique estimates performance from a predictive model....
>
> I am uncomfortable with merging the issues of direct measurement with those of indirect estimation. The difficulties in 1 are primarily system issues; details of the various components are by and large irrelevant. In technique 2 the major issue is the failure relationship between components.

I don't believe the distinction is sharp. Again, most type 1 testing is NOT a naive "try it for a while and see what happens"; one designs tests based on assumptions about plausible failure modes. This is, in effect, a predictive model: We predict that we've isolated all the important contributors to system failure. If we're careful, we even TEST that prediction: After all our tests are complete, we check to see how many failures were the results of causes we did not include in designing our tests. If there are too many, we may have to go back and do it again.

Conversely, we can simply build the system from what we think are independent modules and then do brute force testing for overall reliability.

> The Eckhardt and Lee model (TSE Dec 1985) makes it clear that performance prediction is much more difficult. To evaluate a particular type of system, one must know what fraction of the components are expected to fail over the entire distribution of inputs. The exact data is, from a practical point of view, impossible to collect. Unfortunately, minor variations in the data result in radically different estimates of performance. For a specific system, it is not clear (to me, anyway) what an appropriate "upper bound of failure correlation among modules" would be, let alone how one would obtain it.

See my earlier comments. I don't believe there is any magic solution to this problem; just as in the design of physical artifacts, it's something we'll just have to learn about and solve on a case by case basis.

> Either technique can be used to get believable
>failure estimates in the 1 in 10^8 (or even better) range. Such
>estimates are never easy to obtain - but they ARE possible. Rejecting
>them out of hand is as much a risk as accepting them at face value.

This statement came out sounding stronger than I intended. I don't believe we have the capability today to build a computer-based system for which we could believe error estimates of this sort. Nor do I see any techniques available today that could provide such an estimate. However, I don't see any fundamental reason to belive that such techniques could not exist.

BTW, it's also worth considering just how strong such a guarantee is, and in particular how many of the systems we already deal with in the world are much, much riskier. If I remember the numbers right, about 30,000 people die in car accidents every year. If we do some really stupid estimating, and assume that everyone in the US (about 3*10^8 people) gets into a car once a day, then my chance of dying in a car accident is 1 in 10^4 each year. Not a very reliable system, is it?

In fact, I've always found it interesting how much more we demand from digital systems than we demand from mechanical ones. For example, we always reassure beginners that no incorrect input to a program can physically harm the machine. And yet, consider what will happen to your car should you take it down the highway at 60mph and then suddenly shift into reverse. Does this bother you? Does it make you afraid to drive?

-- Jerry

Saudi air controllers

Peter da Silva <peter@taronga.hackercorp.com>
Fri, 15 Feb 1991 13:58:51 GMT

The following message was posted on a local bulletin board.

Msg#:28798 *HOUSTON SHOUTS*
02-14-91 22:23:32 (Read 10 Times)
From: DONALD SAXMAN
To: HELGA
Subj: WRITE YOUR CONGRESSMEN

(This message is really for anyone). It was recently brought to my attention that the Saudi Arabian government has replaced American traffic controlers in the Desert Shield war zone with native Saudis. This was done partly to appease Saudi nationalists and partly because some of the American military air traffic controlers were women. (Saudi and other Islamic military pilots aren't particularly fond of being directed by women, but they can live with it. Saudi civilian pilots reportedly would refuse to even listen to instructions fro female air traffic controlers, pretending they didn't exist). Anyway, the Saudi controlers may or may not be as good at their job as the Americans. But they reportedly don't speak English very well. (Sidebar: English is supposed to be the international air traffic control language, but there are some holdouts that don't follow this standard. Many of these are Islamic countries, although

Saudi Arabia apparently does use English-speakers.) Anyway, UN Coalition forces are already having trouble coordinating operations. Pilots who operate from outside of the war zone, like refuelers or B-52s, are particularly at risk. Anyway, there has been a suggestion made that users write their Congressmen and complain about this situation. It couldn't hurt.

If anyone out there has Usenet or Fidonet access, I'd appreciate them forwarding this message so that it gets as wide exposure as possible.

(peter@taronga.uucp.ferranti.com)

Enterprising Vending Machines

<DONNER@IBM.COM>
Fri, 15 Feb 91 15:16:37 -0500

Grand Central Terminal in New York City has a number of ticket vending machines that permit travellers who don't want to stand in long lines to purchase tickets. I had an unpleasant experience with one of them a while ago. I arrived at the terminal before the 6:00AM opening of the ticket offices with the intention of taking a 6:10AM train. Not knowing that the ticket offices would open at 6 (it's not posted) I went to one of the ticket machines and pressed the code for my destination. It told me to insert $8.60. The signs on the front of the machine informed me that I could use bills of any denomination up to and including $20. Having only $20s on me (bless the cash machine) I inserted one of them. The light at the little window where tickets and change are delivered flashed just as if it was delivering my ticket (I'd used the machine before and I knew what to expect) but nothing came out. My money wasn't returned, I got no ticket, and I got no change. Deciding that putting another $20 into the machine wasn't wise, I wandered around the main concourse looking for someone in authority for a few minutes until the ticket windows opened.

I explained the situation to the ticket agent (after buying a ticket to my destination) and he said "Oh, yes, it does that if you put a 20 in for a purchase less than $10," and gave me a form to fill out requesting a refund. A few weeks later I received a letter from some official of the rail line asserting that they hadn't found any excess $20 bills in their machines and implying that I had been attempting to cheat them out of money. He also asserted that there were instructions on the machine explaining not to use $20 bills when less than $10 worth of tickets was being purchased. I had looked for such indications on the occasion of my loss and not found them, though on my next visit to the station after receiving the letter I found that little signs saying that had, in fact, been glued to the face of the machine in the intervening time.

I wrote another letter suggesting that when the machine detected this problem it could print out a receipt on ticket stock and give it to the user so that he would have documentation for his loss. This letter, which included several other suggestions for simple, inexpensive solutions to the problem, evoked a rather hostile letter in response. At that point I gave up, though I did fantasize about blowing the machine up for several weeks after.

Marc Donner

Visa voided purchase woes

Jane Beckman <jane@wombat.UUCP>
Thu, 14 Feb 91 17:39:41 PST

I had heard that having to have a purchase voided out can tie up credit block allocations for a while, but here's my experience of last Friday that illustrates what can happen when Murphy really gets rolling...

I had a moderately sized chunk of cash I needed to pay for with my VISA card, over at the local Pay 'n Save. Half the staff was out sick and the checkers who were in were overworked. The checker opens a new register and runs my card through. Nothing happens. She finds that the printer for the reader is turned off. She turns it on. Still nothing. So she runs the card through again. This time, everything acts as normal until it goes to print out a register slip for me to sign. The paper on the printer jams.

Much swearing later, she tries to get into the register to void the purchase, and finds that it has billed me TWICE for the amount of purchase, once for when the printer was off, once for when the printer jammed. The register doesn't know how to handle this, and refuses to void the second charge. She has to go find the manager, who manages to consult the reference manual and get the printer voided.

Okay, now that things are finally (theoretically) working, they run my card through again. It comes back declined. Why? The two rather largish sums that were voided are stuck in my credit allocation, of course. Of course it went through, the first two times. I suppose I could have written a check at that point, but I decided to stubborn it out. (Besides, I was interested in finding out what could be done, now.)

The salesgirl calls the VISA number, hoping she can get a manual override. A mechanical voice wants her to punch in the store code. She doesn't have it. She hangs up, goes to another person, gets the store code. She calls again, punches in the store code, then is asked for the credit card number. I'm sorry, says the other end, that credit is declined. Click. She gets the manager. He punches things in, and manages to get a real human being, and tries to explain what's going on to the credit authorization person. That it was okayed the first two times, but now (with two voided charges on the allocation) it's topped my credit limit. I'm sorry, says the credit drone, but I am not authorized to okay that credit authorization, despite what you tell me. That can only be done by the credit card company. Fine, says the manager, do you have a number for Citibank? Call the customer service number on the back of the card, she suggests. He calls the number, and explains to the Citibank service representative what has gone on. The Citibank rep says that if he puts the card through one more time, he can manually override the declined credit order. They put my card through one more time. The credit goes through. I get a slip to sign.

However, you can bet I will be looking at my next bill very carefully. Also, the override was obviously a once-only, and the credit is still set aside, somewhere, as I tried to use my card for a small purchase, this week, and it was declined. That second charge is still in the system, somewhere. Some time, someone is going to have to program the system to accept voids.

--Jane Beckman [jane@swdc.stratus.com]

Credit enquiries appear to expose client lists to competitor's scrutiny

<janson@ATHENA.MIT.EDU>
Thu, 14 Feb 91 18:57:34 EST

I have become sensitive to my exposure due to electronically compiled and disseminated personal data, but, until recently, i had never considered ways in which the users of such data expose themselves to possible losses. I was both amused and disconcerted to learn that a company which uses a credit reference service makes it easier for a competitor to target customers through traces which are maintained by the credit agency.

This last week i received in the mail, from MCI, an offer for a rebate in exchange for electing them as my long distance carrier.
[Ignore for the present discussion ethical issues raised by the particular incentive mechanism which MCI employed.]
I had expected, and did receive, a number of enquiries from various alternative carriers at the time when equal access provisions went into effect in this area. I was, however, perplexed as to why they chose to target me now.

It took a bit of reflection, but i finally concluded that one focus of MCI's current mailing is the holders of ATT Universal cards.
[MCI used an address which gave them away.]
Not really the kind of thing which one company would deliberately give to a competitor. So i called ATT to ask what happened. I was informed that they knew the likely path which the information had traveled, but that once they had made a credit enquiry, they were powerless to preventing MCI from approaching the credit agency and obtaining a list of those people for whom ATT had requested credit histories.

Search RISKS using swish-e

THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

ACM Committee on Computers and Public Policy, Peter G. Neumann, moderator

Volume 11: Issue 13

Tuesday 19 February 1991

Contents

MAD HACKER appeal fails [From Darren Dalcher]

"Peter G. Neumann" <neumann@csl.sri.com>
Tue, 19 Feb 1991 14:15:18 PST

Nicholas Whiteley, 21, of Ascot Gardents, Enfield, UK, was convicted earlier [see RISKS-10.03,09,10,27] on four counts of damaging property, and sentenced to 12 months in jail, 8 of them suspended. A week later he was out on bail, pending appeal. The appeal process was completed on 22 January, and was dismissed. He was reportedly the "first computer hacker in Britain to be jailed". He had "deleted and added files, put on messages and changed

passwords of existing users enabling himself to use the system." [Thanks to Darren Dalcher at King's College, London, for a clipping received this morning from the 6 Feb 91 Enfield Independent, apparently mailed on 6 Feb, although unpostmarked, with a stamp that was uncancelled.]

Paid to know everything about everybody?

Kent M Pitman <KMP@STONY-BROOK.SCRC.Symbolics.COM>
Mon, 18 Feb 1991 16:24-0500

In last night's ``Murder, She Wrote'' one of the key characters was a pesky little IRS agent that went around always getting his way by making veiled threats which bordered on extortion. Irksome, but nothing really new from a plot perspective.

What disturbed me more was that as the plot progressed, Jessica knew she was out of clues and needed help. So she went to what she called ``somebody who is paid to know everything about everybody'' (the IRS guy) ... and with only a little bit of coaxing, managed to the agent that it was in the tradition of trapping Al Capone on his taxes for him to reveal to her information on the suspect. And she probably thought that neither of them had done anything wrong.

I'm going to write to CBS about this one. Maybe I won't be the only one.

It seems to me like a little well-placed pressure on TV writers and producers might not only get them back in line, but could even lead to some interesting plot lines exploring the potential bad side-effects of ``well-intentioned'' invasions of privacy, such as this one.

Retail Sales Oversight -- No backup

Dave Rotheroe <rotheroe@convex.com>
18 Feb 91 21:02:00 GMT

I went to my local 'Best Buy' - a new home appliance, electronic, and computer discount store in my area, to buy a few things last Saturday. Things went smoothly until I wanted to pay. Turns out their main store computer was dead - down for the count. In their incredible wisdom, there was no backup system, as the system was supposed to "come right back within a few minutes of going down". There was one (1) printout of prices in the entire store, which was being kept at the service desk so they could continue to work. The registers had no price help, which ment there were people running all over the store getting prices. In addition, the automatically printed credit card receipts weren't, forcing the clerks to manually imprint and fill out the forms, and make phone calls for authorization - tasks they admitted they weren't properly trained for, and had never done before. Probably the only reason the store managed to deal with it at all was that business was light. I found it both amusing and scary that the chain apparently has no backup system (like a printout for each register), and does not train their employees in exactly what to do and expect in the event of a long-term failure.

Dave Rotheroe, CONVEX Computer Corporation, Richardson (Dallas), TX 75083-3851
(214) 497-4512 rotheroe@convex.COM

Re: Tube Tragedy (RISKS-11.03)

Pete Mellor <pm@cs.city.ac.uk>
Wed, 13 Feb 91 21:24:38 PST

Following my original mailing, Bill Carney <8332P@EARN.NAVPGS> wrote to say:

> I had always thought that the were pressure sensitive switches located on
> each of the doors. I am basing this assumption on the fact that on the
> New York City Transit system, a child can hold the subway doors open.

This gave me pause for thought. Eventually I replied more-or-less as follows:

I hope no child brought up in New york ever tries it on the London Underground! The doors *can* be held open, but only by brute force. I would say it would take a fairly strong man to prevent them closing. This is based on observation of strong men attempting to get on as the doors were closing, and on feeling the force personally when doing the same myself. The safety feature is that the train will *not* move while any door (other than the guard's) is open.

I have watched the guard carefully (on the few remaining two-man trains). He checks the platform, and pushes a button to close the doors. If these are obstructed, a light illuminates on the control panel. He opens the doors, to give the passengers a chance to get clear, checks, and tries again. When the doors close successfully and the warning light goes out, he pushes another button, and the train starts to move. (In the case of a driver-only train, I assume that the system is similar, except that the driver operates it, and checks using a TV monitor at the end of the platform.)

The limit for a door to trigger the warning seems to be a couple of inches, so that if a leg or arm is trapped, there should be no problem. If a shoulder-bag is trapped outside, and the door closes on the strap, however (as once happened to me), the train will move.

The interesting thing on two-man trains is that the guard's door must remain open as the train starts to move. Often there are several carriages with a guard's control panel, though obviously, only one is operational on the train at any given time. There must therefore be a way of selectively disconnecting a door from the warning system, and I *think* that this is what the "butterfly clasp" does. I asked the guard the other day where the clasp was. (I couldn't see anything resembling a butterfly anywhere.) He knew what it was, all right, but he wasn't going to tell me. "There've been too many accidents with those things!", he said. He told me to write to LU if I wanted more information.

In the meantime, is there anyone out there who is well-informed about safety systems on the London Underground, who can explain a) how a *passenger* could

operate such a device, b) why no special key is required to operate it, and c) why the warning system cannot be designed so that *only* the door next to the active guard's control panel can remain open *for whatever reason* as the train begins to move?

I have also heard a story that a woman was strangled a short time ago when the doors closed around her neck. Can anyone confirm this?

Peter Mellor, Centre for Software Reliability, City University, Northampton Sq.,London EC1V 0HB +44(0)71-253-4399 Ext. 4162/3/1

---

serious bug in SVR3.2 gives root access easily (RISKS-11.10)

Richard H. Miller <rick@pavlov.ssctr.bcm.tmc.edu>
15 Feb 91 17:27:11 GMT

> Date: Wed, 13 Feb 1991 12:19:18 CST
> From: pwolfe@kailand.kai.com (Patrick Wolfe)
> Subject: serious bug in SVR3.2 gives root access easily
>
> In my opinion, the rest of us are probably screwed. I seriously doubt any of
> these OS vendors will stop working on SVR4 to fix this bug in SVR3.2, except
> possibly for customers who pay for software maintenance. Many vendors are just
> about ready to ship their SVR4 release. I suspect most will tell those of us
> who don't pay for maintenance that we must upgrade to fix the bug.

[As an aside, I have a difficult time understanding why a person who does not pay for software maintenance expects to have bugs fixed. If you choose to not pay for the service, then don't expect the vendor to fix it for free.]

Now, as far as the risk is concerned, is this a good stand? Should security holes be in a special category as far as fixes from the vendor are concerned? The risk here is obvious since I, as a user of a BBS with a system with a security flaw which is not fixed due to the unwillingness of the operator to pay for software maintenance, have some exposure due to the hole. Should a system operator disclose the type of hardware and software he is running as well as the status of his maintenance so his users can determine their exposure?

Should vendors provide security fixes free to authorized purchasers since the type of risk is different than other bug fixes? What is the liability of a system operator who chooses not to disclose that S/W maintenance is not done and thus 'fixed' security bugs for a platform are not present? Can any liability be attached to the vendor because of the operator's decision to not pay for security fixes?

Richard H. Miller, Asst. Dir. for Technical Support, Baylor College of Medicine, One Baylor Plaza, 302H, Houston, Texas 77030 (713)798-3532

Re: Serious bug in SVR3.2 gives root access easily

<sef@kithrup.com>
Sun, 17 Feb 91 00:33:35 -0800

In RISKS DIGEST 11.10 pwolfe@kailand.kai.com (Patrick Wolfe) writes:
>It just goes to show that it was a good idea when I set my bbs up to run in a
>"chroot" filesystem, where even if a user could break out of the bbs program
>into a shell, there is no compiler (in fact, there are hardly any useful
>commands at all) to mess around with.

This seems like a good place and time to point out that that isn't really 'secure' from the bug in question. The major security aspect in the above described system comes from the fact that there is no compiler or (easy?) access to the shell; the chroot() only makes things slightly more interesting and challenging. (I leave it to the reader to figure out how to change u.u_rdir, since *the entire u block is writable*.)

Systems known not to be affected by the bug include Dell UNIX (both 3.2 and r4), in addition to the ones listed by Patrick.

For more details on the entire affair, read comp.unix.sysv386.

Sean Eric Fagan sef@kithrup.COM

Re: serious bug in SVR3.2 gives root access easily

Steve Nuchia <steve@nuchat.sccsi.com>
Fri, 15 Feb 91 23:16:44 GMT

On the subject of the 386 Unix security bug, which we recall makes the u area (per-process system data structure) writable by user processes, Patrick Wolfe (pwolfe@kailand.kai.com) said:

>It just goes to show that it was a good idea when I set my bbs up to run in a
>"chroot" filesystem, where even if a user could break out of the bbs program
>into a shell, there is no compiler (in fact, there are hardly any useful
>commands at all) to mess around with.

The number of ways one can go about getting bits into a file is truly amazing. Even cat, or any of its moral equivalents, might do it if the bytes can get past the serial driver. In fact, finding a way to turn on an execute permission bit is the hardest part of getting out of many chroot boxes.

The point I wanted to make here, lest anyone think that chroot is a shield against this bug, is that the process' current root is stored (just like its current directory) in the u area too.

This coupling of failure modes may strike one as undesirable initially, But security is not the same as functional failure protection. Rather than making a single point to failure by grouping individually tollerable failure points, putting all the security eggs in one u-area basket makes a *single* single point to failure out of a whole clutch of them.

If the failure of any *one* component breaks the system, you don't
gain anything by running them on seperate power supplies.

Steve Nuchia South Coast Computing Services (713) 964-2462

---

386 Unix Security bug fixes from vendors

<[anonymous]>
14 Feb 91

Without addressing any of the detailed (and significant) issues surrounding the
security bug in question at this time, the following is worth noting in any
case:

A recent poster to this list implied that they felt there would be no bug fixes
forthcoming for non-most-recent versions of 386 Unix from the various vendors.
This is not the case. Two of the main vendors involved, ISC (386ix) and Everex
(Esix) have announced no-cost bug fixes or upgrades to be available to deal
with the problem. ISC said that they expected their fix to become available
around 22 Feb 91. Other involved 386 Unix vendors can hopefully be depended upon
to follow suit.

Discussion of major security hole AT&T SYSV/386 in comp.unix.sysv386

Daniel A. Graifer <dag@fciva.UUCP>
Mon, 18 Feb 91 11:33:51 est

Over the last few days, there has been a substancial discussion occuring in
comp.sysv.386 regarding a major security hole in a number of the commercial
Unix System V/386 version 3 releases.

On Thu Feb 14 08:11:04 EST 1991 lumpi@dobag.in-berlin.de posted a complaint
that he had found a technique by which any process could give itself
superuser priviliges under ISC Unix. He claimed that ISC had been ignoring
his communications for half a year. In "dispair" he posted a 50 line c program
which when executied made the /etc/passwd and /etc/shadow files world
writable. He also posted an uuencoded binary.

Responses poured in from owners of other systems. SCO Unix appeared immune,
as were newer Dell releases. ESIX was vulnerable, as are some of the
hardware vendor's proprietary releases (such as Prime's EXL300 series).

The bug arises from a combination of two factors in Intel 80386 based
machines. Since many of these machines run without a numeric coprocessor,
allowance must be made to trap floating point instructions and invoke an
emulator. Since the performance degradation of switching to kernal mode
for each instruction would be large, the emulator runs in user mode. However,
it stores some items in the same memory page as the process' userid, and
must have write access to this page (SysV/386 memory protection is on a
per page basis, the second contributing factor). A process which may call
the emulator can dummy-up a pointer into this page and set it's uid to zero

(superuser).

It was claimed that AT&T has known about the trapdoor for some time, had informed the source licensees long ago, and had distributed a fix with the V.3.2.1 tapes. An employee from SCO claimed they had fixed the problem independently prior to the AT&T release. After someone on the net confirmed that older versions of Dell unix were affected, an employee of Dell posted a telephone number where owners of outdated releases could obtain fixes. An ISC employee posted that a fix would be available to A SUBSET (emphasis added owners after February 22 by calling ISC's support number.

The discussion contained two threads especially interesting to risks readers:

> Was it proper for the "discoverer" of the hole to post it so widely and in such a dangerous form? In his defence, he has not only raised the community's awareness of a serious problem, he has also forced ISC to respond to the issue. I did not see any postings in the group saying "Oh yeah, we systems administrators new about that."
>
> If it can be established that the vendors were well aware of the problem prior to the release of the software, were they legally negligent in distributing those release, and liable for any losses there customers sustained due this bug?

Because these systems are so 'cheap' (you can build a nice workstation for significantly less than $1000), they are being installed at an enourmous rate throughout the economy. Even when the vendors get off the dime and distribute fix already supplied by AT&T, how many vulnerable systems will be left in operation?

This reminds me of the "sendmail bug" exploited by the Internet-Worm, or the less well know System V "Inode Bug". As a purchaser of operating systems, I have no expectation that they will be bug free, but I am incensed when vendors fail to distribute available fixes to well known major problems. Or at least make sysadmins aware in the release notes of their existence!

Daniel A. Graifer, Coastal Capital Funding Corp., 7900 Westpark Dr. Suite A-130, McLean, VA 22102 (703)821-3244 fciva.FRANKCAP.COM!dag@uunet.uu.net

---

Re: Errors on Vietnam Veterans Memorial

Al Arsenault <arsenaul@usafa.af.mil>
Fri, 15 Feb 91 16:22:03 MST

The following excerpts are taken from an Associated Press story in the Friday, 15 February Colorado Springs Gazette-Telegraph.

"Up to 38 live Viet vets may be listed as dead"

The man responsible for deciding which names were carved on the Vietnam Veterans Memorial says there may be as many as 38 Army veterans mistakenly listed as dead. Robert W. Doubek said he wasn't positive at the time that the

men had been killed because their records were incomplete. But he included them anyway because he didn't know that it would be possible to add names once the memorial was built. "I had the idea these people might be lost to history if we didn't include them", Doubek said in an interview.

The Associated Press disclosed earlier this week that 14 Army veterans listed as dead on the wall are alive. After reading that story, Doubek volunteered that there may be another 24 errors. Apparently it is `impossible' to REMOVE names.

---

vietnam vet's name on memorial

Mary Smolka <GA82293@INDYLLY.BITNET>
Fri, 15 Feb 91 08:07 EST

Regarding the comment about a name on the Vietman Memorial possibly being MIA:

I was a tour guide in Washington DC for two summers while I was in college, and learned all sorts of trivia about the various memorials. It's true that there are different symbols on the memorial to denote KIA or MIA; a diamond next to a name indicated KIA while a cross, or a plus sign, indicates MIA. If a soldier listed MIA is found to have been killed, a diamond can easily be carved over the cross. If a soldier formerly MIA is found to be alive, the plan is to engrave a circle around the cross to denote "the circle of life." At the time I was guiding ('87,'88) there were no cases of this occurring, and I haven't heard of any since.

With over 58,000 names on the memorial, there WERE mistakes made. Between my first and second summers, several names were added that had been found to be left off the memorial when it was first commissioned. And from what I understand, there are some other names that SHOULD be on, but there isn't any more room. Hope this helps.

Mary Smolka.

Driving records (was Risks of having a sister)

Jim Griffith <griffith@dweeb.fx.com>
Fri, 15 Feb 91 10:38:36 PST

sullivan@poincare.geom.umn.edu discussed tying tickets to drivers' licenses and vehicles. My understanding of California law is that they distinguish between parking tickets and moving violations. A moving violation is tied to a driver's license, while a parking ticket is tied to a vehicle. So moving violations can affect license renewal, while parking tickets can affect vehicle re-registration. Strikes me as an intelligent approach, although I'm curious as to how the DMV deals with changes of ownership of cars with unresolved violations.

Jim

Re: Quick n' easy access to Fidelity account info

Steve Golson <sgolson@east.sun.com>
Thu, 14 Feb 91 19:14:45 EST

In RISKS 11.03 Carol Springs reports on a Fidelity Investments account inquiry service that can be accessed with only the account holder's SSN.

I called Fidelity to ask them about it. They said the service had been discontinued due to customer complaints, and that in any case it did *not* allow complete access to holdings info. What you got was the closing prices of the stocks etc. being held in the account, but *not* the total value. Still this is bothersome enough.

Fidelity does has a service called FAST (Fidelity Automated Service Telephone) which requires an account number and the last four digits of your SSN. Once you are into FAST you can get balance inquiries, make account transfers, and even open new Fidelity accounts...

Steve Golson -- Trilobyte Systems -- Carlisle MA -- sgolson@east.sun.com
(consultant for, but not employed by, Sun Microsystems)
"As the people here grow colder, I turn to my computer..." -- Kate Bush

Search RISKS using swish-e

THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

ACM Committee on Computers and Public Policy, Peter G. Neumann, moderator

Volume 11: Issue 14

Wednesday 20 February 1991

Contents

Another Computer Application fiasco story

Christopher Allen <Allen@RELAY.PRIME.COM>
20 Feb 91 11:09:43 EST

The following copied from the (Manchester, UK) Guardian Weekly, Feb 17, 1991:

High-tech blackout

Whitehall's auditors are unable to verify Foreign Office spending last year because of a breakdown in the main computer controlling the accounts. John Bourn, the Comptroller and Auditor General, has refused to approve the Foreign Office accounts, covering embassies, Nato, the United Nations, military

aid, the BBC World Service, and the British Council, because the ministry cannot produce accurate evidence of the spending.

At one stage auditors found discrepancies totalling 458 million pounds between the money granted to the Foreign Office and their own records. After extensive checking the auditors were left with 26 million pounds of imbalances in accounts for embassies, external relations, the BBC and the British Council.

The trouble began when it was decided to replace its six-year-old computer system with a new high-technology version. Ministers allocated 560 thousand pounds for the scheme, but ended up paying 937 thousand pounds employing a software company, Memory Computers, which failed to deliver on time and went into liquidation just after it did deliver. Meanwhile, a hard disc shattered inside the old computer, destroying all the information, and leaving officials to rely on the new untried system. Within months it started shutting down unexpectedly, and inexplicably posting money to the wrong accounts. All the bookkeeping staff left and their replacements were not able to familiarise themselves properly with the system to prevent further errors.

A consultant from the bankrupt software company is now working for the FO at a salary of 53 thousand pounds a year to try to solve the problems. MPs on the Commons Public Accounts Committee are to summon Sir Patrick Wight, permanent secretary at the FO, to explain the mess.

[FO=Foreign Office, MP=Member of Parliament, 1 pound ~ $2]

Software failures and safety of American (Red Cross) blood supply

<JAMESRC@QUCDN.QueensU.CA>
Wed, 20 Feb 1991 12:51 EST

Recently "60 minutes" presented a report on the American Red Cross and on the accidental release of untested donations to transfusion centres. The FDA documented >2000 such cases, although (to my knowledge) no documented cases of transfusion associated infection have yet been reported in the literature. Some of the failures were associated with software problems in the various regional AmCross centres, but that is as much as I know.

If anyone has further information on these (apparent) software failures, I would appreciate additional information.

Rob James, Department of Community Health and Epidemiology, Queen's University Kingston, Ontario, Canada K7l 2M1 613-542-3696

MD-11 computer problems

<smb@ulysses.att.com>
Wed, 20 Feb 91 15:50:02 EST

According to the AP, American Airlines has suspended flight certification tests on a new MD-11 plane because of ``computer problems''. That, and

some other problems with fuel economy, may lead the airline to refuse delivery of a second MD-11. No technical details on the computer problems were given in the article; does anyone on RISKS know more?

More on very reliable systems

Anthony E. Siegman <siegman@sierra.Stanford.EDU>
Wed, 20 Feb 91 12:13:10 PST

Anyone concerned with the subject of multiple correlated failures in systems with very reliable individual components should look back at the incident some years ago when a United Airlines jet lost all three engines simultaneous in flight over the Caribbean south of Miami.

As best I recall, a mechanic servicing the plane had made the same mistake, leaving out a needed O-ring (!), on the oil pressure sensors in all three engines. He did this because the stockroom clerk, who normally installed the O-rings on the sensors before handing them to the mechanic, was temporarily away, so the mechanic went behind the counter and got the sensors himself.

This incident seemed to have multiple classic elements:

1. Minor change in procedures had major consequences.

2. The problem was really a false alarm, i.e., the oil pressures were OK, just the sensor indications were wrong.

3. Confident claims that multiple jet engine failures were totally improbable proved completely wrong.

Oh, they did get one (or two?) of the engines restated, just in the nick of time, however, and limped into Miami.

Re: Predicting system reliability

<henry@zoo.toronto.edu>
Tue, 19 Feb 91 23:40:50 EST

>Argument 2: A system as complex as SDI can never be evaluated in a way which
>would give reasonable grounds for claiming that it would work correctly when
>deployed.

Of course, just what constitutes "reasonable grounds" is itself something that should be part of the specifications, and it is something that may have to be justified. None of the complex systems designed for fighting nuclear wars -- including the ones whose supposed efficacy has preserved the peace of the planet for circa 40 years -- has *ever* been evaluated in such a way (i.e. under nuclear attack!). The design of test criteria for such systems all too easily becomes a second-order way of cooking up fallacious "proofs" that the system is anywhere from trivial to impossible.

Our lives depend frequently on systems that cannot possibly be tested to the "reasonable confidence" point before they are used... if you interpret that to imply reasonable confidence under the worst conceivable conditions. No airliner is ever tested in six-sigma turbulence. No building is tested in once-per-century wind loads. Space-shuttle payload limits are based on landing weight for the "Return To Launch Site" abort mode... a procedure that has never been tried and which some astronauts doubt is survivable. Operating-system kernel software is rarely stress-tested under truly severe operational loads.

(As an example of that last, one of the major RISC-processor manufacturers does massive simulation of new designs, to the point where their machine rooms go from fairly quiet to furiously active at the time in late evening when the night's batch of simulation jobs fire up. This sudden huge surge in load has, I'm told, had a serendipitous side effect: at least once it uncovered the existence of very short "interrupt windows" in kernel code, where erroneous assumptions about the atomicity of operations caused system failures only if an interrupt struck in a window about a hundred nanoseconds long. (Specifically, the programmers had assumed that incrementing an integer in memory was an atomic operation, which is sort of true on single-processor CISCs but is rarely true on multiprocessors or RISC systems.) The code containing this botch is now theoretically obsolete, but it was in wide production use before the problem was discovered and is probably still in use here and there.)

In traditional engineering, it is routine to assess worst-case behavior based on extrapolation from less severe testing. A demand that the worst case be tested is often a disguised call for a system's cancellation, since such testing is seldom feasible for large systems. The proper consideration is not whether we can safely extrapolate from less severe tests, because we must rely on such extrapolation and we already do; the questions are how best to do such extrapolation and what form of testing must be done to permit confident extrapolation.

Henry Spencer at U of Toronto Zoology utzoo!henry

Broadcast LANs and data sensitivity

<henry@zoo.toronto.edu>
Tue, 19 Feb 91 23:45:37 EST

>How much of your data on the average network is really a security issue?
>I work here at Boeing and, at least in my area, sensitive data is not
>kept on the network ...

Unfortunately, this is probably a definition of "sensitive" which is too narrow to be really applicable. How much of your area's data could be posted on a bulletin board in the bus station without upsetting Boeing or one of its customers? Probably not much. Even material which is not "sensitive" in a military sense is often of commercial value or significant to privacy.

Henry Spencer at U of Toronto Zoology utzoo!henry

Re: software warranties (was: the SysV security bug)

Brian Kantor <brian@ucsd.Edu>
20 Feb 91 06:00:25 GMT

>From: rick@pavlov.ssctr.bcm.tmc.edu (Richard H. Miller)
>[As an aside, I have a difficult time understanding why a person who does not
>pay for software maintenance expects to have bugs fixed. If you choose to
>not pay for the service, then don't expect the vendor to fix it for free.]

I do expect the vendor to fix it for free. When I pay for software, I do so under the assumption that it would perform as specified, not that it sorta might work kinda like what the manual said.

When you buy a device (say, a car) you are granted a warrantee that it's free of defects, and will remain so for some length of time that is predicated (disregarding, for the moment, marketing factors) on the designed length of time it's to operate before it wears out. Software does not wear out, although it can become obsolete, so I would maintain that a piece of software which is found, at any time, to not perform as specified at time of purchase is defective and must be remedied by the vendor. A manufacturer must remedy the errors of his employees. That you hire peoples' mistakes when you hire their talents is one of the RISKS of doing business.

A company which is selling defective or adulterated materials should be made to replace those materials with goods of the quality advertised. I see no reason that software should be exempt from this basic principle of fair dealing in business.

Vendors who require paid maintenance agreements to repair faults where their software does not perform as specified are ripping off their customers. I believe that it is unjust enrichment.

Does it seem fair to you that the product you bought does not work as specified and could not have been tested by the maker of the product or he would have found out that it didn't so work? Not only have you been burned by buying something that is broken, but you've had to act as the manufacturer's unpaid quality control department, and they want you to pay for the privilege of getting a working item! Recall the definition of chutzpah - the man who kills his parents then begs mercy from the court because he is now an orphan.

Now while I've overstated this for effect, I would really like people to think about software warrantees, before the courts do it for us. Ethics ARE important: a professional should strive to be "an ornament to his profession."
- Brian

---

serious bug in SVR3.2 gives root access easily (RISKS-11.13)

David Lamb <dalamb@avi.umiacs.umd.edu>
20 Feb 91 14:07:18 GMT

A *bug* is a defect in the product. Why *shouldn't* the vendor fix it for

free? Enhancements, I'll agree, ought to be paid for. Maybe this is diverging from what RISKS ought to talk about, but...What are the risks to society of fostering an attitude that the vendor has no responsibility for defects like the security bug mentioned?

"Due to a design defect, your 1986 Model X car blows up if hit from behind in an accident. What, you didn't buy the $4000/year maintenance agreement?** Sorry, no free recall for you. Buy a 1991 Model X."

**25% of purchace price per year: a software "maintenance" price I've seen a few times.

David Alex Lamb

Charging for bug fixes (was: serious bug in SVR3.2 ... RISKS-11.10)

Steve Eddins <eddins@uicbert.eecs.uic.edu>
Wed, 20 Feb 91 14:37:22 GMT

I'll be the first to admit that I don't understand the economics of the software industry and the in's and out's of software maintenance. I'm just a customer. However, as a customer, I expect that when I pay for any product it will work as advertised. If it doesn't work, and the vendor wants to charge me more money to make it work, I will cease purchasing from that vendor.

Steve Eddins University of Illinois at Chicago, EECS Dept., M/C 154,
1120 SEO Bldg, Box 4348, Chicago, IL 60680 (312) 996-5771

Re: RISKS DIGEST 11.13

Peter da Silva <peter@taronga.hackercorp.com>
Wed, 20 Feb 1991 13:34:26 GMT

Poster #1:
> [As an aside, I have a difficult time understanding why a person who does not
> pay for software maintenance expects to have bugs fixed. If you choose to
> not pay for the service, then don't expect the vendor to fix it for free.]

Why not? The bug is the vendor's responsibility. Imagine Ford selling cars with doors that unlocked if you hit them in the right place. Do you think they would get away with only providing fixes to people with maintainance agreements?

Poster #2:
> Because these systems are so 'cheap' (you can build a nice workstation for
> significantly less than $1000),

Could you explain how? My own system was more than that and I bought it from a friend for a phenomenal price. The operating system alone is a significant part of the cost.

I've seen 386SX platforms for $875. Add $375 for the cheapest runtime

only 2-user UNIX I've seen, and you're already at $1250. Add $300 for the RAM and as much or more for the bigger hard drive, and you're in the area of $2000. Now, $2000 I might be able to believe.

Re: serious bug in SVR3.2 gives root access easily (RISKS-11.10)

<henry@zoo.toronto.edu>
Wed, 20 Feb 91 13:12:44 EST

As I understand it, the people in question are not demanding free software maintenance. They are demanding that when they pay good money for software, they get software that meets specifications at least to the extent of being free of catastrophic flaws, and that if this cannot be assured at time of purchase, some minimal effort is made to assure it when flaws are found.

Henry Spencer at U of Toronto Zoology

Re: serious bug in SVR3.2 gives root access easily (RISKS-11.10)

Flint Pellett <flint@gistdev.gist.com>
20 Feb 91 16:31:20 GMT

I would say that there is no reason software should be any different than anything else you buy. If you buy a new appliance, you get a guarantee for 90 days against defects in materials and workmanship, and when you buy software you ought to get a similar guarantee. A bug like this is a defect in the workmanship, and if you are still covered by the guarantee, you ought to get it fixed free. But if you are past the 90 days (or however long) and you didn't buy a maintenance contract, then you are (and ought to be) just as much out of luck as if you didn't buy a maintenance contract on your fridge. Software buyers are likely to start paying attention to how long the guarantee is for, and not buy from companies with really short guarantee periods.

However, there is another category of safety related bugs which have always been in a seperate class: If the gas tank in your Pinto tends to explode, or the car tends to shift itself into gear by itself, Ford does a recall (often because the Govt. ordered it to) and fixes it at their expense. The laws about automobile recalls are a lot stricter than the ones on Software Developers, but if software companies can't clean up their act themselves, then what we are going to end up with is a big Federal bureaucracy monitoring stuff like this just like the one that monitors the automakers.

This particular bug is pretty clearly a "safety related" bug, in that failure to fix it could result in substantial losses by customers. I believe the software vendors also have a responsibility to let their customers know about it too, and need to mail something out to all their users they know about that either gives them the fix or tells them how to get it, just like the recall notices that you get if something is wrong with your car that could affect your safety. If too many vendors decide that it will cost too much now to act responsibly, then they're going to end up having to deal with a bunch of federal regulators who will make them act responsibly, and it will end up

costing them (and us software buyers) a lot more.

Flint Pellett, Global Information Systems Technology, Inc.,
1800 Woodfield Drive, Savoy, IL 61874 (217) 352-1165 uunet!gistdev!flint

Search RISKS using swish-e

THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

ACM Committee on Computers and Public Policy, Peter G. Neumann, moderator

Volume 11: Issue 15

Thursday 21 February 1991

Contents

Racetrack overpayments

Rodney Hoffman <Hoffman.El_Segundo@Xerox.com>
Wed, 20 Feb 1991 15:16:26 PST

A short item by Steve Schuelein in the 'Los Angeles Times' 18 Feb. 91 says that "a series of computer malfunctions" resulted in $26,000 in excess payouts at the local Los Alamitos racetrack. A too-lucrative payoff was posted for several minutes before the error was corrected.

Track president and general manager Lloyd Arnold said the computer problems also prevented satellite wagering at 14 outlets in Nevada, and the Nevada Racing Commission might suspend wagering on races at Los Alamitos until the problems are corrected. According to Arnold, "[Amtote] said a printer on the computer malfunctioned, but I think the personnel here is not qualified."

Peace Shield in trouble

<henry@zoo.toronto.edu>
Wed, 20 Feb 91 22:21:48 EST

No, this is not another SDI contribution! "Peace Shield" is the USAF-managed project to provide Saudi Arabia with an integrated air-defence control system. From Flight International, 23 Jan:

> The USAF is looking to Hughes, Unisys, Westinghouse or General Electric to pick up the pieces of the Peace Shield Saudi Arabian air-defence ground environment following termination of most of Boeing's contracts on the beleaguered programme.
>
> The USAF says it cut the bulk of the $1.05 billion contract because of Boeing's "...failure to make progress so as to endanger final operational capability". [sic]
>
> [Original target date was April 1991. Revised Boeing estimate was August 1994; USAF hopes others can do better. USAF action probably prompted by Saudi pressure.]
>
> Boeing's difficulties centred on developing the software for integrating the disparate sensors, sector operations, sector command and command operations centres.
>
> The programme appears to have suffered a similar fate to other software-intensive projects in that the prime contractor underestimated the quantity and the technical complexity of the software. Peace Shield required hundreds of thousands of code lines to be developed.
>
> The depth of the problem encountered by the company was indicated by its failure to meet even a considerably revised continental United States integration testing. [sic]
>
> [Boeing retains some minor hardware contracts for Peace Shield.]

Is Unix the ultimate computer virus

"Martin Minow, ML3-5/U26 19-Feb-1991 1606" <minow@bolt.enet.dec.com>
Wed, 20 Feb 91 13:12:19 PST

[Slightly edited by Martin Minow]

From: "mt@media-lab.media.mit.edu"
To: unix-haters@mc.lcs.mit.edu
Subj: Worse is better

I apologize for the relative lack of vituperation in the following, but you can draw your own conclusions.

MADRE::MWM 203 lines 8-FEB-1991
15:14

<> I once went to hear a talk by Thompson at MIT. Thompson said one of
<> the professors had said to him, "I hate you. UNIX stopped all research
<> in operating systems." Thompson apologized.

The professor exaggerates - but not by much. The comments by Bob in .29 are relevant in both cases. Oddly enough, there's been some talk in comp.society.futures about windowing systems, and an interesting article (included below) on OS developement (included below) landed in my mailbox recently.

The problem with OSF/Motif - and X in general - is not that it's missing features; it's that critical parts of it are arcane and unusable. I'm not sure that the resource mechanism can be deleted from it in any reasonable way.

Re: Murder, She Wrote (RISKS-11.13)

The Polymath <hollombe@ttidca.tti.com>
21 Feb 91 02:01:58 GMT

}It seems to me like a little well-placed pressure on TV writers and producers
}might not only get them back in line ...

Alas, they never were in line in the first place. I'm the son of a lawyer and have many friends in the legal professions. All agree on one thing: Practically everything you see pertaining to the U.S. legal system in television dramas is _wrong_. Always has been. Don't expect them to clean up their act any time soon.

Jerry Hollombe, Citicorp, 3100 Ocean Park Blvd., Santa Monica, CA 90405
{rutgers|pyramid|philabs|psivax}!ttidca!hollombe (213) 450-9111, x2483

Re: Maintenance (car recall/software analogies, RISKS-11.14)

Charles Shub <cdash@mumm.Colorado.EDU>
Wed, 20 Feb 91 16:16:34 -0700

=> [several articles on who gets fixes to bugs in software]

I find this thread of discussion interesting and amusing.

We don't really do any "software maintenance" in this field. What we are really doing is "software upgrades" no matter what we want to call it. I don't know the history behind the term "maintenance" in this context but can hypothesize several reasons.

The discussion brought to mind some past frustrations in dealing with a

subsidiary of Ford Motor Company, the frustrations arising on my part because of my inability to convince some people there that software was somehow fundamentally different from automobiles, and hence the construction processes were probably dissimilar. My frustration reached its peak when I was unable to properly convey my incredulity at the notion of periodic scheduled preventive maintenance on a piece of software. I still do not understand what that means.

The risk, of course, is that by using a "wrong" term we imply wrong things as aptly demonstrated (albeit peripherally) in the recent discussion of bug fixes.

charlie shub cdash@boulder.Colorado.EDU -or- ..!{ucar|nbires}!boulder!cdash
cdash@colospgs (BITNET) -or- (719) 593-3492

Warranties

"Joseph M. Newcomer" <jn11+@andrew.cmu.edu>
Wed, 20 Feb 1991 18:18:37 -0500 (EST)

<>From: rick@pavlov.ssctr.bcm.tmc.edu (Richard H. Miller)
<>[As an aside, I have a difficult time understanding why a person who does not
<>pay for software maintenance expects to have bugs fixed. If you choose to
<>not pay for the service, then don't expect the vendor to fix it for free.]

> brian@ucsd.Edu (Brian Kantor)
>When I pay for software, I do so
>under the assumption that it would perform as specified, not that it sorta
>might work kinda like what the manual said.

Absolutely. In fact, if Brian hadn't written this, I would have. If a shrink-wrap software license was applied to any product other than software, Ralph Nader or his equivalent would be on the industry in nanoseconds, and rightfully so. I am a former product developer. We took the attitude that you had to add new features to a product, enough to justify the upgrade fee, AND fix all the bugs reported in the previous version, insofar as possible (note that it was not a bug if the software didn't do something the user expected, as long as it hadn't been promised). I find it immoral and unethical to charge for bug fixes; the product was defective. But since we couldn't afford to give out free updates, we simply made the user buy the bug fixes by buying the new features. This is not totally acceptable, but is the best a 2.5 person company can do. On the other hand, I find it totally unacceptable that a company like Apollo could release a Pascal compiler with known code generation problems and refuse to fix it for a year because "it wasn't in the release cycle". The compiler generated incorrect code for compile-time constant expressions.

If we don't police ourselves, some vastly less competent and authoritarian group will eventually do it for us. And as software gets out more into the public there is less and less tolerance for the past attitudes.

Law is a way of formalizing what should be polite behavior. If everyone were polite, laws wouldn't be needed.

Business-as-usual is putting us all at RISK.

Re: Serious bug... (Pellett, RISKS-11.14)

Richard H. Miller <rick@pavlov.ssctr.bcm.tmc.edu>
21 Feb 91 00:26:50 GMT

Well, of all the postings so far in response to my original aside, this seems to be the only one which read the rest of the article. I specifically made a point of asking whether this type of software defect warranted special treatment from software vendors.

It is my feeling that there are two catagories of software defects that could fit under this catagory, security defects and data corruption defects.I consider these two catagories to be similar to the type of defect which would require a car to be recalled. They can cause the system to be destroyed or data within it to become unreliable. [In a software sense this is comperable to having the brakes fail or the gas tank explode.] These defects should be fixed free of charge.

Other types of defects would fit into the same category as what you get with a car. The software is warrented for a period of time in which fixes will be provided. At the end of this time, if you choose to not pay for maintenance, then you are out of luck. [Just as if your distributor goes out on your card after 1 year].

With this premise, what are the responsibilities of the vendor in providing fixes to the two types of defects? I can see no problem on the part of S/W vendors if a patch is all that is required to fix a problem. But if the problem is in the design of the software and requires a redesign which would appear in the next release, should users be provided the new version for free.

For the record, I believe that for security and data-integrity problems, the vendor does have an obligation to provide fixes within the scope of the original purchase.

Richard H. Miller, Asst. Dir. for Technical Support, Baylor College of Medicine, One Baylor Plaza, 302H, Houston, Texas 77030 (713)798-3532

Re: software warranties

<sullivan@poincare.geom.umn.edu>
Wed, 20 Feb 91 20:21:30 CST

Risks 11.14 had a very interesting discussion on software warranties. Many people responded to Richard Miller's suggestion (that someone who does not pay for maintenance should not expect bug fixes) by pointing out that bugs are defects and thus covered under the standard implicity warranties.

Flint Pellett suggests that software come with a limited-time guarantee, but
->if you are past the 90 days (or however long) and you didn't
->buy a maintenance contract, then you are (and ought to be) just as much out of

->luck as if you didn't buy a maintenance contract on your fridge. Software
->buyers are likely to start paying attention to how long the guarantee is for,
->and not buy from companies with really short guarantee periods.

Since software does not deteriorate over time like hardware, I see little point in putting a time limitation on any warranty. Vendors may wish to allow a short time period in which a dissatisfied customer could get a refund, but bugs (no matter when they are discovered) were presumably present at the time of purchase and should still be covered. Of course, there might be a problem if the company has long since discarded the product. But software usually has a limited useful life so I don't really think we have to worry about people making warranty claims 20 years later.

There needs to be some limit, however, on the kinds of bugs covered.
Brian Kantor says
->I would maintain that a piece of software which is
->found, at any time, to not perform as specified at time of purchase is
->defective and must be remedied by the vendor.
I think this would merely lead to a lack of detailed specifications:
"You found a bug? Oh, no, that's a feature."

It seems clear that safety-related bugs, like holes in operating systems, should be fixed for free. And if there is gross misrepresentation of what the software does, or if it is so flaky as to be unusable, you would want a refund. If you buy a "screen editor" and get "ed", you return it. But if you get "vi", I'm afraid you're stuck with a few minor problems and shouldn't expect to have them fixed. Everyone seems to know bugs in "vi" (especially in autowrap), but don't hold your breath waiting for Sun or Silicon Graphics or anyone like that to fix them. The bugs are often annoying, but "vi" is still quite useful, and does its basic job. But does it "perform as specified"?

Software vendors should be expected to fix major bugs for free, but when it comes to more obscure problems or those with easy workarounds, this is less clear. If the vendor has switched to a new version, with substantial improvements along with fixes, it is hard for them to keep maintaining all earlier versions. While we might want free upgrades for life, this should be an option at purchase time, not required by the government, as it might drastically increase the cost of some software.

John Sullivan sullivan@geom.umn.edu

Software is not Hardware...(AT&T != Ford)

Greg Johnson <johnson@castor.cs.uga.edu>
Thu, 21 Feb 91 00:37:30 EST

Flint Pellet says:

>I would say that there is no reason software should be any different than
>anything else you buy. If you buy a new appliance, you get a guarantee for 90
>days against defects in materials and workmanship, and when you buy software

>you ought to get a similar guarantee. A bug like this is a defect in the
>workmanship, and if you are still covered by the guarantee, you ought to get it
>fixed free. But if you are past the 90 days (or however long) and you didn't
>buy a maintenance contract, then you are (and ought to be) just as much out of
>luck as if you didn't buy a maintenance contract on your fridge.

I disagree. The salient difference is that software, unlike hardware, is not affected by physical laws. Software is the expression of thought, and does not wear out. There are no bearings to go, no heat to fatigue. Thus, the defects which manifest themselves are purely a result of a failure on the part of the manufacturer. There is not, and should not be a MTBF for software. Though migration between architectures may be grounds to void this warranty, I cannot see how software houses can rationally set a warranty period shorter than that on my hard drive.

Re: warranties etc. (RISKS-11.14)

Gene Spafford <spaf@cs.purdue.edu>
21 Feb 91 17:02:00 GMT

In RISKS 11.14 there were many responses along the lines of "If I pay good money to buy software, I expect it to work as it should."

Brace yourself -- you didn't buy it. You have licensed it. If you check out all the fine print somewhere, you'll see that you have a limited license to use the software.

Also, if you look in that same fine print, you are probably going to find a disclaimer of warranty that absolves your vendor of all liability, and that explicitly disclaims any warrant of mechantability or fitness for any purpose. I.e., the software may not do anything, but they aren't *legally* representing it as supposed to be doing anything!

I don't think this is a proper way to do business, but it has become standard in the industry. There have been some cases where such warranty disclaimers have been struck down in courts if the software failed to even boot up, but I have never heard of the provisions being struck down for something like the security bug leading to this discussion.

In general, if you were to purchase a car or TV or any other major appliance, and in so doing had to sign a piece of paper that said (effectively):

> "You are not really buying this, you are leasing it. You can't sell it or give it away without our permission, nor are you allowed to take it apart to see how it works. We don't promise that it does anything in particular, despite what the salesman said. If you try to use it and it fails, we're not responsible for any damages of any kind. If really pressed, we'll exchange the item for a pile of the raw materials we used to construct it, at no charge to you. No other warranties are in effect on this item (except what may be in your state law) no matter what the salesman says -- we disavow any promises he made beyond this statement."

would you buy it? We do it with software all the time.....

The problem has complex roots, beyond the scope of a short message here: intellectual property, software specification and testing, and poorly-informed consumers add to the problem. We have cultivated a professional and commercial attitude that is really like only 2 other professions -- and they have state licensing imposed on them:

"I'm sorry, we did everything we could to treat the infection, but he just didn't respond."

"I'm sorry -- we gave it our best shot, but the jury didn't believe you."

"I'm sorry -- we used state-of-the art methods, but you know how hard it is to find *every* bug."

The bottom line: by current definition and tradition, your vendor is not really obliged to provide a fix unless you have a separate maintenance agreement. Talk of a recall is "silly." If you don't like it, you can always try to find another vendor to whom you take your business.

Before any of you get too outraged by this, check carefully:

* If you sell a computer product, what do *you* disclaim?
* If you are a consumer, how many products have you bought this way without complaint?
* When have you conveniently blamed something on "the computer"?

Gene Spafford, NSF/Purdue/U of Florida, Softw. Eng. Research Center, Dept. of Computer Sciences, Purdue University, W. Lafayette IN 47907-2004 (317) 494-7825

Search RISKS using swish-e

THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

ACM Committee on Computers and Public Policy, Peter G. Neumann, moderator

Volume 11: Issue 16

Monday 25 February 1991

Contents

RISKS in radiation treatment of cancer

Peter Kendell <pete@tcom.stc.co.uk>
23 Feb 91 10:07:42 GMT (Sat)

>From the Guardian (London edition) Saturday February 23rd

Patients die after radiation mix-up

A Spanish health official said yesterday that he feared the worst for 24 cancer patients who received high doses of radiation when a Zaragoza hospital's linear

accelerator went haywire for 10 days. Three patients have already died.

A Zaragoza judge is investigating the causes of the disaster, which the director of the Insalud chain of state-run hospitals called "the worst accident in the world" of its type.

"We fear the worst for some of the patients," an Insalud spokesman, Fernando Gomez, said. "We are seeking information to find someone who has experience in this kind of situation."

General Electric officials were unable to comment on the machine's operation. Hospital officials said that the machine was now functioning normally.

Peter (pete@tcom.stc.co.uk)

Computer Tax Glitch in Los Angeles

"Steve Milunovic" <Steve_Milunovic@qm.sri.com>
25 Feb 91 10:31:19 U

[abridged by PGN]

A story by Denis Wolcott (with contributions from Walter Hamilton) in today's Los Angeles Daily News from the NY Times service described how thousands of LA County homeowners were billed up to $15,000 for three years' property taxes, because of a 1988 glitch in an $18M computer system (`Optimum'), which did not work and had to be rewritten from scratch. As a result, the county was unable to collect $10M in taxes, and has kept them from disbursing the tax money to schools districts and other agencies. Mercifully, the county will not charge back interest on the unbilled back taxes!

Computer problems with MD-11 jumbo jet

Fernando Pereira <pereira@klee.research.att.com>
Sun, 24 Feb 91 14:55:19 EST

According to the AP (2/20/91), American Airlines might refuse delivery of a second MD-11 jet from McDonnell Douglas because of computer and fuel problems with the first MD-11 it received. American's chairman said that the airline is ``very, very, very unhappy'' with the plane. American has suspended flight certification tests for the plane because of the computer problems.

Warranties

Jim Horning <horning@src.dec.com>
Thu, 21 Feb 91 12:31:18 PST

I, too, consider the standard shrinkwrap warranties scandalous, and definitely a RISK to the public. But it's not easy to see how to fix them. Even though

the function of hardware is much better specified, computer hardware generally comes with what I call the Kodak Film Warranty: "liability limited to cost of unexposed film."

The current round of discussion has relied too much on strained analogies with automobiles, and not enough on a rational discussion of the issues. Greg Johnson and Gene Spafford separately made two important points in RISKS 11.15. Taken together, they provide a basis for considering what a sensible warrantee should promise.

1) Software isn't a "thing" that can be purchased, it is a design. As Dijkstra has said, "The true subject matter of the programmer is the design of computations." If we pursue the automobile analogy, we need to consider, not defective automobiles, but defective automobile designs (e.g., Pinto gas tanks).

2) Software doesn't wear out, and hence doesn't need "maintenance" to cope with physical wear. Any defects were present at the outset.

I think publishing provides a more natural and enlightening analogy:

- We buy media containing software, just as we buy CD's containing music or books containing words.

- There is a sharp distinction between the medium being defective (lost bits or missing pages) and the contents being defective.

- Most publishers warrantee only the medium, not the contents. However, if a CD was labeled as Beethoven's Fifth Symphony and the contents turn out to be 2 Live Crew, you can probably get an exchange during the first week after purchase, even if you've broken the shrink wrap.

- The medium is subject to physical wear and decay, not the contents.

- Some publishers of certain kinds of books will, for a fee, provide periodic updates to the contents of their books. Most book buyers don't pay for such services, but they are invaluable for a few. Other publishers will supply errata on request.

- There are few legal restrictions on what purchasers may do with the medium, many more about what they may do with the contents.

Not much software is sold with a specification precise enough to allow a customer to prove it "doesn't perform as specified."

Maybe someone who is outraged at the security hole that started this discussion would post the part of his vendor's specification stating that no such security holes exist? Failing that, maybe someone would post a specification that the vendors "ought to have" based their warrantees on?

After we see these specifications, we can discuss:

- What fraction of the total functionality of the operating system this component of the specification represents. We need some idea of the size

of the total specification that a warrantee should be based on.

- What fraction of the outraged customers would have noticed if JUST THIS PIECE of the specification had been omitted by their software vendor. And what fraction of those who noticed would then have refused to buy it.

Until we have ANSI standards (or their equivalents) for complete operating systems and application packages, I'm afraid that the ordinary customer is at the mercy of the competence and goodwill of the software vendors.

Jim H.

Accuracy in movies and newspapers (Re: Hollombe, RISKS-11.15)

Tom Neff <tneff@bfmny0.bfm.com>
21 Feb 91 00:00:14 GMT

The beauty of TV and newspapers is that _everything_ in them is wrong! This is really true. No matter what the subject matter is, if you happen to be a specialist in that area, you'll grit your teeth when you read or watch. Neurosurgery -- ballet -- the law -- names of streets in your own hometown -- archaeology -- accounting -- you name it, they get it wrong. I'm not surprised: the media have to talk about everything under the sun but couldn't possibly afford to be experts in all of it. The fun part is that even when we're done rolling our eyes at, say, some egregious astronomy error, we sit back and take at face value something about China or Churchill or Chernobyl or child development! We shouldn't. Experts in those areas are busy gritting their teeth even now -- while they swallowed the astronomy stuff without complaint. :-)

> [Another instance that strikes home even more is being directly MISquoted after making a carefully worded direct statement and insisting that it be used verbatim if at all... Perhaps there is nothing special about computers and related technologies that causes many media folks to be so far off the mark. But there are lots of technological nonsophisticates writing on technology (and only a few really thoughtful and careful ones). Perhaps the worst problem is the tendency toward 10-second sound bites and 25-words-or-less oversimplifications. PGN]

Re: Biology of Unix; Message attributions

<mt@media-lab.media.mit.edu>
Thu, 21 Feb 91 15:39:14 EST

Sorry, but I'm not the author of that message, it was forwarded from some company's internal mail system and the best guess at the author ID is MADRE::MWM. My own opinion of Unix is that it's more like crabgrass, or rabbits in Australia -- a rapidly-spreading and obnoxious weed that invades computational ecologies and displaces the native species.

Also, the Mike that signed the first few paragraphs is not me as you

inferred; it must be MWM. I only wrote the first sentence.

[finger informs me that "mt" is Michael Travers. Apparently he was unaware that HIS OWN FROM: field did not give his own name! In response to a poke from me, he has now upgraded. PGN]

worse-is-better for the 1990s

"Joseph M. Newcomer" <jn11+@andrew.cmu.edu>
Thu, 21 Feb 1991 15:32:30 -0500 (EST)

Here we are in 1991. The two primary operating systems (at least in volume) are representative of O/S technology of the late 1960s to early 1970s (Unix and MS-DOS), and the three important languages are C (vintage mid-1960s, i.e., it is BCPL in disguise), LISP (vintage late 1950s) and Ada (vintage early 1970s). With the exception of LISP, there have been many better operating systems and languages lost along the way, and there seems to be no interest in updating our technology. I have my list of better languages and O/Ss (and it is probably different than yours). But on the whole, the barely-adequate-but-portable has replaced the not-too-bad or even pretty-good but-not-portable. There is a lesson here. There is a risk of accepting the barely adequate; you may have to live with it for a long time.

Peace Shield and "software development problems"

<henry@zoo.toronto.edu>
Mon, 25 Feb 91 14:45:19 EST

A friend, who has asked not to be identified, says it looks to him like the Boeing problem with Peace Shield was not software-development trouble but cost estimation. (He has worked for Boeing but is not currently a Boeing employee.) His feeling is that Boeing bid low on a fixed-price contract, discovered an impending cost overrun, found that the Saudis weren't interested in pumping in more cash, decided that the best way to cut its losses was to encounter fatal software-development problems, and more or less stopped work on the project until the schedule slippage became too severe to ignore and the contract was cancelled.

This explanation is certainly plausible. Whether accurate or not, it points out a significant issue: problems in developing large software systems are sufficiently common that it's convenient to use them as an excuse when something goes wrong elsewhere. It's probably wise to be very cautious about blaming the software people for recent military systems, in particular. DoD has recently been using fixed-price contracts a lot, and a good many military contractors have discovered -- the hard way -- that they've forgotten how to do realistic cost estimates. Since DoD basically has no memory, it's better to default on the contract and accept some transient bad feelings than to fulfill it and lose money. Software makes a wonderful excuse, since it's considered a natural law that a certain fraction of big software projects inexplicably fail with nobody to blame.

Henry Spencer at U of Toronto Zoology utzoo!henry

Monopoly Security Policies for Thumb Prints

baldwin_bob#tsii@tandem.com <Bob Baldwin>
25 Feb 91 11:53:00 -0800

The California department of motor vehicles requires a right thumb print to get a driver's license or state ID card, so the DMV now has a large online database of thumb prints. The primary purpose of this database is to prevent people from taking on new identities without DMV knowing about it (and thus getting clean driving records).

What if someone is supposed to have a new identity? What about witness relocation programs? What about undercover police officers? The DMV has to treat all its thumb print data as being as sensitive as the most sensitive thumb print it contains. One alternative is for each government agency submit a list of the thumb prints that need special restrictions. Needless to say, the DMV wouldn't want to pay for the safeguards that would be required on such a list.

The underlying problem is the desire to enforce security (access) policies that imply monoploy control of data. For example, the FBI wants to know about all queries matching the finger prints of its employees. The National Crime Information Center can support this policy, but such a policy is hard to enforce when different states are involved. The FBI doesn't what to tell all the states about all its employees.

What's the solution? We could eliminate monopoly security policies and the programs that depend on them. We could have the federal government maintain its monopoly, and provide services to the states. We could trust the states to make sure that only "good guys" access the data. Perhaps the best solution is to ignore the problem and go to lunch.

Re: More on very reliable systems (Leichter, RISKS-11.12)

rod simmons <rod@uceng.UC.EDU>
Sun, 24 Feb 91 11:56:15 -0500

>In fact, I've always found it interesting how much more we demand from digital
>systems than we demand from mechanical ones. ^^^^^^^^^^^^^^^^^^^^^^^^^^^^

Perhaps we "do" because we "can," or at least we think that we "can," based upon an inspection of failure probabilities for various types of components and devices (such as those given in WASH 1400, and other similar compilations of failure data).

--Rod Simmons

Re: More on very reliable systems (Siegman, RISKS-11.14)

Robert I. Eachus <eachus@d74sun.mitre.org>
Mon, 25 Feb 91 17:11:12 EST

Anthony E. Siegman (siegman@sierra.Stanford.EDU) said:

> Anyone concerned with the subject of multiple correlated
> failures in systems with very reliable individual components should
> look back at the incident some years ago when a United Airlines jet
> lost all three engines simultaneous in flight over the Caribbean
> south of Miami....

> 2. The problem was really a false alarm, i.e., the oil
> pressures were OK, just the sensor indications were wrong.

No, the engines were really overheating because all the oil leaked out past the (missing) seals.

> Oh, they did get one (or two?) of the engines restated, just in the
> nick of time, however, and limped into Miami.

When the middle engine started to overheat, the pilot shut it down, declared an emergency, and immediately headed back toward Miami, grabbing for altitude. When the other two engines showed overheat, I think he cut the RPMs back so that engine failure would not be catastrophic, but in any case ran them to failure. When these two engines failed he was on a straight in glide to Miami International, with calculations showing that at best glide, the plane would hit the water a mile short of the runway. Passengers were told to prepare for the possibility of a water landing.

At an altitiude of 200 feet as planned (and apparently as explained to the passengers) the crew restarted the middle engine (which they had shut down remember) and got the hoped for two minutes of life out of it, long enough to land and get off the main runway. All three engines were damaged beyond repair.

Risks (or lessons learned) from this and the Gimli Glider incident? First, airline pilots should be required to have glider experience. In both these cases, the pilots knew what to do, however there have been several cases where the aircrew behavior during a multiple engine shutdown has verged on panic, most recently a Chinese 747. (There have been lots of such incidents, usually involving flying through clouds volcanic origin.)

Also, and much more important, but often overlooked, is the value of experience in knowing when some condition is "new" unknown and the trust which should be given to the pilots by their employers (and the FAA) in such cases. What would have happened if the pilot in this case took his time about turning back to see if he had a "real" ememrgency? In this case he acted immediately to turn around--he could always turn around again if the problem wasn't serious, and expect the airline to back his judgement. With some airlines, the pressure is in the opposite direction (schedule ahead of safety) and that was a contributing factor in the Gimli glider incident.

Search RISKS using swish-e

Report problems with the web pages to the maintainer

Search RISKS using swish-e

THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

ACM Committee on Computers and Public Policy, Peter G. Neumann, moderator

Volume 11: Issue 17

Tuesday 26 February 1991

Contents

The RISKS of automatic payments

<rhialto@cs.kun.nl>
Mon, 25 Feb 91 15:39:16 +0100

De Volkskrant" (a national daily newspaper in the Netherlands), 22 Feb 1991:

"Inhabitant of Amsterdam lies dead in appartment for half a year"

AMSTERDAM - In an apartment in Amsterdam-Southeast the police found the remains of a 51-year old man, who turned out to have died half a year ago.

[...] The man, who lived alone, died a natural death. The police discovered the man accidentally. A police officer heard from the caretaker of the building that he recently removed a large pile of mail for the victim from his mailbox. The occupant, who did not wish to have contact with his neighbors, had not been seen for a long time. When the police forced the door of the man, the inanimate body of the man was found. The skin of the man "looked like leather".

[This is the RISKy part:]

Because the rent and [natural] gas [for heating] and electricity bills were automatically transferred, nobody missed him. The man also automatically received an amount transferred into his bank account every month. Also, not one institution missed the man."

Need I say more?

Olaf 'Rhialto' Seibert, University of Nijmegen, The Netherlands

---

"Autopilot malfunction causes engines to break off"!

Martyn Thomas <mct@praxis.co.uk>
Tue, 26 Feb 91 11:07:33 GMT

According to Flight International [27 Feb-5 March 1991. Page 8]:

A Boeing KC-135 apparently had two engines break off, shortly after take-off, during Desert Storm operations in the Gulf. Apparently, autopilot malfunction overstressed the airframe, causing one engine to break away and hit a second, which was also torn from the wing. The 'plane is repairable, which says a lot for the pilot's skill!

According to the caption on the accompanying picture (of an undamaged, 4-engine USAF KC-135) "KC-135s have overstressed in the past because of autopilot disconnects".

Apparently, the 'plane performed a dutch roll, which can lead to overstrain of the airframe because of the divergent coupling of roll and yaw.

Martyn Thomas, Praxis plc, 20 Manvers Street, Bath BA1 1PX UK.
Tel: +44-225-444700. Email: mct@praxis.co.uk

Re: Computer problems with MD-11 jumbo jet

<faigin@aerospace.aero.org>
Tue, 26 Feb 91 07:50:57 PST

Well, someone who did vendor software IV&V on a minor subsystem does remember a few "oddities" -- like the vendor for the main flight computer not conforming to the system ICD, and everyone else rewriting all interface software during integration testing (on a crash basis) because the flight control software was so kluged that everybody including MD was afraid to touch it. And that one of the hydraulic control LRUs does the ARINC bus monitor checks, and tells

everyone else when to ignore the system (main flight) computers...

Re: Computer problems with MD-11 jumbo jet

<henry@zoo.toronto.edu>
Tue, 26 Feb 91 11:49:34 EST

As an interesting, and perhaps ominous, sideline on MD-11 computer problems, McDonnell Douglas recently decided that its next big airliner, the MD-12, will be fly-by-wire.

Henry Spencer at U of Toronto Zoology

Reliability extrapolation

Martyn Thomas <mct@praxis.co.uk>
Thu, 21 Feb 91 14:57:35 GMT

Henry Spencer comments that many systems which we currently trust (such as large buildings) rely on extrapolation as part of their safety case. He suggests that it may be reasonable to do the same for computer systems.

Maybe. Isn't most extrapolation based on the assumption that the system behaviour is continuous? Chaos aside, most physical materials do exhibit continuous behaviour up to the point of catastophic failure, and materials science gives us some insight into where the catastrophic failure may occur. (And sometimes that insight turns out to be wrong ...). Digital systems are, by their nature, discontinuous. You cannot easily justify extrapolation *or interpolation* of behaviour. There are digital weighing machines which give the correct weights *except for a few specific values*. How do you assess the probability of failure of a weighing machine with these characteristics?

So can we justify extrapolation? Under what circumstances? To what limits?

Risks of EMI?

<finkel@tartan.com>
Fri, 22 Feb 91 16:38:57 EST

As a mechanical engineer with a diverse career path, I have a few insights into the controversy over the "cancer causing" electromagnetic radiation. (I have enough statistics, chemistry, and analysis software experience to almost, sort-of, maybe know what I am talking about.)

1) POWER LINES CAUSE CANCER -- They most certainly do, but not because of EMR. To keep the access roads clear and to keep vines and other plants from growing around the power towers, the companies sprayed 2-4D, commonly known as dioxin or Agent Orange. (If you live near a power tower you have probably been exposed to a lot of agent orange).

The possible carcinogenic effects of this chemical are well known.

2) HAIRDRYERS AND TVS CAUSE CANCER -- Again, I have no argument with the truth of this statement. However, the cause is likely a chemical one. A hairdryer, they have removed all asbestos, is still a potent source of vapors. The high heat release some amount of the plasticisers into the air. This vapor laden air is promptly breathed in. The vapors then reside in the lungs because the particles fall into that marvelous size that only floats, never settles.

With TVs, you again have lump of plastic which give off continual emmissions. The transformer and "sealed" electronic components also give off toxic emissions. A warm PCB gives of a field of vapor that reaches a lot further than any stray RFI.

3) CRTS CAUSE CANCER -- The plastics argument still holds. All the hot cases and components on the PCBS give off toxic fumes. Yet another source of the vapors is the office itself. All those pretty sound deadening screens, particle-board desks, plastic counter tops, synthetic carpets, paint, ... give off significant amounts of vapor.

The kicker is that a NON_SMOKING environment contributes to the problem. The American Society of Heating and Refrigeration Engineers (ASHRAE) has established "safe" airflows for smoking and non-smoking areas. The non-smoking airflow is roughly 1/3 that of a smoking area. Therefore, filtration is also about 1/3. The ducts are also smaller, and so on. SOOO, all those cute chemicals have a lot of time to sit in your lungs.

The larger volume of air required for smokers also results in far more clean air coming into a building. Much of this new, clean air comes in by design, where air is drawn in by vents. Air also comes in through doors and windows. The increased incoming airflow also results in more air going out, along with all the stale, chemical laden air. Net result: smoking sort of helps air quality.

Another direct CRT confound is that the screen creates an electrostatic field. This field draws particles (dust, stray plasticisers, ...) which increase the concentration of hazardous chemicals around the CRT. The electrostatic field creates an airflow of garbage into your work environment.

I have no easy solutions. Some of these links may be be tenuous, but they are no more tenuous than the possibly erroneous correlations already drawn. The only real difficulty with my arguments is that the problems are worse, more pervasive, and harder to fix than just setting up a Faraday cage around a terminal.

Re: Risks of radiation treatment of cancer

Clark Savage Turner - WA3JPG <turner@ICS.UCI.EDU>
Mon, 25 Feb 91 20:17:42 -0800

I am keenly interested in the details of the Zaragoza, Spain accidents.

I have spoken with Gordon Symonds of the Canadian Bureau of Radiation and Medical Devices (who investigated the AECL Therac-25 early on....) and he surmises that since GE is mentioned in the news bits, that the culprit could be the CGR Saturne. He explains that GE recently bought out CGR.

The Saturne is the underpinning machine for the Therac-20, predecessor of the Therac-25. Of course, the Therac-25 is well known for its several elusive problems which caused massive overdoses. The Therac-20 is also known to have problems similar to those of its successor.

Can anyone lend a hand in tracking down these incidents?

- Clark Savage Turner, UC Irvine

Re: Accuracy in Movies and Newspapers

<John_Richard_Bruni@cup.portal.com>
Tue, 26 Feb 91 09:59:13 PST

I can understand the frustration that people feel when watching TV stories that extend into a field in which they are experts. But remember, the frustration may not be due to the *people* covering the story so much as the level of simplicity needed to convey a complex story to the general public. To claim the networks use ignorant people to cover the news is itself an ignorant statement. Speaking for my own network, it happens that our science correspondent has a doctorate in Immunology from a top-level school. Not too shabby considering how many stories on AIDS we have to do. One of our anchors is incredibly well-versed in statesmanship, coming from a long line of experts in the field and with more qualifications than you can imagine, both in terms of degrees and expertise. If he ever retires I`m sure any Political Science school in the country would vie for his time. It`s an easy thing to criticize the press. We don`t ballyhoo our credentials all over town but many of us have `em. How bright would you look in your field if you had to explain all your subject matter so the general public could understand you?

Actually, you`d be a darned good teacher if you could do this. The best lecture I ever heard on relativistic effects was explained in a way that made the topic seem almost simple. That was a talented professor who gave that lecture!

JRB

Re: worse-is-better for the 1990s

Jerry Gitomer <jerry@TALOS.UUCP>
26 Feb 91 16:14:49 GMT

Perhaps what we are seeing is Gresham's Law as applied to computers:

> The operating systems and languages of lesser intrinsic value
> will drive the operating systems and languages of greater
> intrinsic value out of circulation, because those of greater
> intrinsic value will be hoarded.

Now if I could only figure out how to hoard an operating system or high-level language :-)

Jerry Gitomer at National Political Resources Inc, Alexandria, VA USA
(703)683-9090 (UUCP: ...{uupsi,vrdxhq}!pbs!npri6!jerry

Automatic download of patches

Bill J Biesty <wjb@edsr.UUCP>
Tue, 26 Feb 91 09:32:22 CST

>From this week's Computerworld

"HDS downloads disk code" by Jean S. Bozman

Santa Clara, Calif. - Hitachi Data Systems Corp. (HDS) is not content to let its disk drives "call home" when they are not feeling well. Now, HDS engineering staff can send some prescription medicine down the modem line, the compandy said last week.

HDS claimed that an enhanced version of its Hi-Track maintenance program adds the dimension of on-line repairs to a 5-year-old automatic failure-reporting system. "We can apply many microcode changes without taking the customer site down," said Jeff German, manager of technical support at HDS.

The new feature, called Dynamic Microcode Download, adds to Hi-Track's existing capability to monitor, detect, diagnose and repair failing storage systems before they crash.

"If you're reacting to the threshold of pain that people at you customer sites have, then you won't prevent failures," German said.

After notifying customers of a device's impending failure, HDS technicians can send patched the software down a deadicated telelphone line. Payment for the Hi-Track service is included in the normal maintenance fee; the same automatic call-in service will be extended to the new generation of HDS EX mainframes later this year.

< Hi-Track is installed in 3,000 disk drive and tape storage systems world-wide, according to HDS.

The Right Approach?

However, some industry analysts are unsure whether this kind of service can build HDS's market share relative to IBM and Amdahl Corp. "This feature is not by itself going to convince a customer to buy an HDS 7380 or 7390 disk drive," said Robert Callery, a senior storage analyst at Technology Investment Strategies Corp. in Framingham, Mass. Not all microcode changes will be simple enough to transmit over the wire, Callery added. [...] IBM has a service director plan that automatically relays disk drive errors to IBM field sevice centers [... which when] recieved, IBM calls the customer site to schedule maintenance. [...] DEC and HP also offer automatic device-error tracking

services....

The competitive market place is making a bigger push for reduced costs (customer service visits) and introducing greater risks. It will be interesting to see if any of the problems with the new service get reported in the press.

Is anyone familiar witht he service and can give additional details about what kind of changes can be downloaded?

I believe there was an earlier dicussion concerning the Prodigy service's ability to automatically download changes to the remote PC's communications software.

I currently subscribe to America On-Line (AOL). We recently got a flyer in the mail saying that new features were going to be made available soon to users. I never got a disk in the mail. Then just last week when I signed on I got a dialog box saying "Updating software database" (or close to that). When I went to read postings on a bulletin board, there were new buttons to implement the announced features! My guess is that the data base changes were just the icon image and associated codes to transmit to the host computer rather than an executable. I haven't been able to find any documentation on this "feature" (which I'm sure saves AOL a ton of money avoiding mailings and disk duplication) much less an agreement that I permit AOL to change data on my disk drive!

Bill Biesty, Electronic Data Systems Corp., Research and Advanced Development,
7223 Forest Lane, Dallas, TX 75230 edsr.eds.com!wjb

Workshop on Designing Correct Circuits

<Victoria.Stavridou@prg.oxford.ac.uk>
Mon, 18 Feb 91 10:58:28 GMT

IFIP WORKSHOP ON DESIGNING CORRECT CIRCUITS IFIP
WG 10.5 Call for Papers WG 10.2
Lyngby, 6-8 January 1992

The purpose of this workshop is to bring together researchers interested in the design of provably correct hardware. The intention is to have a small informal workshop with focus on formal methods for designing correct circuits. In particular we would like to see presentations of methods that have been used in real designs. To keep this focus we will discourage papers which primarily discuss tools or the theoretical foundations. The program committee will be asked to observe these guidelines in their selection. Relevant topics include but are not limited to:

- formal hardware design languages,
- hardware design by transformation,
- computing-aided design and verification of hardware,
- methods of designing testable circuits,
- analysis of circuit descriptions,
- experience of the application of these techniques,

- experience (good or bad) with formal methods.

The workshop will be of interest to researchers in the area of formal methods for hardware design, and to engineers in industry wishing to keep abreast of this fast-moving and exciting field.

Programme committee: Joergen Staunstrup, Lyngby (chairman), Luc Claesen, IMEC, Peter Denyer, Edinburgh, Hans Eveking, Darmstadt, Mike Fourman, Edinburgh, Geraint Jones, Oxford, Tom Melham, Cambridge, Mary Sheeran, Glasgow, Robin Sharp, Lyngby, P.A. Subrahmanyam, AT&T

In addition to paper selection the program committee will find a "responder" to each paper selected for presentation. The responder will give a 5-10 minute criticism of a paper just after the presentation and the option of getting a 1-2 page contribution in the printed proceedings.

Call for papers: You are invited to submit a draft full paper on a relevant subject by 15th August 1991. Four copies should be sent to the chairman of the program committee: Joergen Staunstrup. Notification of acceptance will be posted by 15th October, and revised copies of full papers must be received by 1st December in order to be distributed at the workshop. The proceedings will be published by North Holland.

Local arrangements: The workshop will meet at the Technical University of Denmark in Lyngby. Robin Sharp is in charge of local arrangements. We intend to keep the cost of the workshop, meals and accommodation around Dkr. 2000 (US$ 350). Questions about the subjects of the workshop and other technical enquiries can be addressed to one of the organizers:

J. Staunstrup or R. Sharp,
Department of Computer Science, Building 344
Technical University of Denmark,
DK-2800 Lyngby, Denmark
e-mail: jst@id.dth.dk or robin@id.dth.dk

tel: (+45) 45 93 33 32 fax: (+45) 42 88 45 30

Search RISKS using swish-e

THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

ACM Committee on Computers and Public Policy, Peter G. Neumann, moderator

Volume 11: Issue 18

Thursday 28 February 1991

Contents

A weird error message -- old Cyber clock tale

Andrew Clayton <dac@prolix.pub.uu.oz.au>
25 Feb 91 11:43:46 GMT

When NOS/BE finally got to a stable configuration (about two years after they decided it was a dead O/S), three places in the world noticed a problem - if the machine stayed up for 24 DAYS, the system time-of-day clock would go haywire, and crash the system. :-)

The bug had never previously been found, because nobody had a Cyber running NOS/BE that had stayed _up_ for 24 days continuously!

Tennis anyone?

<[anonymous]>
26 Feb 91

Svensson moves up after error spotted

PARIS, Feb 26 (AFP) - Jonas Svensson of Sweden was the victim of the sort of unintentional error he thought he had put behind him when this week's ATP rankings were calculated. Svensson, the beaten finalist in the Stuttgart Classic at the weekend, originally appeared to have dropped from 13th to 17th. But the error was due to the confusion over his tennis-playing namesake, and the revised rankings reveal that he has actually moved up one place to 12th.

Svensson dropped the initial B. from his original playing name Jonas B. Svensson once the other Jonas Svensson on the circuit retired from the game and the possibility of confusion seemed to have disappeared. But when it came to compiling the new rankings, someone apparently keyed in the points Svensson earned in Stuttgart under the other Jonas Svensson's name. That had the additional effect of catapulting the now-retired Svensson into 140th place in the rankings, which was even more surprising as during his entire career he never rose higher than the 445th place he occupied in January 1984. [...]

Burden of Proof: name confusion in driver's license bureau

Steve Sears <sjs@iconsys.icon.com>
Wed, 27 Feb 1991 12:02:14 MST

The recent article by Robyn Grunberg reminded me of an experience I had in 1984.

I received notice from my insurance company that my automobile insurance was being raised drastically (4X as I recall). After deciphering the code that gives the reason for a rate increase, I found that I had been booked for a DWI (Driving While Intoxicated). At first I found this amusing, as I don't drink at all.

I called the insurance company to clear up what was an obvious mistake, and found that not only did they disbelieve me, but was given a lecture on driving and drinking! In order for them to change, I had to supply them with proof that I did not have a DWI, in triplicate, as well as a character witness. They made the mistake, yet I was given the burden of proof; not only of my not having committed the alleged offense, but of my personal integrity as well. And no, they had the facts and did not see any reason to verify them.

At the drivers license bureau, my record was as clean as I thought it to be. I got the printout (for a fee) and then had it notarized (for another fee). It was a slow day, and the clerk was amused by my little story, so he started playing with my drivers license number to see if a juxtaposition mistake had been made. We finally found the offender, who has the same last name and hence (in Utah), the same drivers license number but with an ADDITIONAL postfix character.

After sending this information, along with a letter from a couple of people who know me stating they had never seen me ingest alcohol, I was out $21 cash and had missed a few hours of work.

I then received a call from the insurance company who, instead of apologizing for the mistake, cross examined me on every point. I finally broke off with this person by threatening to sue unless they corrected their mistake.

Needless to say, I changed insurance companies. I also finally received notification that I had been reinstated to my previous status. No apology. The risk here comes down to a burden of proof sort of thing. I can see myself going broke in the event a large percentage of the companies I deal with all made mistakes and put the burden of proof on me.

Rather than just switch insurance companies in the first place, it seemed to me that if the record was not corrected, this disinformation would propagate and leave me in a worse position than meeting them head on.

Steven J. Sears, Sanyo/Icon sjs@iconsys.icon.com (801) 226-8057

But the computer person said it was OK!

<rlw@ida.org>
Thu, 28 Feb 91 12:46:55 E

Yesterday I went to the pharmacy to pick up a prescription that had been phoned in. When you pick up there, they make you sign across a computer-printed label that is origianlly clipped to your prescription but which they peel off and stick to a clip board for you to sign. After signing, I noticed that I had signed two identical labels that were sort of overlapping. Seems bogus so I asked the clerk, "Why two?" Answer: "Sometimes the computer prints two labels."

Abbreviating a longer interchange:
Me: I only got one prescription, tear one up.
Clerk: I can't
Me: Let me talk to pharmacist
Pharmacist: Don't worry about it.
Me: I am worried.
Pharmacist to clerk: Tear it up
(Clerk goes on to serve next customer)
Me: ?
Clerk: I'll do it later.
Me (to manager): ...labels...
Manager: I'm too busy to worry about that now.

Next morning, I recount the story over the hone to the insurance company who pays for my prescriptions. Thanks. They'll get back to me.

Several rounds of telephone tag. Then a completely satisfactory explanation: "The computer person said they can't charge you twice for the same prescription." "But suppose they are charging for two

prescriptions." "Don't worry, we have a numbering scheme that prevents our being charged twice."

Repeat for frustration_level:= 1 to 4
  Me: but...
  Ins. Co.: the computer person said that can't happen
Taeper

Nuts. Maybe the computer DOES accidently print two labels sometimes. After all, I'm smarter than their computer and I make misteaks sometimes.

--Dick Wexelblat (rlw@ida.org) 703 845 6601

Dave Rotheroe's "Retail Sales Oversight -- No backup" note

<wex@PWS.BULL.COM>
Thu, 28 Feb 91 15:40:44 est

While Dave notes the technological problems and customer-relations problems inherent in the situation he described, he only hints at what, to me, is the biggest RISK of all.

The problem is that the automation of these positions has led to the de-skilling of the workforce involved in them. It takes much less initiative and much less smarts that it used to: running something over a laser scanner, pressing a few buttons, and getting the customer to sign a receipt is not nearly as mentally or physically complex as the task used to be.

This is true not only for sales/retail positions, but for almost every job which has been automated. Where people have not been outright replaced by machines, they've been replaced by people with lower skill levels and often less experience and less education.

The result is a (you should pardon the phrase) dumbing down of the workforce. This leads to more and more situations where the workers are unable to understand/deal with/repair the machines with which they interact and are unable to perform the machine's functions when it fails.

As I see it, this has two negative consequences (call them risks if you like). There are situational problems such as customers being unable to get the product or service they want (and possibly businesses failing as a result), and there are societal problems such as loss of control, loss of motivation, loss of our country's position in the world.

I recommend interested RISKS readers pick up a copy of Barbara Garson's THE ELECTRONIC SWEATSHOP (Simon & Schuster 1988 ISBN 0-671-53049-6). She takes a step-by-step look at a number of jobs which are being automated. Even in places like financial planning where we'd like the planners to be smart, she shows how automated systems have led to dumber users.

--Alan Wexelblat phone: (508)294-7485
Bull Worldwide Information Systems internet: wex@pws.bull.com

LINAC deaths at Zaragoza

Trevor Cradduck <trevorc@uwovax.uwo.ca>
Thu, 28 Feb 91 12:25:33 EST

I am given to understand that the linear accelerator in Zaragoza that has given rise to the recent deaths from radiation treatment is a Sagitar 35 manufactured by CGR and marketed and serviced by GE. Unlike the earlier tragedies involving Theratrons from AECL, this machine does NOT have any computer control. So far as one can tell, this "accident" came about due to the machine having been left in an improper condition for treatment following service for a fault, and the improper condition was not detected before a number of patients had been treated. The case is due to go before the courts so that the parties involved are (understandably) reluctant to release detailed information.

Trevor Cradduck, Dept. of Nuclear Medicine, Victoria Hospital, U. Western Ontario, LONDON, Ontario, Canada, N6A 4G5 (519) 667-6574 TREVORC@UWOVAX.BITNET

Multiple failures

David Lesher <wb8foz@mthvax.cs.miami.edu>
Wed, 27 Feb 91 17:05:18 EST

Date: 27 Feb 91 17:48:49 GMT
Path: mthvax!news.miami.edu!ncar!ames!skipper!shafer
From: shafer@skipper.dfrf.nasa.gov (Mary Shafer)
Newsgroups: rec.aviation
Subject: Re: ref. to 3 holer/o -rings incident
Organization: NASA Dryden, Edwards, Cal.

(David Lesher) writes:

> I'm looking for a reference to tell me the date/carrier on that 727
> that took off from MIA without vital o-rings on the burners, and barely
> limped back in time, roaching the 3 fans in the process.

1. Report No. NTSB/AAR-84/04

4. Title and Subtitle: Aircraft Accident Report--Eastern Air Lines, Inc., Lockheed L-1011, N334EA, Miami International Airport, Miami, Florida, May 5, 1983.

16. Abstract: At 0856, on May 5, 1983, Eastern Air Lines, Inc., Flight 855, a Lockheed L-1011, N334EA, with 10 crewmembers and 162 passengers on board, departed Miami International Airport en route to Nassau, Bahamas. About 0915:15, while descending through 15,000 feet, the low oil pressure light on the No. 2 engine illuminated. The No. 2 engine was shut down, and the captain decided to return to Miami to land.

The airplane was cleared to Miami and began a climb to FL 200. While enroute

to Miami, the low oil pressure lights for engines Nos. 1 and 3 illuminated. At 0928:20, while at 16,000 feet, the No. 3 engine flamed out. At 0933:20, the No. 1 engine flamed out while the flightcrew was attempting to restart the No. 2 engine.

The airplane descended without power from about 13,000 feet to about 4,000 feet, at which time the No. 2 engine was restarted. The airplane made a one-engine landing at Miami International Airport at 0946. There were no injuries to the occupants.

The National Transportation Safety Board determines that the probable cause of te accident was the omission of all the O-ring seals on te master chip detector assemblies leading to the loss of lubrication and damage to the airplane's three engines as a result of the failure of mechanics to follow the established and proper procedures for the installation of master chip detectors in the engine lubrication system, the repeated failure of supervisory personnel to require mechanic to comply with strictly withe prescribed installation procedures, and the failure of Eastern Air Lines management to assess adequately the significance of similar previous occurrences and to act effectively to institute corrective action.

Contributing to the cause of the accident was the failure of Federal Aviation Administration maintenance inspectors to assess the significance of the incidents involving master chip detectors and to take effective surveillance and enforcement measures to prevent the recurrence of the incidents. [...]

Mary Shafer shafer@skipper.dfrf.nasa.gov ames!skipper.dfrf.nasa.gov!shafer
NASA Ames Dryden Flight Research Facility, Edwards, CA

Re: MD-12; Automatic download of patches (Biesty, RISKS-11.17)

"Martin Minow, ML3-5/U26 26-Feb-1991 2248" <minow@bolt.enet.dec.com>
Wed, 27 Feb 91 15:04:19 PST

Henry Spencer writes that, irrespective of the MD-11 computer problems, the MD-12 will be fly by wire.

This reminds me of the old joke:

> How many programmers does it take to change a light bulb?
> One, but you can never change it back again.

Bill Biestly writes about automatic download of patches in disk drives. I've seen a lot of new hardware designed -- roughly -- as follows:

-- core functions in ROM or EPROM.
-- everything else loaded at boot time.

For example, a large part of the Macintosh system software is in ROM, but much of it is patched by the operating system bootstrap. I've also seen disk drives where the ROM code is just smart enough to load the real disk code from a manufacturer's "private" area on the disk. These disks had

two ways to modify the firmware:

-- a "secret" sequence of SCSI commands could be used to read/write the
private area.
-- there was an asychronous terminal line interface that could be connected
to a debugging terminal. This could be used to patch the firmware and/or
dump internal tables and error logs.

I also know of a modem that can have its firmware updated over the phone
(I begged the manufacturer to put a jumper/switch on the board to prevent
this without direct user intervention. I also recommended some sort
of signature mechanism that would allow users to verify that they
have correct firmware. This was not a Dec product, by the way.)

While I'm quite aware of the risks involved, one should also understand
that there benefits to the user. Finding the tradeoff between trust,
mistrust, and convenience is a difficult problem, of course. My real
worry is that these changes are being made without customers who may
have good reason not to use a re-configurable modem understanding the
issues involved.

Martin Minow minow@bolt.enet.dec.com

Re: Risks of EMI? (Finkel, RISKS-11.17)

Bob Ayers <ayers@src.dec.com>
Tue, 26 Feb 91 17:17:57 -0800

In RISKS 11.17, mister "enough statistics, chemistry, and analysis software
experience to almost, sort-of, maybe know what I am talking about" writes that

> 1) POWER LINES CAUSE CANCER -- They most certainly do, but not because
> of EMR. To keep the access roads clear and to keep vines and other
> plants from growing around the power towers, the companies sprayed
> 2-4D, commonly known as dioxin or Agent Orange. ... The possible
> carcinogenic effects of this chemical are well known.

Unfortunately, as they say, "that turns out not to be the case." I have
enough chemistry background, and have done enough recent reading, to know
that dioxin, 2-4-D, and Agent Orange are three separate things:

> 2-4-D: a chemical herbicide
> Agent Orange: a mixture of 2-4-D and 2-4-5-T, a second chemical herbicide
> Dioxin: a minor chemical contaminant (production byproduct) in 2-4-D.

And "the possible carcinogenic effects" of those chemicals (he means the
dioxin) is *not* well known. The only bad effect of doixin on humans that has
been reasonable established is chloracne.

Zero for two. Bob

Search RISKS using swish-e

Report problems with the web pages to the maintainer

Search RISKS using swish-e

THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

ACM Committee on Computers and Public Policy, Peter G. Neumann, moderator

Volume 11: Issue 19

Friday 1 March 1991

Contents

About Risks in Believing AI Gurus (M.Minsky)

Klaus Brunnstein <brunnstein@rz.informatik.uni-hamburg.dbp.de>
1 Mar 91 17:45 +0100

On February 19-20, 1991, Borland collected, on the occasion of its 10th anniversary, a rare collection of gurus, experts, engineers, artists in Munich (Title: European Software Festival). On the program:

- Niklaus Wirth on his Oberon language concept (lecture, workshop)
- Bjarne Stoustrup (AT&T) with 2 lectures on C++/Object Oriented Programming
- Marvin Minsky: Lecture on Personal Software and Programs Who Know You
  (but he really gave a survey of AI history)
  plus Lecture on Artificial Animals
- Philippe Kahn: Back to the Future

- Joseph Weizenbaum against overestimation in research
- Izumi Aizu: Hypernetwork Society

Some more could not come (Alan Kay should not use plane), others really did not come (Cyberspace guru Jaron Lanier was only virtually present in a video)

One of the most stimulating (and generally uncomparable) events was a concert of Tod Machover (composer, director MIT Media Lab) who demonstrated his "conductor-aiding handglove" in a new composition, after having demonstrated his concept of "hyperinstruments" with a piece from his opera "Valis".

Also some native German speakers:
- Computer Art professor Herbert W. Franke on Experimental Esthetics
- Thomas von Randow on Cryptosystems ("If Mary Stewart had applied crypto-logy..."
- my own contribution was on Risky Paradigms in Informatics' Box of Pandora (starting from J.v.Neumann's assumption, that his EDVAC be equivalent to the human brain, with peripheral devices analog to "organs", I analysed risks in misconceptions, errors in realisations, misunderstanding on the users side, and malicious misuse, with examples well known to Risk Forum readers).

For about 2,000 participants in gigantic Gasteig Philharmonic site, this must have been a stimulating experience, but at least some of them will have corrected (hopefully) their world model on trustable gurus when Marvin Minsky, in a `press conference' was asked whether he would like to connect his nerves and brain to a `desktop brain' machine. Following his lecture where he argued that the human brain consists of about 40 neural machine each of which may have a specific frame architecture (he represented theories of Darwin, Freud, Piaget as specific search trees, and he discussed several types of frames representing brain activities), he then exclaimed: Imagine that you install 400 neural machines which will give 10 times the power of a brain! While Joseph Weizenbaum sat on the other side very quietly, Marvin became even more explicit when he discussed the possible role of philosophers (at most, those of the last 200 years seemed relevant to him) and religion (which he suggested to forbid as religion does not contribute to problem-solving).

No surprise that philosophers such as Socrates are not discussed in AI circles: following the relativity of knowledge (Oida ouden eidos! =I know that I do not know!), a knowledge base is a self-contradiction! (I now understand why MIT students were forbidden philosophy in Marvin's time as dean, as Joe Weizenbaum remembers).

>From a European point of view, the rational aspects, Human Information Processing and its Informatics equivalent "Artificial Intelligence" were so overemphasized that it became very difficult to believe that Marvin Minsky really believed what he said. With his special inspiration, Joseph Weizenbaum brought this to the real point when (summing up his experiences in discussions at MIT) he mentioned a dream: "I dreamt that Marvin leaves at his end - which is hopefully very far in the future a letter - saying: I never meant what I said!"

Personally, I would feel much more comfortable if I knew that Marvin Minsky is more conscious of the impact of his words; but I think that he just means what

he (and many others) says: that there is only a difference in material (dry Silicium realisation of "intelligence" versus the evoluted wet Carbon-based brain), and that it is only lack of contemporary knowledge why today's machines' intelligence seems inferior to human one. And that the vanishing difference between machine and brain will evolute in intelligence amplifiers where human nervous system may be connected to a desktop machine. In my analysis, it is this kind of misconceptions that are an esssential reason for contemporary computer accidents - misconceptions of scientists (uncritically following paradigms and unverified assumptions), top- and medium-level-misconceptions, misimplementations, misunderstandings on the users' side, conscious use of side effects and other misuse...

Klaus Brunnstein, University of Hamburg (March 1, 1991: 5 p.m. GMT)

PS: apologies to those who regard such philosophical discussions as mere speculations; I honestly do not wish to distract anybody from analysing real accidents on a realistic (that is, non-philosophical) basis.

Re: Jim Horning's note on software warranties (RISKS DIGEST 11.16)

<wex@PWS.BULL.COM>
Fri, 1 Mar 91 13:21:57 est

While I don't want to turn this into a comp.software-eng flamefest, I would like to disagree with something I think Horning is implying. He says:

> Software doesn't wear out, and hence doesn't need "maintenance" to cope
> with physical wear. Any defects were present at the outset.

This is true only in the most trivial sense. "Defects" can be one of two things. Either:
- a defect is a difference between the actual operation of the program and some formal specification of its intended behavior; or
- a defect is a difference between the actual operation of the program and some expectation on the part of the users/designers/clients.

Now, in the first sense it's true that software doesn't come to have more defects over time (though more may be discovered, obviously). However, it's important to remember that the latter definition is the one more commonly used, and under that definition, programs will indeed "wear out."

That is, I assert we cannot think of a program only as having a static set of defects which prevent it from meeting its intended purpose. Rather, there is a dynamic gulf between the expectations of the users and the operation of the program.

This is why software engineers are taught "the specification is *never* frozen." This is why complex systems which take years to be delivered so often fail. It's not that they don't do what they were originally intended to do -- it's that they can't cope with all the additional things they were asked to do during development (q.v. any number of military systems, command & control systems of all sorts).

As an aside, I don't like the analogy between software and books because books are primarily inert conveyers of information; people expect programs to *do* things. It's one thing to complain that your on-line encyclopedia is "wrong" and another thing entirely to complain that your aircraft-landing system is "wrong."

--Alan Wexelblat, Bull Worldwide Information Systems phone: (508)294-7485

Faxing a horse

<JERRY@HMCVAX.CLAREMONT.EDU>
Fri, 1 Mar 1991 00:40 PST

Today I attended an "Adobe Technical Conference." Contrary to its name, this was mainly a marketing meeting.

One discussion examined PostScript Level 2. One addition is the ability to create forms that are cached in memory (or on disk.) The idea is that one will be able to call up a form that will have already been imaged and thereby speed printer output.

Another discussion focused on the integration of PostScript and FAX technology. Adobe would like to see printers which have built in fax send/receive capabilities. Their idea is that with such a printer/fax device one could have remote printing on any fax machine in the world. They have planned extensions to PostScript Level 1 & 2 to permit a user to print a file with a phone number and have the printer fax the file to the phone number.

In many ways, this is an attractive idea. To push it further, they would have these PostScript printer/fax machines recognize when they had connected with another PostScript printer/fax device and in those cases send PostScript files. This is also an attractive idea when you consider a) the visual improvement PostScript can add to faxes and b) the compression in data of sending the PostScript over the scanned bits (Adobe claimed reduction of transmission times by factors of 2 to 25.) Adobe demonstrated this benefit by stating that 1/2 of all phone calls from Japan to the United States are made by fax machines. You can imagine the money saved by reducing the length of these phone calls by a factor of two.

The Adobe representative also portrayed what seemed to him an excellent idea. A company (a manufacturer for example) might cache their purchase order form on a supplier's printer/fax machine's disk and then reduce their fax transmittal times to the order itself, with no time spent transmitting the form.

Later on, I cornered the Adobe representative in a hallway and spoke of my concerns that some manufacturer could play tricks by ordering parts for a competitor and use a competitors purchase order form to make it all seem very legitimate.

Well, I didn't know the half of it. The representative admitted that security issues were great and offered a better scenario:

Imagine thieves faxing a trojan horse into another printer/fax machine. The receiver would be looking at an innocuous message, something like, "Hello World.", or "Joe's Pizza is now open", but his printer/fax would contain a PostScript program that copies future output to disk and late at night faxes that output back to the thieve's machine.

It's good to know that Adobe realizes the potential problems before producing the product and is trying to install features to prevent the abuse. Still, Adobe has many "unsophisticated" users and it will be interesting to see how they teach these users that their printer/fax machines can become a corporate spy.

Jerry Bakin.

But the computer person said it was OK!

<smb@ulysses.att.com>
Thu, 28 Feb 91 20:26:15 EST

That reminds me of an incident that happend to me a few Saturdays ago. I needed to pick up some 12-gauge electrical cable. I browsed past the 14-gauge coils, then picked up a 25' coil of 12-gauge. The price was about twice what the 14-gauge cost. Odd, and unreasonable; I checked further. The 25' coil of 12-gauge cost exactly the same as a 50' coil; that price in turn was slightly more than the same length of 14-gauge. Ah -- someone put the wrong sticker on the 25' coil, I thought. There was a clerk standing nearby; I pointed out the error to him. He consulted a handy printout. ``Nope; it's priced correctly; see?'' Sure enough, the printout showed that 25' and 50' of 12-gauge wire cost the same thing. I tried pointing out that that was unreasonable; he shrugged and walked away.

Having a bit of time, I decided to tell the manager. It took a bit of explaining to get my point across; one of the two individuals I was speaking to didn't understand anything I was saying. After all, the computer had the price as the sticker; what was the problem? I finally made myself understood, but to no avail -- store prices were set from the regional computer center a few towns away, and nothing could be done until the office re-opened on Monday. The price was wrong, and absurd -- but there was no way for them to fix it. (That they didn't do anything else, such as pulling the erroneously- marked coils from the shelf is another matter, of course.)

--Steve Bellovin

P.S. The next time I was in, a few days later, the pricing had been corrected.

Automatic Patching

Larry Nathanson <lan@bucsf.bu.edu>
Wed, 27 Feb 91 22:29:00 -0500

When I read the first half of the article on the Hi-Track Dynamic Microcode Downloading, my thoughts turned immediately to America Online.

I can vouch for the fact that AOL is self patching- I've seen Macintosh and Apple //e code come down the pike, into my computers. Sometimes it's icons, sometimes the inherent menu structure changes- sometimes new modules appear. I don't think there is any limit to what they can send over the lines- after all, they have game modules available on an optional basis (for the //e anyhow) which contain much code.

Nowadays, the patches are rather infrequent. During beta testing they were almost daily. The risks of accepting executable code, straight off the line, and executing it w/o giving the user a chance to virus check seems nerveracking, and my first impulse was that it is a risk. However, after some thought I decided that it should be relatively safe.

There are 2 ways viral code could get through- an outside job, and an inside job. For an outside job, the hacker would have to figure out the communiction code, (As a beta tester of the original Applelink Personal, let me tell you that this is NOT easy to do.), AND dissassemle the entire communications software- to find out where to patch. Then our illustrious hacker would have to establish a link to the user's pc. To do this, #1) The user would have to call the hacker's machine which would emulate a telenet node, or #2) the hacker would have to take over one or more telenet nodes. Neither is easy to accomplish without either the user knowing, or telenet getting VERY upset (i.e., litigious).

While anything is possible, I'm willing to bet that this is sufficiently improbable that AO is safe to external hacks using the patch command to give me a virus. Remember that nothing is 100% safe. Also- if they DID give me this virus, then SAM should grab it as soon as it starts to go after another application.

As for inside jobs, well, I don't know. One would hope that a disgruntled employee couldn't do anything alone that the 'gruntled' employees wouldn't stop. I know that 'freedom of hacking' is kept rather tight around Quantum- sometimes the people who are supposed to be doing things run into trouble. My feeling is that they are aware of the risk, and have safeguards to prevent such a thing - it would be the end of a very promising online system, if such a scandal was to occur. And the same caveat- while nothing is 100% safe, a runtime infection checker should catch anything while it's on the move.

(NOTE- I am not an employee of Quantum Computer Inc, makers of America Online, and other nifty things. I am a former beta-tester and online guide, with no current formal affiliation, except for lots of friends.)

--Larry Nathanson lan@bucsf.bu.edu

Risk from workstations with built-in microphones

"Steve Greenwald" <sjg@reef.cis.ufl.edu>
Fri, 1 Mar 91 12:46:49 -0500

A lot of new workstations and personal computers now come with a built-in microphone with hardware to digitize the microphone input. Example applications are digital signal processing and voice-annotation of software for documentation purposes. Many of these workstations are designed to be used as stations on local area networks (LANs). Additionally, it is quite common in some organizations to have workstations in the offices of individuals.

One risk of this technology seems clear: it is entirely possible for a determined person to write software that will activate the microphone and digitizer without the knowledge of the workstation user. The digitized acoustic data could then either be locally stored in the workstation (say, on a hard disk) for later retrieval, or, if the workstation is attached to a network, the data could even be sent to the eavesdropper's location. If the network is used, it would be quite possible (given the throughput of modern LANs) to send digitized voice. Using common techniques, digitized voice data requires a data rate in the neighborhood of 56 kilobits per second, while most LANs have data rates in the area of megabits per second. Of course, this method would require that the eavesdropper somehow acquire access to the workstation (perhaps with a trojan horse, or even physical access). Naturally, this would allow someone remote in time and/or space to eavesdrop on the area around the workstation.

Some possible solutions:

1) Eliminate the microphones when not absolutely required.

2) Have a switch (either manual or software controlled) to turn the microphone circuitry on or off. A problem with this solution is that it requires the user to remember to turn the microphone off when it is not in use, and would not eliminate eavesdropping while the microphone was turned on during periods when the user was not using it. Additionally, if the switch were software controlled, the eavesdropper's software could simply turn it on if it detected it as being turned off.

3) Have some sort of indicator (say, an LED) which would clearly show when the microphone circuitry was active. The indicator should be under the control of hardware only, to prevent it being disabled by the software of the eavesdropper.

4) Have an automatic logging function which would record the time and duration of each use of the microphone circuitry. A problem is that such a log would have to be frequently examined by the user, unless some sort of automated exception reporting were used.

5) Have some sort of sound-blocking cover which the user can put over the microphone when it is not being used. A possible problem with this solution is that if the eavesdropper has physical access to workstation, it would be possible to replace the cover with a fake one which is not sound-blocking. Therefore it would be desirable

to have some sort of build-in facility which could test the operation of the cover.

6) Require some sort of user authentication whenever the microphone is to be used. Even something as simple as a "dead man's switch" would work (although that could be annoying in practice).

Steve Greenwald, graduate student, Computer and Information Sciences
University of Florida, Gainesville, Florida

> [The microphone problem was previously discussed in the context of NeXT by E. Loren Buhle, Jr. in RISKS-10.65. PGN]

Specs for special equipment

Jim Purtilo <purtilo@cs.UMD.EDU>
Wed, 27 Feb 91 00:54:53 -0500

I have just checked into the hotel wherein a large meeting of software folks is held. The meeting announcement stated "if you plan on bringing a PC for use in the hotel room, then be sure to tell the hotel this when you make reservations. They will have the special equipment for you to hook your modem to the hotel phone system." I did this when making reservations.

There are specs and then there are specs, of course. At the desk, I asked "do you have the equipment I asked for?" to which I received a cheery "of course, Dr. Purtilo! We have your request entered right here in our computer."

Indeed.

I find my room is spacious, and quite special. It is well suited for a person who is environmentally disadvantaged. The front desk's reservation system, it seems, allows a flag for "special equipment" to be set, which refers to a room with all furniture placed for easy wheel-chair access. Mirrors, bath gear, toilets, etc, are all placed and oriented for someone with much different patterns of mobility than I exhibit.

I have not quite decided whether this is a software design flaw (desired state information not expressible in the system), user interface error, or just my usual luck.

(I am, obviously, overcoming my own handicap in this room, namely, that a phone cord is permanently fixed to the wall without nice modular jack for nethacking. Screwdrivers, 'gator clips, and an attitude ... don't leave home without them!)

Jim

Re: worse-is-better for the 1990s (Newcomer, RISKS-11.16)

Tim Chambers <tbc@hp-lsd.cos.hp.com>

Tue, 26 Feb 91 16:03:20 mst

>From: "Joseph M. Newcomer" <jn11+@andrew.cmu.edu>
> There is a risk of accepting the barely adequate; you may have to
>live with it for a long time.

I think the author misses Dick Gabriel's point. By the way he chooses his words, he is lamenting the fact that the world suffers from living with "barely adequate" implementations. The issue seems is more one of standards than of what is The Right Thing.

The company I work for has a long-standing tradition of trying to Do the Right Thing with technologies in our products. A funny thing happened when we ventured into larger and larger markets -- the slogan "standard is better than better" began to catch on with engineers battling with competitors for shares of billion-dollar markets. We began to seek out standards and promote them in our products.

I'd like to know if examples exist of cases where Right Thing technology *has been* compatible with mass markets. I can think of plenty of counter-examples: VHS versus Beta; multi-process, high-cost-of-entry computers (UNIX workstations) versus single-process, low-common-denominator computers (PC); and technologies used in television and power transmission. In all cases, the poorer candidate for being the Right Thing has more economic clout (i.e. it thrives in a larger market than Right Thing alternatives). (Perhaps FM radio is closer to the Right Thing than AM -- I welcome comments from an expert of what an ideal radio broadcast system would be so AM and FM could be compared to it.)

I don't see this as much of a lesson at all. It's the natural order of things in a competitive world.

Re: worse-is-better for the 1990s (Newcomer, RISKS-11.16)

Mark McWiggins <mark@intek01.UUCP>
Wed, 27 Feb 91 18:34:43 GMT

"Joseph M. Newcomer" <jn11+@andrew.cmu.edu> writes:
> ... There is a risk of accepting the barely adequate; you may have to
>live with it for a long time.

Hear, hear. Admiral Grace Hopper was quoted as saying "Well, it's not really what we want, but we'll fix it in the next release" on the occasion of the release of the original COBOL.

Mark McWiggins, Integration Technologies, Inc. (Intek), 1400 112th Ave SE #202, Bellevue WA 98004 +1 206 455 9935 mark@intek.com

---

Re: worse-is-better for the 1990s (Gitomer, RISKS-11.17)

Flint Pellett <flint@gistdev.gist.com>
27 Feb 91 21:48:09 GMT

>Perhaps what we are seeing is Gresham's Law as applied to computers: [...]
>Now if I could only figure out how to hoard an operating system or high-level
>language :-)

That's easy: you overprice it. When you can get BASIC for free but have to pay $100 for a C compiler, you end up with things that should have been in C written in BASIC. When it costs $400 for a bare-bones UNIX vs. $100 for DOS, the lesser system pushes out the greater one quite often.

Flint Pellett, Global Information Systems Technology, Inc., 1800 Woodfield Dr., Savoy, IL 61874 (217) 352-1165 uunet!gistdev!flint flint@gistdev.gist.com

---

Re: worse-is-better for the 1990s (Gitomer, RISKS-11.17)

<dan@BBN.COM>
Wed, 27 Feb 91 10:53:41 -0500

If you're a hardware manufacturer, you can hoard your software by just not letting it run on anybody else's hardware! This is one reason that UNIX drove out better, or at least better-adapted, operating systems: they couldn't run on anything except their own vendor's hardware, and the vendor wasn't interested in changing that situation since the greater intrinsic value was a competitive advantage in selling hardware.

If you're not a hardware manufacturer, you can still accidentally "hoard" an OS or high-level language by specializing it to a particular architecture so that you can't easily move it onto newer hardware. Multics and ITS are examples. In this case the problem is that operating systems and languages of greater intrinsic value usually end up requiring hardware of greater intrinsic value or specialization in order to do their job. Multics had protection rings and true dynamic linking, with specialized hardware to make them fast; UNIX has neither, so it can run on machines without the extra hardware.

Fortunately, Gresham's Law need not apply if the creator of the software isn't interested in hoarding it. GNU Emacs and gcc are good counterexamples.

Dan Franklin

Search RISKS using swish-e

Search RISKS using swish-e

THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

ACM Committee on Computers and Public Policy, Peter G. Neumann, moderator

Volume 11: Issue 20

Saturday 2 March 1991

Contents

Red clocks run faster than green ones!

Paul Leyland <pcl@robots.oxford.ac.uk>
Fri, 1 Mar 91 13:53:46 GMT

Copied from _The Times_, London, March 1 1991.

Speeding clocks cause for alarm

New street lighting systems in an East Midlands village have been playing curious games with alarm clocks, causing them to race up to four hours ahead while their owners slept.

Residents of Castle Donnington, Leicestershire, who own clocks with the

familiar red display [presumably LEDs -- pcl] had to call on the detective skills of East Midlands Electricity Board staff to solve the problem. Owners of more sophisticated clocks with a green display [plasma discharge? -- pcl] found they were sticking to Greenwich rather than Omani time.

An inspection of the local airport and voltage checks in houses and at substations failed to disclose the cause. Interference from cellular telephones was also ruled out.

The culprits were finally tracked to signals being transmitted by electric timers controlling local street lights that had recently been fitted by Leicestershire county council. Julian Evans, an electricity board spokesman, said the timers had been replaced and things appeared to be "ticking along nicely".

[Can anyone explain why "red" clocks should be more susceptible to this form of interference than "green" clocks?]

Re: Faxing a horse (RISKS-11.19)

Ed Wright <edw@sequent.com>
Fri, 1 Mar 91 12:31:21 PDT

I keep waiting for the day when someone releases a (postscript) laser printer, that incorporates a scanner so that I can use it as a printer, a scanner, a copier. Add fax to that concept and I think we would have a winner. Ed Wright

---

call for papers -- ACM SIGSOFT '91 [REMINDER. ORIGINAL IN RISKS-10.57]

Nancy Leveson <nancy@murphy.ICS.UCI.EDU>
Mon, 29 Oct 90 17:45:06 -0800

CALL FOR PAPERS

ACM SIGSOFT '91
Software for Critical Systems

New Orleans, Louisiana
December 4-6, 1991

Computer systems are beginning to affect nearly every aspect of our lives. Examples include programs that control aircraft, shut down nuclear power reactors in emergencies, monitor hospital patients, and execute banking transactions. Although such programs offer considerable benefits, they also pose serious risks in that we are increasingly vulnerable to errors and deficiencies in the software. [NO NEWS TO RISKS READERS!]

The SIGSOFT '91 conference seeks papers on all aspects of quality in critical systems. A critical system is a system that must exhibit, with very high assurance, some specific qualities such as safety, reliability, confidentiality, integrity, availability, trustworthiness, and correctness.

The conference will focus on such topics as architectures, design methodologies, languages, analysis techniques, and processes that can increase the likelihood that a system exhibits its required qualities.

Papers will be judged on relevance, significance, originality, correctness, and clarity. Papers will be read and evaluated by the program committee and must not be under consideration (or published) elsewhere in the same or similar form. Papers are limited to 6,000 words, with full-page figures counting as 300 words. A paper that significantly exceeds this limit is likely to be rejected.

Authors should submit 6 copies of the full paper to:

Peter G. Neumann, Computer Science Laboratory, SRI International,
Room EL-243, 333 Ravenswood Ave., Menlo Park, CA 94025

Persons submitting papers from countries in which access to copying machines is difficult or impossible may submit a single copy. Submissions should be received by May 3, 1991 and should include a return mailing address. Authors will be notified of acceptance or rejection by July 12, 1991. Full versions of accepted papers must be received in camera-ready form by August 30, 1991. Authors of accepted papers will be expected to sign a copyright release form. Proceedings will be distributed at the conference and will subsequently be available from ACM.

CONFERENCE CHAIR	PROGRAM Co-CHAIRS	
Mark Moriconi	Nancy Leveson	Peter Neumann
SRI International	Univ. of California, Irvine	SRI International
moriconi@csl.sri.com	leveson@ics.uci.edu	neumann@csl.sri.com

PROGRAM COMMITTEE

David Barstow	Schlumberger
Dines Bjorner	Technical University of Denmark
Marie-Claude Gaudel	Universite de Paris - Sud
Jim Horning	DEC Systems Research Center
Bill Howden	University of California, San Diego
Hermann Kopetz	Technical University of Vienna
Carl Landwehr	Naval Research Laboratory
Bev Littlewood	City University, London
Leon Osterweil	University of California, Irvine
David Parnas	Queen's University
Fred Schneider	Cornell University
Vicky Stavridou	University of London
Martyn Thomas	Praxis, Inc.
Walter Tichy	University of Karlsruhe
Elaine Weyuker	NYU Courant Institute

Risks of naming a node

"Rao V. Akella" <RAO@moose.cccs.umn.edu>
Tue, 26 Feb 91 15:50 CST

In addition to all the other problems associated with computers, have you ever wondered about the risks of _naming_ one? The study I work for has a workstation called SUCKER (ugh! my system manager -- who is a fishing maniac -- named it after a lake in the Boundary Waters Canoe Area in northern Minnesota).

Ever since we brought this machine up on the net, we haven't had a moment's peace. All the teenage wanna-be freshmen hackers from all the neighbouring state colleges who have just got their first computer account and have read "The Cuckoo's Egg" are drawn to it like a magnet. There's rarely a Monday when I come in and don't find breakin attempts on all the usual accounts: SYSTEM, FIELD, DECNET, INGRES, GUEST, ANONYMOUS...you name it. Fortunately, DECnet provides a pretty good traceback to the originating point of the attempt, and most system managers take such reports very seriously, so we've had about half-a-dozen amateurs kicked off their systems (I say amateurs, because nobody has gone beyond trying to guess passwords).

But then, we probably only have audit and intrusion trails for the ones that failed...

Rao Akella, Research Assistant, Colon Cancer Control Study
University of Minnesota, Minneapolis

Plugging in, in Singapore

<WWEAVER@cmsa.Berkeley.EDU>
Sun, 24 Feb 91 20:23 PST

In light of RISKS recent series on the Americard, I found the following interesting. Reprinted from the 24 Feb 91 Chronicle (Punch Section, page 5). All typographical errors mine.

THE PUSH-BUTTON SOCIETY
In Singapore, 2.6 million people are coming on-line.
By Reginal Chua (Reuters)

Singapore is striving to become a push-button city. From cashless shopping to electronic paperwork and even a computerized pig auction, Singapore is plugging its 2.6 million people into electronic grids linking the entire island nation. In less than a decade, it plans to build computerized electronic pathways to enable people to shop, book theater tickets, check information, and to allow companies to send documents.

Singapore's small size and highly centralized bureaucracy has made it relatively simple to establish the groundwork for the electronic society. All citizens carry a numbered identification card, allowing information about them to be cross-indexed between ministries and government bodies. Not all Singaporeans are thrilled ath the prospect of life in this version of a brave new world with an electronic ``Big Brother'' keeping tabs on them.

Some were unhappy to find that census takers calling at their homes already had detailed information about them printed on the census forms. ``It seems like they know more about me than I do,'' one housewife said.

The advantages of being plugged in, however, have become obvious to many. ``The purpose... is to turn Singapore into an intelligent island in which IT (information technology) will be fully exploited to improve business competitiveness and, more importantly, to enhance the quality of life,'' said Tay Eng Soon, minister of state for education. A new master plan, IT 2000, will be unveiled at the end of the year, Tay said. Parts are already in place.

TradeNet -- which allows companies to submit documents electronically to the state Trade Development Board -- now accounts for 90 percent of all trade documentation, a board official said. ``We're going to phase out the remaining 10 percent by the end of the year,'' she said. Some freight forwarders have reported productivity gains of up to 30 percent with the new system, she added.

Introduced only two years ago, the system handles 10,000 forms a day. Each takes 15 minutes to process, compared with as long as two days by the old method. Even payment for the service is electronic. Shippers used to have to paste revenue stamps on each form. Now the board deducts the fee electronically from their bank accounts. ``Up-to-date knowledge and information become of utmost importance when a country or company seeks to be competitive in the international arena,'' Minister of Communications Yeo Ning Hong said at the launch of a teletext system, Televiewe.

The Network for Electronic Transfers, a cashless shopping system, has been in operation for five years and is now used by more than a third of the population and 1,500 stores. Consumers have the cost of their purchases automatically deducted from their bank accounts. ``Certainly there was resistance at first. There was a lot of resistance, primarily from the retailers,'' said the network's general manager, Patrick Yi. ``We now have a critical mass of consumers and retailers.''

In the next five years, the network plans to expand to 6,000 outlets and boost transactions from about $300 million last year to $1 billion in 1995. Plans also include an ``electronic purse,'' which could replace several electronic cards being used at the moment. ``The concept is that from a national perspective, wouldn't it be nice if we could just have one card,'' Yi said. [!! --ww]

There are also other electronic networks -- for air cargo (Star Net), medical claims (MediNet) and company registry (LawNet).

The next futuristic concept is ``Smart Town,'' which envisions a national electronic grid to which households would be linked. ``The idea here is to build into the town a whole range of IT services,'' Tay said. ``People who live and work in such a town will have maximum and convenient access to many services.''

Even the local pig market has entered the microchip age. Wholesalers at the Hog Auction Market, or HAM, bid silently for swine on an electronic system which deducts winning bids from traders' deposits.

Only the odor remains.

Re: Singacard anyone?

JueyChong Ong <75216.726@compuserve.com>
25 Feb 91 00:09:00 EST

Having lived in Singapore for most of my life, I think I can comment on parts of Bill J Biesty's article in RISKS 11.09.

NETS was set up by a number of banks in Singapore primarily as an ATM network much like Cirrus or Plus System in the US. With one notable exception, if you bank with a NETS member, you can use any ATM machine belonging to a bank that is a NETS member (the notable exception being the Post Office Savings Bank, which claims to have the most ATMs nationwide, and therefore does not need to participate in the ATM network; but they do participate in the cashless shopping service mentioned next).

The other thing you can do with NETS is that merchants can subscribe to the service, and that allows NETS ATM card holders to use their ATM card as a debit card at stores. Shoppers use the same PIN they use at the ATM, and they can choose to have the purchase amount deducted from their checking or savings account.

On a recent visit to Washington, DC, I noticed a similar service being provided at a Safeway supermarket.

>I think it was mentioned in Risks, but was mentioned in WSJ that Singapore
>plans to install sensors in cars and roads and start taxing vehicle owners
>based on usage rather than an average fee to cover maintenance costs of roads.

Depending on how much the government decides to charge for road usage after implementing the sensors, it may turn out to be a welcome measure. Currently, cars prices in Singapore are more than double the prices in the US because of import taxes. Road taxes go for about US$600 a year now for a car with a 2-liter engine (more for bigger cars, less for smaller ones). The idea is to prevent traffic congestion by making it difficult for people to afford even one car. I don't think that's fair.

To reduce road usage during rush hours, there is a surcharge to enter the downtown area/city center/business district.

Implementing Electronic Road Pricing (ERP) gives the government an alternative to rapidly increasing vehicle import taxes, increasing rush-hour entry fees and, recently, annual car sales quotas. The hope is that it will result in fairer charging, and that they do not abuse the flexibility of ERP.

Incidentally, Singapore got interested in ERP because of its apparent success in Hong Kong.

Also, you may also like to know that some people do not believe in being charged "an average fee to cover maintenance costs of roads." The Feb. 1991 issue of New York Motorist (AAA Automobile Club of New York's newsletter) ran two articles: one was about the Club urging lawmakers to reject legislation that would put a flat-rate auto-use tax on vehicles in Westchester County. The

Club vice-president said the tax was "regressive - levied on the owner of a Rolls Royce at the same rate as on the owner of an old jalopy." While the main reason for opposing the fee was that it was "essentially a second registration fee" (and also a way for the county to raise more tax money in a bad year), I also took it to mean that charging everyone an "average" fee isn't very popular either.

The second articles was more interesting: the Port Authority of NY and the Triborough Bridge and Tunnel Authority are trying out Automatic Vehicle Identification (AVI) equipment to see if it could replace toll booths. A transponder is mounted on the vehicle windshield. A transmitter at the toll area generates a radio signal that is modified by the transponder when it is within range, at speeds of up to 35mph, to "the tag's individual identification code. The reflected signal with the new information is then transmitted to a central computer" which would then deduct the proper amount of toll from the vehicle owners account. I see a very blur distinction between this and Singapore's ERP efforts. In fact, from the photograph accompanying the article and the description, it seems uncannily similar to the system (or one of the systems) that the Singapore government plans to try out. The article also addresses several implications, among them: "A first step towards congestion pricing (charging a higher rate for driving during peak periods and encouraging off-peak use by lowering fees)", "Facilitating an expanded toll road system" and a "Big Brother" potential for "governmental agencies to keep tabs on citizens via their recorded passage through toll facilities". Sounds like Singapore?

--jc

Re: Singacard anyone?

Bill J Biesty <wjb@edsr.UUCP>
Mon, 25 Feb 91 08:30:46 CST

[Pravin Kumar <ppk@Sun.COM> responds to my submission of a Wall Street Journal article about the computerization of commerce in Singapore by pointing out that the U.S. is close behind in implementing the same technologies.]

Dallas, Texas, USA has similar technologies in use. The Dallas North Tollway, the only toll road in Dallas, put the AVI system into effect last year. I also have seen the use of ATM cards to pay for groceries and gasoline (whose risks were discussed recently).

One difference that does exist is that the Cirrus, Plus, and other ATM networks are not run by the government but by independent businesses that manage the networks.

I submitted the article not only as a follow up to the Americard idea but also the discussion of Margaret Atwood's "The Handmaid's Tale" where womens rights were removed by removing their economic freedom. This is risk that still exists (but not just for women I'm sure) in Singapore.

Access fees for driving in certain areas can be handled by selling permits to drive in congested areas. Other drivers can take the risk of driving into the area without the permit and getting a ticket. This method avoids the loss of

freedom in letting some accounting system keep track of where you are.

The Tollway incidentally provides a quicker access to downtown
as many drivers don't want to pay the tolls ($1.00 each way), in essence making
it an access fee or a service fee depending on how you want to look at it.

With a commercial network there's probably greater access to the information
(similar to the dubious information security at credit reporting agencies)
than there would be if it were under government control. Or are they the same?
Is it better to have such "democratically" restricted access? I think so.
It's pretty difficult to get the CIA to release uncensored information that
the (may) have collected about you. With a commercial network you can (attempt
to) hire a cracker and at least be forewarned.

Bill Biesty, Electronic Data Systems Corp., Research and Advanced Development,
7223 Forest Lane, Dallas, TX 75230 (214) 661 - 6058 edsr.eds.com!wjb

---

Deskilling

Peter Brantley <BRANTLEP@ARIZVM1.BITNET>
Fri, 01 Mar 91 09:13:16 MST

Alan Wexelblat notes that many instances of automation are involved in a
deskilling of the workforce. There are many popular images of this effect, and
Alan notes a few. The worry is that this process, extending through society,
will result in a "dumbing" of workers.

This thesis was most forcefully argued, not in Garson's _Electronic Sweatshop_,
which has more to do with surveillance, but in Harry Braverman's _Labor and
Monopoly Capital_. Braverman advanced the deskilling hypothesis as an attempt
to understand what he perceived to be fundamental aspects of workplace
transformation in a particular stage of western capitalism. The facts,
however, do not really support Alan or Braverman.

Braverman described deskilling as a historical process, particularly alive
today within the service sectors. But it is questionable whether the service
sectors have been the targets of a "dumbing." There have been many instances
where computerization has forced the lay off of newly redundant personnel, but
for those who receive or gain control of workplace automation, the story is
different. They often experience a reskilling, or more explicitly, a
redefinition of their job tasks, with even greater required skills. The
operation of machinery does not, and should not, require knowledge of
appropriate intervention, as Alan suggests. Indeed, the very *point* of
automation is to remove these tasks from the province of the worker. But this
is not necessarily a bad thing. Automated workers may or may not be more
happy, but they are not likely to be more oppressed. And as Braverman
accurately noted, the age of craft work -- where you could send Joe to "bang on
it a few times" to fix it are long gone. Braverman did not note that the craft
work population of the U.S. was always *very* small.

Most any business publication discussing the future workplace broadcasts a note
of alarm about the lowering of available skills in the population as a whole.

The requisite skill level for many positions has risen to the point where many large U.S. corporations are unable to find suitably educated workers in the labor force. Massive job training programs have been initiated to give workers a minimum level of technological sophistication necessary to perform their tasks.

The inclination of many writers, Braverman included, to posit a golden happy age where workers knew their work and could fix/own their own machinery is a dangerous misunderstanding of the nature of capitalism. The economic system has extensively organized work for centuries, and automation has only enlarged to scope of this organization. Workers were, are, and will be oppressed.

The danger is in failing to note the increasing skill stratification of the workforce. Those of us who understand technology are a very privileged lot. The workplace demands more extensive skills with each passing year as more information processing becomes required for culturally accepted business practices. If we fail to notice that the U.S. educational and social system does not support the acquisition of these skills, then we have done a grave disservice. This is not something particular to automation, but to our social system. Automation is a neutral force. Society is not.

Peter Brantley, Department of Sociology, University of Arizona, Tucson,
AZ 85721 (602) 621-3804 Brantlep@Arizvm1.BITNET, Brantlep at Arizvm1.Ccit.Arizona.Edu

---

Re: deskilling

Phil Agre <phila@cogs.sussex.ac.uk>
Fri, 1 Mar 91 17:24:33 GMT

In an article in Risks 11.18, Alan Wexelblat (wex@pws.bull.com) mentions the notion of deskilling in relation to computer-based automation. He says:

> Where people have not been outright replaced by machines, they've been replaced by people with lower skill levels and often less experience and less education.

Though I am highly sympathetic to the idea that automation is not frequently motivated by concern about the quality of workers' lives, the matter is fairly complicated. In particular, it would be a mistake to identify automation with deskilling in terms of its effects on the total workforce. (This may simply be a clarification of AW's note.) Rather than go on about it, here are some references which lay out the issues in detail:

William O.~Lichtner, {\em Planned Control in Manufacturing}, New York: Ronald Press, 1924. A fascinating early manual of management rationalization.

Harry Braverman, {\em Labor and Monopoly Capital: The Degradation of Work in the Twentieth Century}, New York: Monthly Review Press, 1974. Origin of the thesis of "deskilling".

Richard Edwards, {\em Contested Terrain: The Transformation of the Workplace in the Twentieth Century}, New York: Basic Books, 1979. A more complex view,

based on the evolving relationship between issues of efficiency and control over the work process.

Barry Wilkinson, {\em The Shopfloor Politics of New Technology}, London: Heinemann, 1983. An ethnographic account of the organizational dynamics of factory automation.

Ann Majchrzak, {\em The Human Side of Factory Automation: Managerial and Human Resource Strategies for Making Automation Succeed}, San Francisco: Jossey-Bass, 1988. A practical guide for managers planning to automate.

Paul Thompson, {\em The Nature of Work: An Introduction to Debates on the Labour Process}, second edition, London: Macmillan, 1989. Good survey of the development of sociological theories of automation since Braverman.

Phil Agre, University of Sussex

Re: Dumbing-down?

Bob Rahe <CES00661@UDELVM.bitnet>
Thu, 28 Feb 91 22:10:00 EST

Alan Wexelbat in Risks 11.18 makes the point of automation of some jobs causing the level of intelligence of the operators hired to do them to be lowered. How can this be ascertained as opposed to the scenario where the quality of the applicants for the job has required a high-tech solution in order to get it done. Have you talked (English!) to a high school student lately? Tried to get into a discussion with one? Definitely on a downward spiral.

Bob

---

dumbing-down and dumbing-up

Edward N Kittlitz <kittlitz@world.std.com>
Sat, 2 Mar 91 07:22:13 -0500

Alan Wexelblat discussed "dumbing down", whereby technology allow less trained people to perform tasks which previously required skilled practitioners. We must also remember that computer-aided processes can inspire contempt in those who are familiar. An example is the oft-discussed failure of skilled persons to follow automated checklist procedures because they know the system "well enough". The best (apocryphal?) example is the Soviet fighter pilot yelling "don't tell me how to fly this plane" to a recorded voice intoning "pull up... pull up". This must be "dumbing up".

PS to Steve Bellovin's note about 25 and 50 feet of wire going for the same price: an inspired bargainer would purchase the 50-foot length, Solomon-style cleave it in twain, and return one piece at the 25-foot price.

E. N. Kittlitz

Search RISKS using swish-e

Report problems with the web pages to the maintainer

Search RISKS using swish-e

THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

ACM Committee on Computers and Public Policy, Peter G. Neumann, moderator

Volume 11: Issue 21

Wednesday 6 March 1991

Contents

Medical image compression & fertile ground for future litigation

"David A. Honig" <honig@ICS.UCI.EDU>
Tue, 05 Mar 91 16:07:01 -0800

I just attended a conference (SPIE, San Jose) that included a workshop on image compression. One particularly RISKy area that received too little attention was the risk of sending medical images using lossy compression schemes. There was much discussion about how compression schemes could exploit the (finite) resolution of the human visual system to send only the info that was perceivable, but no one brought up the fact that what is deemed "detectable" depends upon the tasks that it is measured with. Furthermore, getting closer or farther from an image changes the spatial frequencies present! And of course what radiologists, cardiologists, etc. actually are doing when they're looking at medical images isn't understood, nor are all situations likely to be tested even if a battery of real-life images and experts are used to evaluate compression schemes.

One person *did* bring up the fact that lossy compression might simply be avoided for medical (or other life-critical) images, but there was a lot of the "if you've got a hammer, everything looks like a nail" attitude there and people thought they had a pretty spiffy hammer. A comment was made about how the "corporate types" are highly resisstant to lossy compression of med images in a disgusted, "them damn management anchors" kind of way...

I mentioned to someone that if you had to get your images to your specialist half a continent away that quickly, the expense of several additional phone lines and modems might be considerably cheaper than the cost of several lawyers.... but I thought this fairly obvious...

Flipped and misplaced bits

<jake@mars.bony.com>
Tue, 5 Mar 91 19:23:34 EST

The story of the CYBER clock going crazy after clock-register overflow reminded me of when I was a new CDC systems programmer a very long time ago and found that many earlier CYBERS didn't have memory parity checks and memory (and systems) failed not infrequently.

My first horrified thought was: "You mean all those pipes in nuclear reactors and all those airplane wings were designed on these things and the bits just flip around by themselves sometimes?!" The answer, apparently, was "Yup".

Later I found that FORTRAN code ran faster when compiled so as not to perform array-bounds checking. This RISKy behavior was considered a competitive feature. We even used to joke that we made more mistakes per second than any other CPU on the market.

Preventive maintenance was supposed to avoid memory mishaps and software reasonableness checks and repeated simulations brought such errors to light before it was too late. I hope.

Jake jake@bony1.bony.com

---

telco voice mail snafu

MC CLELLAND GARY <mcclella@news.Colorado.EDU>
Wed, 6 Mar 91 09:49:29 -0700

Excerpt from [Boulder] Daily Camera, March 6, 1991

> A glitch in a computerized telephone answering service provided by US West Communications Inc. of Denver has been plaguing Boulder users for at least a week....The optional service, known as Voice Messaging, has been available in Boulder since the fall of 1989 and operates from phone company headquarters. It enables customers to do without in-home electronic answering machines. [name of local user] said, "it's a nightmare, really. You get it because it's infallible and then this happens." [telco spokesperson] said a faulty device called a translator [??] had been replaced and a team of technicians is watching the system around the clock. Some users said the system had been failing to announce the presence of messages [with a "sutter" dial tone] and announcing messages when there really weren't any.... Billed as a foolproof answer to breakdown-prone tape recorder-based devices, the computerized Vocie Messaging service has more than 1000 subscribers....

[Nothing particularly remarkable about this story. What makes it amusing locally and very embarassing for the telco is that they are in the midst of an aggresive advertising campagin touting the reliability of the electronic system over tape-recorder systems. I should add that I was an early subscriber and that I remain generally happy with the service. At least *I* didn't have to take the *%$^ answering machine someplace to be fixed. System also has decent security features such as allowing the use of long PINS that can easily be changed by the user. But what are we to do about the poor folks who get a computerized service because it's "infallible?"]

Gary McClelland, U. of Colorado mcclella@horton.colorado.edu

Are flaws needed for a standard to succeed?

David States <states@ncbi.nlm.nih.gov>
Tue, 5 Mar 91 22:47:53 EST

The discussion on "doing it right" vs. "doing it well enough" prompts me to observe that many, if not most, of the universally accepted standards in computing are clearly and seriously flawed. A few examples:

RS-232 - cables that costs a small fortune, come in multiple incompatible flavors and require a degree in EE to understand
8088 - We who poke fun now would have been millionaires if we had had a better design back when it counted.
MS-DOS - 640k?, who would ever want more than 640k of RAM on a PC?
Unix - I don't know of a more obtuse collection of abbreviations.
C - One can write intelligible C, it just wouldn't be as much fun.
Fortran - The F word. No *REAL* computer scientists would ever use it, but what a standard.
QWERTY keyboards - What can I say?

Each of these is a widely accepted standard. Each has provoked uncoutably many obsenities, diatribes by the ream, and flame wars galore. Is it random that they are all so far from being the "right" solution? If a standard is really clean, elegant, and free of inconsistencies, it would be too easy. No one would ever have to really dig in and learn the guts of it, and as a result, no one would develop an emotional committment to using it.

A successful standard must avoid building in insurmountable obstacles, but maybe a few surmountable ones are needed to be sure the user is paying attention.

David States

---

carbon versus silicon, Minsky, etc.

George L Sicherman <gls@odyssey.att.com>
Tue, 5 Mar 91 10:02:04 EST

In Risks Digest 11.19, Klaus Brunnstein warns about Marvin Minsky's absolute identification of human intelligence with computer intelligence. I doubt that Marvin Minsky's disinterest in being human is worth worrying about. People who think for a living have always been especially prone to confuse thinking with living. So long as most of us know better, I am content to let thinkers inspire themselves with this error. We need more "mad scientists," not fewer.

I am not impressed by Joseph Weizenbaum's abhorrence of human electrification. Our nervous systems are already plugged in! Every evening millions of people's optic and aural nerves are connected not to reality but to the artistic distortion of reality that appears on television. No physical connection between people and electronics is necessary to create the current disorientation and dehumanization that Weizenbaum dreads as an eventuality.

G. L. Sicherman

A correction (Minsky, etc.)

Richard Schroeppel <r@fermat.UUCP>
Tue, 5 Mar 91 13:42:59 PST

In Risks 11.19, Klaus Brunnstein remarks

> (I now understand why MIT
students were forbidden philosophy in Marvin's time as dean, as Joe Weizenbaum remembers).

I was at MIT from 1964-73, and from my limited perspective as a student, the MIT Philosophy department appeared to be alive and well. I spent several of these years at the AI Lab, and don't recall any discouragement of Philosophy or philosophy. We all spent time speculating about how the mind works. I also don't recall Minsky ever having any position that could be called "dean". Maybe some other time period?

Rich Schroeppel rcs@la.tis.com

Monopoly Security Policies for Thumb Prints (Baldwin, RISKS-11.16)

George W Dinolt <dinolt%wdl45@wdl1.wdl.loral.com>
Fri, 1 Mar 91 18:41:31 PST

Bob Baldwin's comments on ``monopoly security policies'' only scratch the surface of security policy issues and the control of access to data. Even within the Federal Government (sometimes even within a single branch of government) there are many policies for handling the same classified information.

The real issue is that the ``owners'' of information should be able to control it's dissemination. Who owns my ``thumb print?'' I would like to believe that I do, and hence I should be able to tell the state what it can and can't do with it. The problem is that once someone has a copy of my ``thumb print,'' I have no physical control of what they will do with it. A purpose of mandatory access controls in computer systems is to limit that ``copy'' capability.

There is a similar problem with lots of other data about me that unfortunately exists in many computer systems around the country. Currently implemented mandatory and discretionary access controls do not provide the kinds of dissemination controls many of us think are needed to protect that data. (Currently implemented policies probably aren't adequate for the Federal Government either, but that is a story for another time.)

Until (and unless) we articulate the policies about dissemination of personal information, it will be difficult to build systems which will meet those objectives.

George Dinolt (dinolt@wdl1.wdl.loral.com)

Re: But the computer person said it was OK! (RISKS-11.18)

Gord Deinstadt <gd@geovision.UUCP>
Fri, 1 Mar 1991 12:49:30 -0500

Dick Wexelblat (rlw@ida.org) writes:
>Abbreviating a longer interchange:
>Me: I only got one prescription, tear one [receipt] up.
>Clerk: I can't
>Me: Let me talk to pharmacist
[...]
>Manager: I'm too busy to worry about that now.

Report it to your local College of Pharmacists. They will not be amused, since following the correct bookkeeping procedures is 90% of a pharmacist's job.

Many Risks postings reflect situations where a technological breakdown is not addressed because the appropriate agency is not informed. It seems there is a gap between the average person's exposure to Risks and their knowledge of to whom they should complain. What the public needs is for those serving the public to take responsibility; bodies exist (and have existed for decades) to enforce the taking of responsibility; but rarely do the two come together. (And yes, sadly sometimes the regulatory bodies are merely there to whitewash, but I believe most of them are sincere.)

Gord Deinstadt gdeinstadt@geovision.UUCP

Re: But the computer person said it was OK!

Nick Andrew <nick@kralizec.fido.oz.au>
Tue, 5 Mar 91 23:51:17 EST

In comp.risks you write:

>I tried pointing out that that was unreasonable; he shrugged
>and walked away.

>Having a bit of time, I decided to tell the manager. It took a bit of
>explaining to get my point across; one of the two individuals I was speaking to
>didn't understand anything I was saying. After all, the computer had the price
>as the sticker; what was the problem?

G'day,
BTW before you hit 'r', suggest you send your reply to nick@socs.uts.edu.au instead, as Kralizec is temporarily uncontactable from the Internet.

Anyway what I wanted to say in response to your article in Risks is that it is a fairly common thing, so it seems, these days. I can't tell whether it happened much in the past, but it is certainly prevalent today.

The popular term for somebody to whom you are trying to make such a point is "droid". I like the word, it emphasises the kind of robotic behaviour that you experienced. I made up the following definition.

Droid, n:
A person (esp. an employee of a business), exhibiting most of the following characteristics:

* Naive trust or acceptance of something which is patently wrong; blind faith
* An unwillingness to think "outside the 9 dots"
* An "I don't make the rules, but I follow them" attitude
* Unwilling to think "behind" the rules, or go "beyond" them
* No desire to fix that which is broken.

So I guess what you were dealing with there was a bunch of droids running a hardware store. Better find the humans before you start to

complain. (Have you read the Dune books? Early in the first book Herbert makes the distinction between 'people' and 'humans'. A 'human' is not an animal. To wit, (this is Herbert's example) an animal, caught in a trap, would chew its own leg off to escape. A human in the same situation would lie there, feigning death, awaiting a chance to escape.)

I think I'm qualified to recognise a droid, my previous girlfriend was one. Had no faculty for critical analysis whatsoever. She worked for Pizza Hut, and read some magazine article which claimed that Pizza Hut was going to franchise stamps selling from the Post Office (delivery drivers would sell the stamps and other postal things). Instantly believed something which sounded like a crock of shit, with no proof or credibility to back it up, and which appeared in a magazine around early April. Amazing stories, but that's enough reminiscing.

I am entertaining the idea presently that "Society" or western civilization is geared towards droids. So many people at work behave like little cogs in the machine that there must be something appealing in that structure. I guess most of them don't behave the same way (or not to the same extent) outside work, but a certain amount of the droid mentality must always be there. Many of today's laws, and new ones are easy to point out, are there to keep droids under control. Some are to keep prude-droids happy, such as laws against nude bathing.

But I find it hard to reconcile the "droid society" theory with the "cash society" theory, which asserts that the big cogs of the world turn in the pursuit of money, money and nothing else. In short, the pursuit of money explains the entire Gulf War, and nobody moves a muscle without the possibility of making money. Maybe the "cash society" theory on a small scale can be used to derive the "droid society", as it is mostly in the pursuit of money (i.e. at work) that droids appear.

A colleague recently had a similar experience to yours. He tried to pay his phone bill (always a bad move) by phone. Telecom (i.e. the phone company) have two numbers: one for account enquiries and the other for "pay by phone". Clive spent an hour dialling the "pbp" number, which was always engaged. Then he rang the "enq" number and his call was placed in a queue (10 min). Anyway after 5 minutes of conversing with the droid, Clive learned the setup:

* The people on enquiries can do enquiries but can't pay bills
* The people on pay bills can pay bills but can't do enquiries
* Enquiries has a queue handler answering service
* Pay by Phone doesn't

Of course it makes perfect sense to put an answering service on the PbP number as well, so that people can pay their bill eventually, but the droid didn't understand that, didn't know why there was no service, and had no inclination (or authority) to do anything about it. At that point Clive should have tried to go up through the supervisor ranks and got some answers, but he's a busy person and arguing with droids can really waste a human's day if they don't watch themselves.

Anyway take comfort in the thought that you aren't alone & try to stay sane anyway...

Nick.

Automatic patching revisited

Joe Morris <jcmorris@mwunix.mitre.org>
Sat, 02 Mar 91 10:56:20 EST

Several recent postings have discussed the security risks associated with communications applications which can be patched from a remote host without the knowledge of the local user. My reading of these postings is that their entire focus has been on the risks of sabotage; my concern is that another issue has been neglected: configuration control.

If an application is changed without the knowledge of the user, then changes in its behavior may occur...which, of course, is probably the purpose of the (legitimate) download. If the user's use of the system is affected by this, and the user had no reason to expect the system to change, you've got a situation in which that user will probably spend significant worry-time trying to figure out what s/he did wrong *this* time. Lousy PR for the program.

Similarly, users frequently adopt procedures which rely on not-in-specification characteristics of a system. I don't have much sympathy for users who get burned by this *if they were made aware that a change was to be made* (even if they weren't told that the change would affect whatever they were relying on), but it isn't fair or ethical to abruptly change something which the user has reason to treat as local and personal (such as a program in that user's own computer).

Two rather generic examples:

* An operating system invites a user logon with a line containing the words 'PLEASE ENTER LOGON:' and a user writes a script looking for this text. The next release of the system (announced far in advance) changes this to 'Please enter logon:' and the script breaks. Tough.

* The user's communications program is being used to talk to two systems like the one above. The one which is changing to mixed case messages downloads a change to the script to make the text-match string mixed case. The comm program now fails to work with the host which hasn't upgraded its system to use mixed case. Unprofessional and unethical if the host-initiated modification was done without the explicit knowledge and informed consent of the user.

I manage a complex with several flavors of systems (IBM, VAX, Sun). I've got to have records of when changes were made to each so if a system's behavior changes I can reliably determine if a change was made, which of my staff made the change and why. I don't think that it is unreasonable to expect an application to keep at least a bare bones audit trail on the user's system of when changes were made, what the nature of the changes was, and how the user authorized the installation of those changes at the time the change was downloaded.

Joe Morris

Trojan horses and password collectors...some retribution

Joe Morris <jcmorris@mwunix.mitre.org>
Sat, 02 Mar 91 11:11:09 EST

There have been several discussions in RISKS-FORUM over the past years concerning trojan horse programs for host-connected displays, in which the trojan simulates the host OS and invites an unwary user to enter a valid userid and password. The following story, posted on the usenet group alt.folklore.computers, brings up the Gilbert & Sullivan line from _Mikado_, "To make the punishment fit the crime". Joe Morris

==========

From: mike@vlsivie.tuwien.ac.at (Michael K. Gschwind)
Newsgroups: alt.folklore.computers
Subject: Re: Fake operating systems...
Date: 2 Mar 91 14:23:07 GMT
Organization: Vienna University of Technology

In article <95125755@bfmny0.BFM.COM> tneff@bfmny0.BFM.COM (Tom Neff) writes:
>Yeah, and the really big laugh is that while Joe User walks away
>scratching his head at why his usual password doesn't work, the BASIC
>program author is busily accumulating a fat file of real passwords!
>
>Fake shells and OS's are a cute novelty, but they do have their darker
>side.

Yes, they certainly have. A student at the Vienna University of Technology wrote on of those fake login programs which accumulated passwords. Unfortunately for him, the supervisors soon found out. HOWEVER, they did nothing to stop him immediately. They just copied his program.

The next test had some questions about computer security. One question was:

> Explain the following program. Point out how it achieves its aim and
> what potential bugs this program has:

Re: Red and green clocks (RISKS-11.20)

RISKS Forum <CSVCJLD@NNOMED.bitnet>
2 March 91 20:36:25 CST

> [This header is EXACTLY as it was received. I need a Huth Who to figure it out. The message is certainly not "From: RISKS Forum"! It looks as if his mail sender crossed "Mark Huth" with "RISKS Forum". What do you get when you cross a sender with a receiver? Huth paste. What do you get when you cross a sender? Gibberish. Why did the sender cross the addresses? Because it confused the red and green clocks. PGN]

Re: interference to clocks caused by signals superimposed on AC power lines, Paul Leyland asks

>[Can anyone explain why "red" clocks should be more susceptible to this form
>of interference than "green" clocks?]

The older clocks with red LED displays just counted the cycles in the AC power (60 cycles per second in the US) whereas the newer clocks with green (electroluminescent) displays count the cycles generated by a quartz crystal oscillator isolated from the power line by a DC power supply.

Re: Red clocks run faster than green ones!

Henry Spencer <henry@zoo.toronto.edu>
Sun, 3 Mar 1991 02:58:20 GMT

I think the key words are "more sophisticated". That is, I would conjecture a correlation between choice of display and sophistication of the rest of the circuitry. A clock that keeps time based on the power frequency works by counting zero crossings of the AC waveform, and it matters how carefully this is done.

The simplest method is to just count each time the voltage crosses zero. There is an inherent problem here: noise can turn one zero crossing into several, and if the circuit responds quickly enough, it will count them all. The potential for trouble increases greatly if some sort of signalling is also being done over the power lines, because one very popular way of doing such signalling is to send a short burst of data around the time of the zero crossing, when voltage is low and transmission is easy. This almost guarantees multiplication of zero crossings!

A more sophisticated circuit will incorporate safeguards against noise that will also be effective against zero-crossing signalling. One way is to know the approximate frequency of the AC waveform and reject overly-frequent zero crossings as spurious. Another is to charge a storage element from the *peak* of the AC waveform, discharge it at a zero crossing, and count discharges, so that only the first zero crossing after a peak is counted. (I've built both types of circuit.)

LED displays are cheap and easy to drive from digital circuits, so it would not be too surprising to find them in the cheapest clocks. The green displays are probably vacuum-fluorescent types, which are perceived (or at least advertised!) as better for some reason, but need more complicated and costly drive circuitry. So plausibly the green clocks are less cost-critical and get better counting circuitry as well.

Henry Spencer at U of Toronto Zoology
henry@zoo.toronto.edu utzoo!henry

Re: Red clocks run faster than green ones!

Peter Monta <monta@image.mit.edu>
Sun, 3 Mar 91 15:09:55 EST

> New street lighting systems in an East Midlands village have been playing
> curious games with alarm clocks, causing them to race up to four hours ahead
> while their owners slept.

The electrical grid provides a kind of time/frequency service in addition to power---the frequency is accurately held to 60 Hz (or 50 Hz) over the long run, and simple clocks count AC mains cycles.

The problem with electronic clocks is that, if they are poorly designed, they can have much less noise immunity than their mechanical counterparts. The clock on the classroom wall won't care about a 10 microsecond spike on the power line, but a "red" clock may see it as an extra cycle. Lots of spikes, and you have a clock running amok. The new streetlights were probably injecting noise onto the power lines. (Notice that the clock always runs fast---a noise source can't remove cycles, only add them.)

The solution is either a crystal-controlled ("green"?) clock, which must be periodically trimmed to the correct time, or a noise-immune cycle detector. (The synchronous motor in the mechanical clock is such.) I have a 60 Hz source phase-locked to the mains frequency, which is one way to do this electronically, and it's quite interesting to watch the phase with respect to a stable, accurate frequency source. The grid can gain or lose up to a few seconds per day, only to slew slowly back to the correct time during the night to keep the clocks happy.

Peter Monta, MIT Advanced Television Research Program monta@image.mit.edu

---

Re: Red and green clocks

Dave Platt <dplatt@goblin.ntg>
Sun, 3 Mar 1991 12:32:22 PST

> [Can anyone explain why "red" clocks should be more susceptible to this form
> of interference than "green" clocks?]

I'm going to guess that the street-light timers in question might be using some form of RF carrier for coordination and control. The timer might be using a technology similar to the X-10 over-the-power-wires system sold here in the U.S., in which short bursts of low-frequency RF are transmitted over the power lines. Or, it might simply be a matter of some electrical interference (noise) being emitted by the timers.

The X-10 signals are transmitted only during the zero-crossing portion of the 60 Hz cycle. Noise can occur at any pointin the waveform, but certain forms are more likely at the zero-crossing point. Now... most inexpensive AC-powered digital clocks keep track of the time by monitoring zero-crossings in the AC cycle... the long-term accuracy of the AC is better than any inexpensive quartz-crystal oscillator, and it's easy to implement the zero-crossing detector using a Schmidt trigger circuit. My guess is that the signals (or

other interference) transmitted by the street-light timers was of sufficiently high power to spoof the zero-crossing detectors in the inexpensive clocks... this would occur if the amplitude of the interfering signal exceeded the hysteresis curve of the Schmidt trigger. This would cause the clocks to advance more rapidly than they should.

As to why the "green" (plasma-display) clocks are less sensitive to the interference... I believe that the plasma-display technology is inherently more expensive than LEDs, and thus is used only in more up-scale clocks. These more-expensive clocks would have a better chance of having been designed with a more reliable zero-crossing detector... e.g. one which runs the low-voltage AC signal through a low-pass filter designed to prevent interference from spoofing the zero-crossing detector.

Dave Platt, New Technologies Group Inc. 2468 Embarcardero Way, Palo Alto CA 94303 (415) 813-8917 UUCP: ...apple!ntg!dplatt

---

Re: Red clocks run faster than green ones!

Glen Ditchfield <gjditchfield@watmsg.waterloo.edu>
Mon, 4 Mar 91 10:00:59 EST

You probably wouldn't call it "more sophisticated", but I once owned an alarm clock with a green digital display that was basically mechanical. A light shone through a mask and a sheet of green plastic, and an electric motor drove clockwork that slid shutters across segments of the display. Transitions between some digits required a lot of sliding back and forth.

Re: Red clocks run faster than green ones!

Steven King <king@motcid.UUCP>
4 Mar 91 21:03:39 GMT

I don't know if this is the cause for the Castle Donnington problem, but I've seen a similar effect here in the States. My parents were hosting an exchange student from the Netherlands one year. Naturally, the young lady brought her trusty alarm clock with her. She plugged it in one night, set the alarm, and went to sleep. My mom woke to hear MaryLou in the shower around 4am getting ready for her eight o'clock classes! Funny, MaryLou's clock read 6am... Turns out that the clock was pulling its timing information from the line current and, at 60 Hz instead of 50, was running 20% fast.

Is it possible that the same thing happened in Castle Donnington when the new street light timers were installed? Could the timers have been feeding a frequency back into the power lines causing the clocks to run fast? Assuming that's the case, I'd have to guess that "red" clocks commonly key off of line frequency for timing whereas "green" clocks maintain their own independent timers.

Steven King, Motorola Cellular (...uunet!motcid!king)

Search RISKS using swish-e

Report problems with the web pages to the maintainer

Search RISKS using swish-e

THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

ACM Committee on Computers and Public Policy, Peter G. Neumann, moderator

Volume 11: Issue 22

Thursday 7 March 1991

Contents

Digitized signatures for the masses - a not so new risk?

"Albert M. Berg" <0001177220@mcimail.com>
Sat, 2 Mar 91 19:18 GMT

I received a flyer in the mail today that seems to pose a major risk... Orbit Enterprises, Inc. of Glen Ellyn, IL offers to scan your signature into an HP Laserjet format so that you'll "never again sign a letter, memo, note, or any other laser printed document."

This seems to pose a number of threats:

1) If I had my neighbor's signature scanned and then produced a promissory note for $1000 to myself, I could make lots of

trouble for him/her.

2) How do I know that Orbit Enterprises does not have nefarious designs on my signature?

Is it possible to detect a laser printed signature easily?

What is the legality of a laser printed signature?

This has been a potential problem for a long time, but the low cost involved ($60) opens up a new criminal method to the masses.

Your comments?
Al Berg 117-7220@mci.com

City of Montreal to 'access' caller's voices

Peter Jones <MAINT@UQAM>
Thu, 7 Mar 1991 11:00:07 -0500

On Tuesday March 5, the City of Montreal approved a motion to install equipment to record incoming calls to its municipal information service, which is called Access Montreal. A couple of opposition councillors are planning to go to court in order to challenge the decision to record callers' voices. I hope they succeed.

Coincidentally, I also learned from an equipment designer that Bell Canada is planning to introduce Automatic Caller Identification (the caller's phone number is flashed to the called phone between rings using a special modulation scheme). I don't know if callers will be able to block this service.

By combining these technologies, it would be possible to construct a file of which phones called the city, and what was said.

Peter Jones <MAINT%UQAM.bitnet@ugw.utcs.utoronto.ca>
UUCP: ...psuvax1!uqam.bitnet!maint (514)-987-3542

Risks of telco voice mail

<[anonymous]>
Thu, 7 Mar 91 12:30:02

The insidious risks of telco centralized voice mail services aren't really when they don't work--it's when they DO work!

True, nice long PINs being available for the users are nice, but how many people will ever bother using them? Given the choice, most people pick short, simple sequences. One must wonder how many choose 1234 or 4321 as their PINs. It might be argued that given the increasingly short PINs available on newer answering machines (3 digits is typical, 2 is not rare, and sometimes not even all of those digits can be changed by the user) the telco PINs are more secure.

Potentially true, if used properly.

But the real danger is all those nice messages spinning around on the disks down at telco. Of course, we all trust the phone company completely, and when they tell us that nobody will have access to those messages but "authorized persons", we believe them don't we? Sure, encryption systems with the user entering a key could be implemented that would be moderately more secure (though of course, you'd have no way to know that the system isn't recording your keys) but even that level of security is not implemented (nor planned, apparently) in any of the telco offerings.

In any case, telco personnel would never just snoop on people's messages, right? The fact that for years it was common for speakers to be hooked up in central offices so that night-shift workers could listen in on "interesting" lines (just for laughs, right?) shouldn't impact our thinking about today's totally honest and upright telcos!

And of course, nobody who isn't doing something wrong should be concerned about the potential for law enforcement or other agencies to go to telco and demand access to the messages (probably using the same sort of court orders used to do wiretaps in the case of legal taps, and we all know the government never does "illegal" taps--don't worry about the stories in "The Puzzle Palace"...)

But just think--all those nice messages all in one place. And even better, assuming telco keeps (or is ordered to keep) backups and archivals of their data (and what diligent telco wouldn't keep backups?) it could be possible for an agency to go in and not only pick up a person's current messages, but their *past* messages as well, perhaps going back for months or even years! Now that's service!

But these sorts of things would never happen, right? And after all, you *were* able to get rid of your answering machine, and you don't *really* care who listens to your boring old personal messages anyway, do you? And if you can't trust the phone company, who *can* you trust?

Droid Thinking; Schwab Telebroker

HAUSMANN_MADDI@prune
7 Mar 91 16:10:00 +1600

[*prune? Look MAddi, the Tandem Mailer Shrunk Your Address! Nonstop, too. PGN]

The Discussion of droid thinking by Nick Andrew (RISKS 11.21) reminds me of what I went through at Charles Schwab, with the same Telebroker service that was mentioned in RISKS last month.

I too had some problems with Telebroker. In particular, I could not add a stock option to a Stock List (a collection of eight stock tickers). The manual did not explain that options cannot be added. In addition, I wanted to add the ticker for Wang Labs to my stock list. Wang's tickers is WAN.B since the stock is Class B. According to the manual, I should enter it as "WANB", e.g. stock name with the B designation appended. However, this did not work.

I pressed *7 to speak to a representative. While he was able to get the Wang problem resolved (use a space between the ticker and the designator; of course nowhere in the manual is a code for space given), it took quite a few iterations of people to find out that stock options cannot be added to a stock list. Most annoying was the series of questions he asked me. It was clear he was following a standard flow-chart on problem-solving, rather than listening to what I was saying.

Now, having gone through all this nonsense with the Schwab representatives, I went to my local Schwab office and asked for a new manual. They don't have one. So, I asked for a contact who was an expert on Telebroker so I could call that person directly and not deal with the "droids". I thought if I could talk techno-gack-speak directly with a non-droid I'd get some answers. Well, they don't give out contact names. You got questions, go through channels. The office still hasn't gotten back to me on getting a new manual.

I didn't let this drop, though. I dropped a note to the President of Schwab, who I met in my job-seeking days. I included the RISKS posting with my letter. He referred me to the head of Telebroker, who happens to be yet ANOTHER Princeton alum (yes, the old-boy/girl network really DOES work). Maybe I'll have a happy ending to this for everyone, or, at least some fixes to the manual.

Sprint educates customers on risks

David N. Blank <dnb@meshugge.media.mit.edu>
Thu, 7 Mar 91 19:31:01 EST

I received the following letter a few days ago from North Shore Agency ("A National Collection and Debt Recovery Service" as they bill themselves) on behalf of US Sprint Long Distance. The original is in all uppercase, but I'll spare the gentle reader the annoyance. Bad grammar and punctuation is verbatim:

> We know a lot about you, David Blank
> We know where you live. We know your telephone number. In many cases,
> we even know where you work.
>
> After all, that information was requested when US Sprint extended
> credit to you. And you know a lot about US Sprint long distance
> telephone service. Otherwise you wouldn't have placed an order for
> that service.
>
> Since we know so much about each other, how about paying what you owe
> US Sprint. [3 more collection blather sentences deleted]

This was all in reference to a $14.95 sum which had been paid two weeks before the letter was sent. After I spent my anger in a phone call to US Sprint, I realized the humor in the situation. This was an effective public campaign to educate the public in the abuse of a commercial personal information database (an anti-risk, if you will). I hope the US Sprint customers (who aren't

card-carrying CPSR members already) learn that they can be threatened with the very information they gave away to a vendor innocently.

dNb

More hardware risks

"Martin Minow, ML3-5/U26 07-Mar-1991 0932" <minow@bolt.enet.dec.com>
Thu, 7 Mar 91 06:55:17 PST

The personal computer revolution have brought huge amounts of computer power into "ordinary homes." I'm acutely aware of this as I started my career on Illiac-I (1024 words of memory, and a 10K word drum). Now I have a 4 Mips machine (whatever that means) with 8 Mbyte main memory and 300 Mbytes of disk sitting on my dining room table (and it probably costs less than Illiac's daily electric bill).

This has led to an incredible price-crunch in the marketplace, and I'm afraid that quality has often been left behind. Consider SCSI: the drive mechanisms are wonderously reliable, but the interconnection has only single-bit parity error detection. There is no end-to-end data block error detection (on the data bus itself). To make matters worse, some manufacturers are abandoning the standard 50 pin SCSI cable in favor of using a DB-25 "modem" cable. This means that the individual signal wires are not independently shielded, yielding increased cross-talk. They do this in the name of "cost savings." (Note that I am not complaining about the disk mechanisms, but about the boxes they are sold in.)

This problem may be made worse by the proliferation of compression software (mostly built on the public-domain implementation of the Lempel-Ziv algorithm that was distributed on Usenet some years back). One of the negative side-effects of Lempel-Ziv is that a single bit error in the data stream may turn *all* subsequent data to garbage. In a poor implementation, it will also crash the decompression program.

I don't know the right solution to the hardware problem: perhaps Consumer Reports should hire an electrical engineer with an analog oscilloscope (remember analog?) and test end-market SCSI disks. I don't know if there is a decent solution to the software problem -- I don't think "education is the answer" recognizes the reality that the users don't know about computers, and don't care: they're only interested in their invoices and medical records and illustrations and books and love letters.

Martin Minow minow@ranger.enet.dec.com (New address)

Computer insecurity in UK government

Paul Leyland <pcl@robots.oxford.ac.uk>
Wed, 6 Mar 91 15:38:57 GMT

From _The Times_ (London) 5th March 1990

Auditors press for wider computer data security

An audit report published today is expected to say that there have been improvements in how the government administers the security of its networks. Nevertheless, some experts believe there is little room for complacency and that, given the breakneck pace of computerisation of everything from social security offices to the health service, more money needs to be urgently spent.

More than three years ago, the independent National Audit Office issued a warning of the dangers to government computer systems from floods, fires and frauds.

Security and so-called disaster recovery was too low across government departments, with gaps identified everywhere from the Driver and Vehicle Licensing Centre to the National Savings department -- gaps which, it was claimed, put at risk huge stores of confidential and commercially sensitive data and defence information.

Emma Nicholson, Conservative MP for Devon West and Torridge and a former computer consultant, said that the government, its agencies and quangos[1] needed to mirror the spending of industry and commerce on disaster recovery.

The private sector spent up to a fifth of budgets on securing computer systems against fire, floods and fraud, and the public sector should be doing the same, Miss Nicholson said.

The publication of the audit report brings into focus an area of government policy which some experts claim is in turmoil amid concern that a serious review of the way government specifies and buys information technology should be reviewed[2]. It follows difficulties in implementing the computerisation of the social security and health service systems.

Up to eight social security offices are on strike because, it is claimed, the computerisation of the benefits service was made hastily without any notion of the technical difficulties involved. Michael Meacher, the shadow social security spokesman, said.

Some experts believe that the government, which spends \pounds 2 billion a year on information technology, should now consider an information technology minister to oversee the technical ramifications of legislation. The computerised community charge[3], which in some cases has needed more staff to administer than the old rates[3] might never have been passed so swiftly if an assessment of the computing complexities had been made. Others believe that there is a need for a panel of industry experts to advise the government and its own advisers, the Central Computer and Telecommunications Agency.

What concerns some firms is that, in spite of a greater emphasis on competition, it can take up to three years for the government and the agency to approve a system, whereas, in the private sector, the time frame is often a few months.

Footnotes (by pcl, not in the original).

[1] Quango -- acronym for quasi-autonomous national governmental organisations.

[2] This turgid and repetitious phrasing is how it appears in the original.

[3] Two methods of financing local government. Roughly speaking, the "community charge" (popularly termed the poll tax) is a universal charge on adults (with 80% discounts for low income groups such as students, unemployed, etc), whereas the "rates" is a property tax levied on property owners. In both cases, the level of the charge is set by the local government, subject to central government imposed maxima. The old rates system was widely regarded as corrupt; the newer community charge is even more widely held to be unfair. It's not yet clear what an acceptable method of local government finance will be.

---

computer addiction

Phil Agre <phila@cogs.sussex.ac.uk>
Tue, 5 Mar 91 15:42:00 GMT

This book might be of interest. I'll just make a few descriptive comments, but the book deserves a more detailed analysis by someone who knows about the social psychology of addictions.

Margaret A. Shotton, {\em Computer Addiction?: A Study of Computer Dependency}, London: Taylor and Francis: 1989.

A survey-based sociological study of computer addiction. She defines three classes of computer-dependent people (Networker, Worker, Explorer), according to the degree to which computer activity connects with, or displaces, social relationships, with particular attention to marriage problems. The final chapter's analysis presents a more or less conventional account of computer addiction as a safe substitute for social relationships that are experienced as dangerous, by analogy to a variety of other hobbies, such as auto repair.

Phil Agre, University of Sussex

Anthology about social issues of computing available

Rob Kling <kling@ICS.UCI.EDU>
Wed, 06 Mar 91 17:33:08 -0800

Computerization & Controversy, an anthology of articles about social issues of computing (including risks), by Charles Dunlop and Rob Kling is now available.

Computerization and Controversy: Value Conflicts and Social Choices

Charles Dunlop and Rob Kling (Editors)
Univ. of Michigan - Flint Univ. of California - Irvine

Many students, professionals, managers, and laymen are hungry for honest, probing discussions of the opportunities and problems of computerization. This book introduces some of the major social controversies about the

computerization of society. It highlights some of the key value conflicts and social choices about computerization. It helps readers recognize the social processes that drive and shape computerization, and to understand the paradoxes and ironies of computerization.

Some of the controversies about computerization covered in this collection include:

* the appropriateness of utopian and anti-utopian scenarios for understanding the future
* whether computerization demonstrably improves the productivity of organizations
* how computerization transforms work
* how computerized systems can be designed with social principles in view
* whether electronic mail facilitates the formation of new communities or undermines intimate interaction
* whether computerization is likely to reduce privacy and personal freedom
* the risks raised by computerized systems in health care
* the ethical issues when computer science researchers accept military funding
* the extent to which organizations, rather than "hackers," are significant perpetrators of computer abuse

The authors include Paul Attewell, Carl Barus, Wendell Berry, James Beninger, John Bennett*, Alan Borning, Niels Bjorn-Anderson*, Chris Bullen*, Roger Clarke, Peter Denning, Pelle Ehn, Edward Feigenbaum, Linda Garcia, Suzanne Iacono, Jon Jacky*, Rob Kling, Kenneth Kraemer*, John Ladd, Kenneth Laudon, Pamela McCorduck, David Parnas, Judith Perrolle*, James Rule, John Sculley, John Shattuck, Brian Smith, Clifford Stoll, Lindsy Van Gelder, Fred Weingarten, Joseph Weizenbaum, and Terry Winograd. (*'d authors have contributed new essays for the book.)

Each of the seven sections opens with a 20 page analytical essay which identifies major controversies and places the articles in the context of key questions and debates. These essays also point the reader to recent additional research and debate about the controversies.

Published by Academic Press (Boston). 758 pp. Available: March 5 1991. $34.95

ISBN: 0-12-224356-0 Phone: 1-800-321-5068

Individuals may purchase copies directly from Academic Press by calling 1-800-321-5068 or by writing to: Academic Press Ordering Academic Press Wharehouse, Order Dept., 465 S. Lincoln, Troy, Missouri 63379.
[as in SoftWhare?]

Faculty who offer courses about social issues in computing may order examination copies from Academic Press. Write on university letterhead or enclose a business card, and include the following information about your course: class name and number, department, # of students, books used --in the past, adoption deadline.

Send your requests for examination copies to: Amy Yodannis, College and Commercial Sales Supervisor, Academic Press, 1250 Sixth Avenue, San Diego, CA

92101, tel: 619-699-6547, fax: 619-699-6715

Search RISKS using swish-e

Report problems with the web pages to the maintainer

Search RISKS using swish-e

THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

ACM Committee on Computers and Public Policy, Peter G. Neumann, moderator

Volume 11: Issue 23

Sunday 10 March 1991

Contents

IRS agent and information privacy

Unix Guru-in-Training <elr%trintex@uunet.UU.NET>
Fri, 8 Mar 91 23:40:14 EST

New York Newsday, Friday March 1, 1991

"IRS Agent Says She's Penalty-Free", by Leonard Levitt

An Internal Revenue Service agent under investigation by her agency over her contacts with [infamous Bronx defendant in cop-shooting and other drug-related cases] Larry Davis yesterday denied giving confidential tax information to the Bronx murder suspect and said she has resigned her federal job.

[to summarize, the IRS agent was accused of looking up the tax records and home addresses of judges, jurors and detectives involved in Larry Davis's arrests and trials. Why post this on RISKS? Read on:]

[The IRS agent] insisted that she did not get the addresses of court

officials for [Davis]. "I would never go into the master [computer] system. Not that he even asked me," she said.

[So the information the agent is accused of giving out is kept on a computer. Not at all surprising. RISKS readers have known for years that computer database systems often lend themselves to this kind of abuse where authorized people make unauthorized forays into other people's data.]

[The agent] was asked [by the IRS] why she accessed the tax files of [Davis's] sister and brother-in-law, who live in Huntington, L.I., and who a law enforcement source said owed the federal government about $10,000. [The agent's] jurisdiction was limited to [several counties not in Long Island]. [...] It is a criminal offense for a revenue officer to access a tax file outside an officer's jurisdiction.

What I find interesting is that if I've not "read too much" into this article, it would appear the IRS has the ability to tell when its officers peek into computer files they're not supposed to, or at least the ability to find out afterwards if they suspect misdeeds. This kind of audit tracking and control is the kind of stuff CPSR has been asking be put into the NCIC to prevent similiar abuses by police and criminal justice personel. Anyone out there know more about what the IRS uses for their information systems and how they track accesses to it?

glossary:
CPSR: Computer Professionals for Social Responsibility, who track Star Wars and privacy related issues.
NCIC: National Crime Information Center, a nationwide database of stolen cars and outstanding arrest warrants, accessible by state cops and others.

Ed Ravin elr@trintex.UUCP

Secret Service Foils Cellular Phone Fraud

Unix Guru-in-Training <elr%trintex@uunet.UU.NET>
Fri, 8 Mar 91 23:57:30 EST

New York Newsday, March 7, 1991, By Joshua Quittner

The US Secret Service said one of its agents cracked the code of counterfeit computer chips to block a kind of cellular telephone fraud responsible for an estimated $100 million a year in unbillable long-distance calls.

During the past two months, the service has quietly distributed a free software "patch" that blocks unauthorized long-distance calls at cellular telephone switches. The patch is being heralded in New York City, where more phone service is stolen than anywhere else in the country. The first day the patch was put into use in Los Angeles, more than 5,000 illegal cellular calls were blocked, a Secret Service spokesman said yesterday.

[...] The counterfeit chip used by phone cheats exploits a weakness in the cellular telephone system that allows a caller's first call to be completed before the billing status is verified... A legitimate mobile phone has a silicon chip that generates an identification number. When a call is made,

that number is relayed to the carrier, along with the caller's phone number, and the two numbers are compared to establish billing.

However "depending on where you're roaming and how busy the cellular network across the country is, you can make a phone call before that procedure is completed." [Norman Black, Cellular Telephone Industry Association] To exploit that weakness, underground engineers designed a counterfeit chip that generates a different, phoney identification number on each call, tricking [the cellular telephone exchange] into thinking each call is the first.

One illegally rigged phone, confiscated by police in New York City last year, was turned over to the Secret Service, which investigates, among other things, telecommunications fraud. Like a hacker -- a phone computer cheat -- the agent broke into the chip, read the microcode, decoded the algorithm at its core, then wrote a program that would help carriers detect its peculiar pattern.

Dave Boll, who heads the Secret Service's Fraud Division in Washington, said that cellular telephones equipped with the counterfeit chips "sell for as much as $5,000 each". And he estimated that such phones are used to make $100 million in unbillable calls each year.

[The article goes on, to talk about the call-stealing problem being the worst in NYC and how the unbillable calls tied up the network for the paying customers].

It is nice to see a technical issue covered reasonably well in a major newspaper. Even moderately awake RISKS readers will notice that the Secret Service's efforts only help a cellular telephone company reprogram their exchange to recognize one particular random number generator. When the next "counterfeit" chip comes out, probably selling at a higher price, it will no doubt use a different algorithm and the Secret Service will have to do the whole thing over again. It would be nice if someone would expend a little effort to fix the "roamer" system so that it would know a real mobile identification number from a spoofed one; when I use a calling card to make a regular phone call, someone's computer seems to always know if my number is real or not -- what's the problem over in cellular land?

Ed Ravin elr@trintex.UUCP

Telephone risks revisited

Jim Griffith <griffith@dweeb.fx.com>
Sat, 9 Mar 91 22:06:17 PST

We received a telephone bill with a notice of scheduled public hearings on proposed features to be provided by Pacific Bell. The services include:

- Caller ID - a special display device displays the number of the caller.

- Call Return - lets callers dial the last person to call, whether or not the caller actually answered the call.

- Repeat Dialing - when a number you call is busy, it polls the number

until it is no longer busy, places the call, and rings you back.

- Priority Ringing - allows customers to specify a list of "priority" numbers. When someone calls you from one of those numbers, your telephone rings in a distinctive manner.

- Select Call Forwarding - allows customers to specify a list of numbers which are automatically forwarded to another number.

- Call Trace - allows customers to order a trace of the last number called. Information is not provided to customers, but it is held for future use by law enforcement agencies.

- Call Block - allows customers to reject calls from specific numbers.

These features strike me as being both scary and attractive. Certainly, they're intended towards the convenience and protection of the customer. But the potential for abuse is also there. The notice says that the California Public Utilities Commission will be holding hearings around the state to gauge public opinion on the Caller ID and Call Trace features. I can also see where the Call Return feature could be effectively used in place of Caller ID. I suspect this is going to be a hot topic for debate.

Welcome to the age of Big Brother.

Jim

Computer does everything

Robert Mokry <mokry@sirius.ctr.columbia.edu>
Fri, 1 Mar 91 13:26:08 -0500

The Feb 26th issue of the New York Times contained an article about Marist College, a small liberal arts college in New Jersey, that got a large mainframe computer donated from IBM. Here's an excerpt from the article:

> The computer, which might be found at a Fortune 500 company with a spare $10 million, handles tuition bills, class enrollment records, freshman applications, administration records and correspondence, college payrolls and investments, student essays, classroom exams, polling data, student and faculty bulletin boards and messages between professors and students. It handles campus crime records and patterns, investment and marketing plans for hypothetical student companies, all the articles for the student newspaper, faculty lecture notes, campus parking permits, files on every Marist alumnus, all personnel records, every college bill and invoice, every grade for every student in every course, the records for every telephone on the 120-acre campus and communications between Marist and campuses worldwide. Oh, and it holds the library's entire card catalogue and circulation files including when every book is due.

The article praised all these great technological advantages for a small college. The article was headlined "Biggest Brain at this College is Not

Enrolled." Somehow, I would interpret the headline in a different way, perhaps that anyone with any knowledge of computers would not go to this college. I guess that might be stretching the quote a bit, and it's just my opinion.

Some risks that I can think of are: (1) IBM can view and control everything on campus -- this need not even be done in an obviously-illegal way like a wire-tap, since computers need superusers (possibly generously supplied by IBM), and a liberal-arts college is unlikely to have any students who can handle such a complicated computer. (2) Since everything is done on one large computer that everyone has access to, potentially anyone might be able to change anything (students changing grades, for example); sure everything can be checked against written records, but then there's no need for the computer. (3) If the computer crashes, everything crashes and possibly the whole college grinds to a hault.

In my opinion, many small computers are much better than one large computer, because then computers handling unrelated functions (like payroll, grades, and student communication) can be physically isolated from each other, and the computers that are connected together can restrict communications to what is necessary. Perhaps the difference between technological advancement and bigbrotherism is how the computing power is distributed.

Some of these ideas may only be speculation, and I think that most people can think of more problems than I can, so I just sent it in without much comment, leaving potential risks as an exercise for the reader :-).

--Robert

High Tea at the Helmsley in New York City

<TASHKOVI@CRNLGSM.BITNET>
Sun, 10 Mar 91 12:41 EST

My friend and I wanted to pay the $50 bill after enjoying a once-in-a-lifetime (for that price!) High Tea at the Gold Room in the Helmsley New York. She only had enough to cover about 2/3rds of the cost, so I handed that to the waiter and gave him my credit card with the instructions to put the remaining charge on the card.

The resulting confusion was astonishing. The waiter didn't know what to do (and it wasn't a language problem either). He asked his boss, who asked his boss and they finally decided that it couldn't be done. Why? Because the computer system only accepted one method of payment (i.e. cash or credit card) and not a mix of them. Not a very customer-friendly system!

(The reason I had not taken her cash in the first place was because some of it was in quarters! Oh well.)

> [You should have asked for separate checks. But, if there is a "next time", you may need separate tables, if you still want her to pay 2/3. PGN]

Citibank Machines

"David C. Frier {DBADVISOR}" <76702.1417@compuserve.com>
10 Mar 91 08:52:08 EST

My encounter with a Citibank ATM, to which I recently gained access by means of an new link between several ATM nets, left me wondering just who checks the algorithms for these machines: are there any standards?

After dispensing my cash, the large bright screen oriented in the vertical plane announced my account balance in what seemed to my astonished eyes to be characters more than 1/2" high. It did not request my permission to do so, nor did it warn me it was about to do so, nor did it check to see who might be standing with or behind me. It then waited patiently for me to press a key...

...which I did with all dispatch. Now the ATM programmers are obviously readers of Risks and know very well the horrors of receipt printers running out of paper. In an ingenious move to conserve this precious commodity, their next question was whether I wanted a "record." I had to recover sufficiently from my rattled state (after seeing my account balance displayed in a public place for any passers-by to chuckle at) to realize that "record" referred to my printed receipt. Then I had to respond by pressing the correct one of two adjacent keys labelled by the screen "Yes" and "No." Not to mention that determining which key is labelled for which repsonse depends highly on the angle from which the screen and buttons are being viewed: could a user in a wheelchair have seen the "No" key as being "Yes?" I think so. I may try this out next time by crouching low in front of the machine and trying to read the screen from that angle. Passers-by will already be in sufficient hysterics at my balance that they will take no note of my odd contortions.

I leave an enumeration of the Risks as an exercise for the reader.

--David C. Frier, Logical Software, Inc., (301) 358-3100

Re: Medical image compression

<Tom.Lane@G.GP.CS.CMU.EDU>
Thu, 07 Mar 91 15:33:24 EST

In RISKS 11.21, David A. Honig points out risks of using lossy compression schemes for medical images (or, presumably, any other critical application).

I believe the compression scheme involved is JPEG. As leader of a group producing a free JPEG implementation, I've run into the lossy-compression-is-unacceptable mindset quite a bit. I think that in most cases this is a knee-jerk reaction. Why? Because *any digital rasterization of an image loses data* compared to the real world. You lose spatial resolution by reducing the continuous scene to pixels; you lose color resolution by having a finite number of color values (to say nothing of the fact that computer displays have limited color ranges); and in many cases you lose more color resolution by having to

map an image into 256 or fewer distinct colors for display on colormapped hardware. (Or you can trade spatial resolution for color resolution by dithering.) Need I say anything about monochrome (B/W or grayscale) images?

In short, whatever image representation you're using now already loses data compared to the real world. A lossy compression scheme may actually permit more data to be carried. For example, the GIF image format currently popular on Usenet carries only 8 bits per pixel, so quite a bit of color resolution is sacrificed. JPEG compression permits close to 24-bit-per-pixel color resolution to be carried in a file about one-quarter the size of a GIF file, with approximately equal spatial resolution.

The JPEG spec includes a large number of adjustable compression parameters. The extent of compression can be traded off against recovered image quality over a very large range, from thumbnail-sketch quality to below-threshold-of-perception errors. Thus the user has the ability (and responsibility) to decide what is an acceptable error level; a decision which is pre-empted by most older image formats.

I think the true RISK here is rejecting a new technology on the basis of perceived characteristics, without considering the actual characteristics of current technology. If people allow themselves to be dissuaded by the adjective "lossy", they may blind themselves to significant improvements.

Unfortunately, David is probably correct that the lawyers will have a field day the first time a bad medical decision is made on the basis of a compressed image. Never mind about lives that are saved because images are transmitted more quickly, or because more images can be kept on file.

(None of this is intended to claim that JPEG is an ideal solution for all applications; only that thorough appraisal of benefits and disadvantages is necessary.)

tom lane tgl@cs.cmu.edu BITNET: tgl%cs.cmu.edu@cmuccvma

Search RISKS using swish-e

THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

ACM Committee on Computers and Public Policy, Peter G. Neumann, moderator

Volume 11: Issue 24

Sunday 10 March 1991

Contents

---

re: worse is better?

Leslie DeGroff <DEGROFF@INTELLICORP.COM>
Fri, 1 Mar 91 16:53:25 PST

?Does anyone know if its feasible to buy in America a car or truck without a complex fuel injection and computerized pollution control? Is there any reader who would be willing to comment on the feasibility of a simple engine that could meet current California emission standards? Les DeGroff (Degroff@Intellicorp.com)

Re: worse-is-better for the 1990s (Chambers, RISKS-11.19)

Mark McWiggins <mark@intek01.UUCP>
Sat, 2 Mar 91 22:55:55 GMT

Tim Chambers <tbc@hp-lsd.cos.hp.com> writes:

>I'd like to know if examples exist of cases where Right Thing technology *has
>been* compatible with mass markets. I can think of plenty of counter-examples:
>VHS versus Beta ...

This isn't a good example. I don't think there was an appreciable difference in the cost of manufacturing Beta VCRs and VHS VCRs. As I understand it, Beta lost because Sony was too restrictive in licensing it, whereas VHS was easily "clonable."

Seems more a case of "open-is-better-than-closed."

Mark McWiggins, Integration Technologies, Inc. (Intek) 1400 112th Ave SE #202, Bellevue WA 98004 +1 206 455 9935 mark@intek.com

---

worse is better for the 1990's

Tom Brendza <tomb@bellhow.UUCP>
Wed, 6 Mar 91 8:34:11 EST

>Here we are in 1991. The two primary operating systems (at least in volume)
>are representative of O/S technology of the late 1960s to early 1970s (Unix and
>MS-DOS), and the three important languages are C (vintage mid-1960s, i.e., it
>is BCPL in disguise), LISP (vintage late 1950s) and Ada (vintage early 1970s).

If "most important" equates to "largest volume of code" or "most money being spent upon developing or maintaining in", then COBOL and FORTRAN are still the "most important", as these two languages account for 90% of the code that exists in the world today. I think this would lend support to your statement:

Tom Brendza (216) 642-9060 x288 (voice)
..uunet!usenet.ins.cwru.edu!ncoast!ushiva!bellhow!tomb

"Worse is Better" and Standards

Jerry Leichter <leichter@lrw.com>
Thu, 7 Mar 91 08:39:09 EDT

In one of those scary coincidences, shortly after reading the "worse is better" discussion that recently appeared in RISKS, I read an article, "Can the U.S. Stay Ahead in Software", in Business Week (11 March issue). It contains the following quote: "...Japanese rivals see U.S. inattention to quality as a key opportunity. As they did in automobiles and electronics, they are pushing constantly to improve their software. Already, Japanese 'software factories' churn out programs with half as many defects as compar- able American products, according to a study by [MIT]." The Europeans are working in the same direction.

David States wonders if there is some reason why our fundamental computing standards are flawed. For one thing, standards that survive are usually based on "current practice"; given the survival value of "quick and dirty" in current practice, a similar appearance for standards is inevitable.

However, there is a more insidious factor at work. Usually, a standard is based on an already-existing product. However, if the standard were to be made IDENTICAL to the existing product's specifications, the current maker would have a huge advantage. Standards bodies are governed by politics and trade-offs; because of their structure, they are unwilling to give away advantages of this kind. Historically, they always make changes - often, quite minor changes - in order to try to level the playing field among all the participants in the process. This is well known to anyone who's watched the standards game.

What's less well known is the flip side: The participants in the development of a standard themselves will have a major advantage to building products to it. They thus have an interest in keeping the standard obscure and difficult for people outside of the select few to understand.

Now, most - probably the vast majority - of people involved in standards work are NOT trying to make things hard. However, the subtext is there, and it asserts itself in curious ways. For example, watch the Usenet comp.std.c newsgroup. The typical pattern is for someone to ask an obscure question, which generates a lot of debate until one of a small group of cognescenti - who were involved in drafting the standard - point out that a combination of apparently-unrelated constraints from five widely-scattered sections makes "clear" the "only possible" answer. Since the answer is already implicit in the standard as written, there was no need to state it explicitly. In fact, "standards culture" actively DISCOURAGES writing out things already entailed by the standard: Any duplication within the standard might cause problems if the two statements turned out to be slightly different.

I have heard of at least one instance of a DELIBERATELY misleading standard. According to someone who was there at the time, some sections of the Ethernet standard were so written as to make it very difficult for someone to start with the written text and build a reliable multi-port repeater. Oh, once you built the repeater and saw some (rare) errors, you could go back and see that you had missed something - but the process by which the standard was drafted was essentially "Work out private spec of exactly what is to happen; translate back to long list of constraints; remove all redundancy from list, ensuring that at

least one item on list is very obscure and of no apparent importance; publish list - suitably interspersed with other, unrelated discussions - as spec."

-- Jerry

Are flaws neccessary for a standard to succeed?

David Fetrow <fetrow@milton.u.washington.edu>
Wed, 6 Mar 91 19:29:17 -0800

In RISKS 11.21, David States (states@ncbi.nlm.nih.gov) uses as an example of a clearly and seriously flawed standard:

> 8088 - We who poke fun now would have been millionaires if we had
> had a better design back when it counted.

but there were contemporanious chips that were argueably "better" in every respect save one. They were dislike the previous standard: The 8080 (and Z-80). MS-DOS 1.0 and CP/M-80 were very similar and one could (almost) automate converting software from CP/M-80 on an 8080 system to MS-DOS on an 8088 system. I recall that as an arguement given at the time (before the PC IBM had sold a 68000 based lab computer).

In fact this is a stronger arguement for his subject ("Are flaws necessary for a standard to succeed"?) than implying the 8088 was the best of its time.

-dave fetrow- fetrow@bones.biostat.washington.edu

Flaws not needed for a standard to succeed

Dick Karpinski <dick@ccnext.ucsf.edu>
Fri, 8 Mar 91 20:08:36 PST

Most official standards are derived from defacto standards. Indeed, the 8088, MS-DOS, and Unix are only defacto standards. The others mentioned (RS-232, C, FORTRAN (not Fortran), and QUERTY) are all dejure standards derived from prior defacto standards. While I cannot claim that proactive standards like IEEE 754 and 854 are without flaw, I suspect you would have to look harder to find their flaws. This does make them pretty clean, elegant, and free of inconsistencies, but it does not make them easy to implement or even to use. Perhaps there are not many with an emotional committment to using them, but anyone who proposes to build a non-IEEE arithmetic is now required to defend that decision. Few of those defenses succeed.

David States remarks that a better design than the 8088, back then, would have made one a millionaire, but I disagree. The story I now believe is that it was chosen primarily because they could be bought in quantity, not because anyone thought they were better than other contemporary designs. Even MS-DOS was a second choice, allegedly selected because the CP/M crew were unwilling to sign IBM's (probably heavy-handed) non-disclosure agreement. Such are the butterfly wings that so often determine the course of history.

Now, some of these flaws in standards have known roots. In particular, the QUERTY standard succeeded because it slowed down the typist in order to avoid the problem of key jamming. That was so successful that it made typewriters usable, and hence profitable. It is a little hard to object to such success, albeit the standard is decades obsolete and quite deserving of retirement. Present concerns would tend to dictate quite different keyboard layouts to avoid such problems as carpal tunnel syndrome and repetitive stress syndrome caused by the unnatural way ones hands must be held to use the old standard arrangements, even for Dvorack (sp?) key assignments. One new keyboard with palm rests and sockets with four way switches comprising each socket was recently shown on television.

When a standard is derived from a defacto standard, usually several or even many of the deficiencies are cleaned up, but a thorough revision is out of the question. The process doesn't start until the defacto standard is sufficiently widespread to generate enough interest to go through the arduous process of creating a standard. This ensures that many of the participants have already formed emotional committments to specific aspects. Given the concensus rules for standards making organizations, this guarantees that inconsistent aspects will remain in the finished standard.

Dick Karpinski

Re: Risks of naming a node [RISKS DIGEST 11.20]

Paul Fuqua <pf@islington-terrace.csc.ti.com>
Tue, 5 Mar 91 17:26:57 CST

Around 1983, the research group I worked in had a machine whose full name was MIT-FLAME-OF-THE-FOREST. Several FINGER programs around the Internet are said to have broken when they encountered it, unprepared for such a long name.

My present machine has prompted some problems -- "islington-terrace" is too long for its own disk label, so it must boot under an alias and find out its full name later. It used to have the alias "it," until a broken local mailer started sending me all the mail destined for Italy.

Paul Fuqua, Texas Instruments Computer Science Center, Dallas, Texas
pf@csc.ti.com, ti-csl!pf

Re: Risks of naming a node (Akella, RISKS-11.20)

Stephen D Crocker <crocker@TIS.COM>
Sat, 02 Mar 91 20:37:06 -0500

It's not just student hackers who notice an unusual name; routing software can also notice unusual names and favor a node with unwanted attention.

When Aerospace became a node on the MILNET, we needed to register its name along with any acronyms. Unlike many universities and other FCRCs, The Aerospace Corproation has no widely used acronym. In some internal files, the

name is abbreviated to TAC, but we thought that would be a particularly poor choice for a hostname. Aerospace's logo is a slanted capital A inside of a circle, and the company is sometimes referred to informally as the Circle-A Ranch, however, "circle-a" seemed both frivolous and esoteric. Lacking any better ideas, we chose the single letter "A" as the abbreviation and duly registered this with the NIC.

Unbeknownst to us, CMU had been using single letter names as abbreviations for its several internal machines. Within CMU, one could refer to a particular machine with its single letter. CMU's "A" machine was particularly important because it was the mail host. When the Aerospace abbreviation propagated throughout the network, connections intended for CMUA were made to Aerospace. I don't think there was much pain at Aerospace, but CMU's internal connectivity came apart. After a short period of confusion and diagnosis, the abbreviation for Aerospace was deleted, and a new rule was passed requiring at least two letters in an abbreviation.

Acronym Risks

<Brian.Randell@laas.laas.fr>
Fri, 8 Mar 91 10:40:14 +0100

Re: Computer insecurity in UK government (Paul Leyland), in RISKS 11.32

>[1] Quango -- acronym for quasi-autonomous national governmental organisations

My understanding is that Quango is a quasi-official acronym within the UK for "Quasi Non-Governmental Organization". Such organizations are one of the means by which the UK government achieves what in American is termed "deniability", a concept which the UK government prefers not to have a name for!

Brian Randell, LAAS, 7 Ave du Colonel Roche, 31077 Toulouse, France
PHONE = +33 61 336205 (Temporary address, etc., until May 1991)

Re: Red and green clocks (King, RISKS-11.21)

<hugh_davies.wgc1@rx.xerox.com>
Fri, 8 Mar 1991 07:11:38 PST

<...My parents were hosting an exchange student from the Netherlands one year. Naturally, the young lady brought her trusty alarm clock with her. She plugged it in one night, set the alarm, and went to sleep. My mom woke to hear MaryLou in the shower around 4am getting ready for her eight o'clock classes!...>

Actually, I'm surprised at this, since the USA uses 110V AC mains, approximately half the voltage provided in most (all?) European countries, including Holland. Certainly, my electric razor will not run at all on 110V (it just hums to itself). Conversely, of course, plugging in your 110V clock in England will not cause you to get up late. More like immediately in order to call the Fire Brigade.

Hugh.

Re: Droids (Andrew, RISKS-11.21)

Bill J Biesty <wjb@edsr.UUCP>
Fri, 8 Mar 91 09:20:21 CST

Nick Andrew's comments about the risks of citizens being droids reminded me of an article about Japan in the most recent _Whole_Earth_Review_ (No. 69, Winter 1990, "Access to Japan", has a yellow cover with an illustration of a Japanese woman in traditional outfit with a cellular phone).

The article is "E Pluribus Yamato: The Culture of Corporate Beings" by W. David Kubiak.

Excerpts:

"We live in the age of Corporate Organisms. [... They] have wrested the control of the earth from Homo sapiens and supplanted us as the planet's dominant species. It is they -- the multinationals, government bureaucracies, relious hierarchies, military bodies, et. al. -- not individual humans, that generate our era's character, its patterns of wealth and poverty, its technological prowess and ecological peril, its entertainment and political agenda. They have, in short taken over, and nowhere more so than in Japan. [...]

"Like most other traits and preferences in a naturla population, the taste for organizational life is randomly distributed. Some people love hierarchical group existence -- uniforms and rituals, secure routines, superior/inferior relationships, the sense of merging oneself into a larger whole and greater destiny. Others detest it with the majority falling along a normal ditribution curve somewhere in between. [...] "In early Japan as elsewhere the primitive leftists were fractious, independent types who abhorred hierarchy, "extablishments", authoritarianism and just wanted to be left alone. The rightists were joiner types who flocked to the regimented security of the military, clergy, and other bureaucratic power centers. Since even in those days the big bodies grabbed the lion's share of everything, they occasionally rankled the "little people" to the point of rebellion. But because the antiauthoritarian lefties then as now took orders ungraciously, organized poorly, and thus were usually decimated in confrontations, their gene pool slowly began to bleed away. "Japan's most in ingenious contribution to corporatist eugenics was...the samurai's [...] open-ended license to kill any commoner deemed dangerous, disrespectful or offensive [...which lasted over a period of...] 15 generations.[...]

"The Japanese student is trained to not even to question authority, let alone challenge it. The only acceptable behavior is obedience -- total, enthusiastic and if possible brilliant obedience. [...] Most young Japanese can tell you "what is thought" but have great difficulty expressing, or placing much importance on, what they themselves think. This creates an extreme permeability to prevailing authority [...]

"The kobun [a chronic subordinate to the _oyabun_ or _oyakata_ (parent

role/person) who directed their work and lives] and hanninmae ["half helping of man": stunted apprentices...trained to serve useful functions but never permitted to individuate or professionally mature] were cultural antecedants of the compliant salarymen so much in demand in this century.

---end excerpts---

Someone (sorry I can't remember) recently commented in RISKS about the lack of education in this country for dealing with the information needs of the current decade. What happens in Japanese schools happens in American schools but with a different method. I can remember getting a test back in grammar school when a classmate who "didn't do as well" as I did in general and on this particular test complained that he got a much lower grade than I on an essay but had the same content which it did. The teacher made some weak excuse but couldn't deny the facts but didn't change his grade. The almighty curve strikes again.

So if a majority of the students on the hump of the grade curve regularly reiceve this kind of feedback, is it surprising that when dealing with institutions (schools, work, etc) and other droids the droidism gets passed on?

The American educational system (and maybe others, anyone?) seems suited to producing "workers" (accent a la Tom Peters imitation of GM management) and has yet to kick in for the 1980's much lees the 1990's. This decades old trend is made worse by the touchy-feely attitude towards learning that Alan Bloom and the Objectivists (they're not connected) are fighting against.

And while there seems to be a change with science education going more to get younger students interested, most of the money winds up in bureaucracies for political patronage.

New motto: Encourage critical thinking whenever possible!

[I step off my soap box.] Bill

Bill Biesty, Electronic Data Systems Corp, 7223 Forest Lane, Dallas, TX 75230
(214) 661 - 6058 edsr.eds.com!wjb wjb@edsr.eds.com

"droids" (re : but the computer person said...)

Ken Hoover <vu2464@bingvaxu.cc.binghamton.edu>
Sat, 9 Mar 1991 16:00:27 GMT

nick@kralizec.fido.oz.au (Nick Andrew) writes:
>Droid, n:
> A person (esp. an employee of a business), exhibiting most of the
>following characteristics:
> [naive trust, unwillingness to think, follows rules but won't

Just a comment on this:

This is what we (as the public) get when a company decides to spend zillions of $$$ on a neat computer system, and then hires people at minimum wage to use

it.

- Ken

(missing) Parity bits (Cyber, Jake Livni, RISKS-11.21)

*"DAVID B. HORVATH, CDP 8*747/215-354-2468" <HORVATH_DB@scov19.dnet.ge.com>*
Thu, 7 Mar 91 14:05:05 EST

This also applies to many of the IBM PC clones on the market today - no parity bits! The Radio Shack Tandy 1000 series is a good example of this - only 8 bits per byte rather than the 9 in the true-blue IBM PC's.

- David Horvath

Re: Digitized signatures for the masses (Berg, RISKS-11.22)

<jwn2@qualcom.qualcomm.com>
Fri, 8 Mar 91 08:20:20 -0800

Signature rubber stamps have been around for years. A scanned signature is essentially no different. You don't say what if any proof Orbit requires that a client is the authentic bearer of the signature. If Orbit makes that simple requirement, then potential for abuse is _much_ reduced.

> How do I know that Orbit Enterprises does not have nefarious
> designs on my signature?

One can ask the same question about your local office supply store that makes the rubber stamp.

>This has been a potential problem for a long time, but the low cost involved
>($60) opens up a new criminal method to the masses.

The rubber stamp is much cheaper :-)

Laser signatures

"Clifford Johnson" <GA.CJJ@Forsythe.Stanford.EDU>
Fri, 8 Mar 91 09:41:12 PST

> What is the legality of a laser printed signature?

Under the rules of evidence, a document that is signed creates a "rebuttable presumption" of authenticity. (In this context, a "sign" can be any mark attributable in any way to a supposed author; remember, this law *originated* from stamped seals.) This puts the burden of proof of authenticity on the contestor of authenticity. In a civil trial, proof is by preponderance of evidence, but in a criminal trial proof must be beyond reasonable doubt. Thus, laser signatures would always be sufficient to establish authenticity where uncontested; and might carry sufficient weight of proof in a civil case; but

could not by itself provide the degree of proof required for a criminal conviction where authenticity was disputed, though they could contribute in the accumulated evidence.

A laser-printed signature creates a presumption of the signator's responsibility for the the document; but not such a strong one as does a personal signature; and one that is more easily outweighed, in the mind of the trier of the fact, by denials of authenticity made by the supposed author. In other words, common sense prevails in the court of law (at least, it's supposed to).

Digitized signatures and desktop publishing fraud (Berg, RISKS-11.21)

Sanford Sherizen <0003965782@mcimail.com>
Fri, 8 Mar 91 20:04 GMT

Since I am preparing a talk on desktop publishing fraud to be given at an upcoming conference, I find that there are some related issues to Berg's message. Here are some of the risks.

There are a number of instances where signatures are scanned, sometimes without the "owner" knowing that it is happening. For example, many documents are now being scanned in offices, either as part of a records retention imaging process or as part of automating files and forms. The signature is not the target but is incidentally picked up as part of a larger process to control paper or distribute information.

Another example of collecting signatures is found with new business offers. There is at least one bank-by-mail service that advertises that it will process all authorized payments and, by the way, include your signature on each of the payment forms after it is scanned. (The company notes that the process is secure since it is protected by passwords!)

Beyond signatures, however, is the larger issue of copying of documents for illegal purposes. Documents that have been forged through desktop publishing have already been used to collect money. At least one group has been traveling around the U.S. cashing forged payroll checks from a fictitious company that they created on their computer. Fake ID and immigration papers are being sold for $20 a piece. Desktop forgery is joining computer crime and viruses as serious problems of the Information Age.

There is also the related problem of modification of documents, particularly if they are on-line, so that unauthorized changes can be made and distributed on what appears to be authentic and official documents. Employees and others can obtain corporate letterhead and signatures and create "official" documents containing false statements, illegal offers, and libelous comments that are almost guaranteed to cause serious problems for organizations.

Inexpensive computers, laser printers, scanning devices, and desktop publishing technology provide wide opportunities for counterfeiting and creation of fraudulent documents for other illegal or unethical uses. Much of our society's functions are based on a view that documents can be trusted, with the result

that we do not call back the senders of letters to inquire whether they truly did sent the letters. We trust that college resumes are authentic if they look right and come from an authorized source. We assume that most of our paper currency is real.

We even trust that photos are true recordings of events with the result that public opinion is shaped by how wars and political events are brought to us by the media. Yet, these and other documents not only can be created by computer-enhanced technics but copied and changed without indications that there have been changes. Think about how Woody Allen appears in historical events in the movie ZELIG. Read Fred Ritchin's fascinating IN OUR OWN IMAGE: THE COMING REVOLUTION IN PHOTOGRAPHY (Aperature, 1990). See the Office of Technology report INTELLECTUAL PROPERTY RIGHTS IN AN AGE OF ELECTRONICS AND INFORMATION for some of the difficult copyright issues.

>Is it possible to detect a laser printed signature easily?

The authentication of a photo could be known by looking at the negative. Now, not only are there cameras/computers that use disks that do not make negatives and can be reused but a photo can be scanned into a computer and modified so that it can appear as the original even when it is an alteration or forgery. I have heard that the FBI has had difficulty in determining some of these alterations, particularly in a way to prove it in a court of law.

>What is the legality of a laser printed signature?

Once again it is a problem of old law and new technology. The law accepts that under certain circumstances, that images can be replacements for storing original documents. The Best Evidence Rule, the Federal Business Records Act, and the Uniform Photographic Copies of Business and Public Records as Evidence Act are relevant sources. The law will change as there are more challenges and problems come to the surface but that is not a quick process. Yet, if a signature is used by someone other than its owner and the original document gets replaced by a stored electronic document, it may be very difficult to prove that an illegal act has taken place.

So, guard your signatures from scanning and your souls from technology. Otherwise, as the songtitle say, "From the Gutter to You Ain't Up."

Sandy

Sanford Sherizen, Data Security Systems, Inc., 5 Keane Terrace, Natick, MA 01760 USA (508) 655-9888 MCI MAIL: SSHERIZEN (396-5782)

Re: Ownership of Thumb Prints (Dinolt, RISKS-11.21)

David G. Wonnacott <davew@cs.UMD.EDU>
Fri, 8 Mar 91 16:07:22 -0500

Has anyone thought of copyrighting their thumb (and finger) prints? Would this have any legal significance? Would the benefits outweigh the problems, namely (a) that you have sent your finger prints to "Big Brother" already, and (b) you may have to have a copyright notice tatooed on your fingers to enforce your copyright?

David Wonnacott

RE: Thumb print data base

<34AEJ7D@CMUVM.BITNET>
Tue, 26 Feb 91 12:07:54 EST

As described, the CA database is illegal under the ADA (Americans with Disabilities Act) in that it denies services (Driver's licenses, ID cards, etc.) to anyone who DOES NOT have a right thumb.

Re: Monopoly Security Policies for Thumb Prints (Baldwin, RISKS-11.16)

Bill White <bwhite@inmet.inmet.com>
Thu, 28 Feb 91 19:21:13 EST

Actually, the DMV has to treat each of its thumb prints as being as sensitive as might ever become. The way this is stated, the DMV might keep separate databases at different security levels. Consider, however, an accountant who, late in life, changes careers slightly and becomes an undercover investigator for the Federal Reserve Bank, investigating some sort of bank fraud cases by posing as a crooked bookkeeper. This is not really terribly likely, but it is not impossible. The accountant's thumb print would go from not terribly sensitive to highly sensitive.

Bill White

---

more on the American Airlines MD-11s

<smb@ulysses.att.com>
Fri, 08 Mar 91 16:39:54 EST

American Airlines announced today that it is delaying delivery of a second MD-11 jet until some problems with the cockpit computer are resolved. Apparently, the problems cause some screens in the cockpit to ``malfunction''. They did say they feel like they're making progress, though.

Delta Airlines, which has two MD-11s, is happy with them, though they've repaired some ``computer glitches'' and once had to fly back empty from Tokyo to repair something.

--Steve Bellovin

Search RISKS using swish-e

THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

ACM Committee on Computers and Public Policy, Peter G. Neumann, moderator

Volume 11: Issue 25

Monday 11 March 1991

Contents

A pulsar re-pulsed!

"Peter G. Neumann" <neumann@csl.sri.com>
Mon, 11 Mar 1991 14:09:28 PST

The 1989 discovery of an apparent supernova-remnant pulsar, blinking 2000 times per second, has now been attributed to electrical interference from a closed-circuit television camera used to operate the telescope in Chile.
[Source: an AP item in the San Francisco Chronicle, 11 Mar 91, p.A8]

I suppose it would have been much more obvious had it been blinking at 60 cycles (or is it 50 in Chile?), although certainly less spectacular. A little like hearing a loud thumping in a quiet room and discovering it the pulse of your own heart beat? Ah, yes, for you statistical types, we need superANOVA, which would have detected A NO VAriance situation.

Robert Tappan Morris conviction upheld

"Peter G. Neumann" <neumann@csl.sri.com>
11 Mar 91 09:56:14 PST

According to today's N.Y. Times, a federal appeals court has upheld the conviction of Robert Tappan Morris. The original conviction was for violating federal computer crime statutes that restrict unauthorized entry into federal computers. In his appeal, Morris argued that because he had had legitimate accounts on Cornell University computers, he had been authorized to use special mailing programs that transfer documents within networks. In denying that appeal on Thursday, a three-judge panel of the U.S. Court of Appeals for the 2nd Circuit, in New York, said he had exceeded his authorization in using the nationwide computer network.

As has been pointed out in RISKS previously, it is interesting to note that the sendmail debug option, the finger program, and .rhosts require no authorization for their use. Copying an encrypted password file in most vanilla Unix systems requires no authorization. It seems to me that there is still a significant gap between what it is thought the laws enforce and what computer systems actually enforce.

Re: Secret Service Foils Cellular Phone Fraud (RISKS-11.23)

<bart@cs.uoregon.edu>
Sun, 10 Mar 91 16:11:20 -0800

In "Secret Service Foils Cellular Phone Fraud" (RISKS 11.23)
elr%trintex@uunet.UU.NET (Unix Guru-in-Training) quotes:
> New York Newsday, March 7, 1991, By Joshua Quittner
> ... Dave Boll, who heads the Secret Service's Fraud Division in Washington,
> said that cellular telephones equipped with the counterfeit chips "sell for as
> much as $5,000 each". And he estimated that such phones are used to make $100
> million in unbillable calls each year. ...

Let's just arbitrarily assume that cellular long distance costs an average of $100/hour (I expect that's only a little high...). At $5000/phone, that means that each buyer, just to pay for their investment, must make *50 hours* of long distance calls per year, or almost 10 minutes per day! It's possible that there's people out there with that much usage, but *how many*??? If I had to guess, I would figure that $5000 is the max of a distribution with a strong peak somewhere around 1/10th that figure...

Now, assume that the average buyer of one of these devices uses *10 times* that much long distance time -- 500 hours per year. At $100/hour, that's $50,000 per caller, implying 2000 of these phones, each with the same chip, were built to make the $100 million worth of calls. This is probably a *serious* underestimate, but even then, 2000 chips is a pretty impressive underground business!

Not to mention the fact that the $100 million mentioned is almost certainly the value of the calls if they had been purchased legitimately, not the cost to the

phone company of completing them. I would be willing to bet that few of those calls would have been made if they weren't free, and that the cost of servicing these extra calls was substantially smaller than their purchase value.

In case you haven't guessed, I suspect that this "estimate" is just inflated numbers with little real basis intended to make the problem look more severe than it really is. The computer-related RISK, as I've mentioned here before, is that resources will be wasted on overkill solutions to a minor problem because of a lack of technical and social understanding of computer-related crimes, while far more serious problems go unattended.

Anyone have any facts about where the numbers quoted above *really* came from?

Bart Massey

QWERTY urban legend

Mark_Jackson.wbst147@xerox.com <mjackson.wbst147@xerox.com>
Mon, 11 Mar 1991 06:38:02 PST

In Risks 11.24, Dick Karpinski <dick@ccnext.ucsf.edu> writes:

> In particular, the QUERTY [sic] standard succeeded because it slowed down
> the typist in order to avoid the problem of key jamming.

No. The arrangement of the typewriter keyboard into the now-traditional layout *was* intended to address jamming, but by reducing the tendency to jam and not by slowing the typist.

Examine the mechanism of a mechanical typewriter, if you can find one. It will jam if the typebar for character N+1, in approaching the typing area, interferes with the departure of the typebar for character N. The time-window for such interference is greatest for adjacent typebars. The QWERTY arrangement was designed to separate commonly-occuring letter-pairs so that they could be typed more quickly without jamming.

(The "QWERTY-slowdown" legend is widespread. Possibly it was started by Dvorak and his partisans.)

Etaoin Shrdlu <MJackson.Wbst147@Xerox.COM>
[Etaoin Shrdlu, he said, QWERTYously]

Pilot Error - an impartial assessment?

Henry E. Schaffer <hes@ccvr1.cc.ncsu.edu>
Mon, 11 Mar 1991 01:52:13 GMT

A front page article in my local newspaper 3/10/91 from the L A Times (by W. C. Rempel and R. O'Reilly, dateline Seattle) opens with the Madrid Boeing 747 accident in which the captain ignored the "Pull Up" recording and hit a hilltop approaching Madrid - "Official cause of the accident: human error." The

article continues, "Boeing research into three decades of commercial airline accidents found that pilot error was the primary cause of more than 72 percent (compared with 10.89 percent blamed on aircraft failure and 5 percent on the weather.) The article continues with discussion of the Aviation Safety Reporting System, and how its leading complaint is about pilot fatigue, and how Boeing advocates routine review of the flight data recorder to check on the performance of flight crews.

Then, there was a page 12 smaller article, unsigned but from the same source, starting "Early ground warning systems issued so many false alarms that airline crews routinely ignored them ..." There was a short discussion on how Boeing says that these systems are now more reliable and should be followed.

It's good to know that the fox is still watching the hen house, and that the press is approving.

--henry schaffer n c state univ

FEEDBACK on glass cockpits

Martyn Thomas <mct@praxis.co.uk>
Mon, 11 Mar 91 13:45:51 GMT

The CHIRP report on the survey of pilots' and engineers' attitudes to cockpit automation has been published (FEEDBACK No 23, Feb 1991). There will be a statistical analysis in a peper for the Royal Aeronautical Society this month.

They had over 1400 responses to the survey. Overall, the replies were strongly positive. The view seems to be that automation is here to stay and, to quote one response, "...aircraft of this type are meant to be flown automatically for all phases of flight including take-off and landing. ... when [pilots] hand fly they put the aircraft into an abnormal configuration, and cause an immediate and dramatic increase in the workload of the other pilot."

There were criticisms:

"I spent a few years on 757. The moving map gave incorrect position on several occasions, and one time could have been very serious. Danger was avoided by my doing an auto go-around. Twice, all the screens went black for a few (5-10) secs. several times the aircraft turned the wrong way on ILS interception. ... PS. The 757 catchword was "What's it doing now?" Not due to bad pilot inputs, but it made its own mistakes, like several spurious auto go-arounds. ... I don't trust automatics at all."

and finally ...

"The most often heard expression on the flight deck is no longer 'what's it doing now?' but 'well, I've never seen that before' ".

I'll try to get the RAeS paper and post a summary.

Martyn Thomas, Praxis plc, 20 Manvers Street, Bath BA1 1PX UK.
Tel: +44-225-444700. Email: mct@praxis.co.uk

MD-11 glass cockpit

"Peter G. Neumann" <neumann@csl.sri.com>
11 Mar 91 09:55:56 PST

American Airlines spokesman Tim Smith said that in the ``glass cockpit'' of the McDonnell Douglas MD-11, American test pilots noted they ``would see things on the screen where they were not sure what it meant, and the manuals don't tell us.''

[Abstracted from NEW JUMBO JET HAS PROBLEMS WITH ITS COMPUTERS, By SCOTT THURSTON, c. 1991 Cox News Service, 11 March 1991, which also noted two earlier mechanical problems.]

Presumably there is considerable experience required to adjust to this sphere of flying.

Search RISKS using swish-e

THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

ACM Committee on Computers and Public Policy, Peter G. Neumann, moderator

Volume 11: Issue 26

Monday 11 March 1991

Contents

Droids (Re: Andrew, RISKS-11.21)

Michael L. Duerr <duerr@motcid.UUCP>
8 Mar 91 00:33:36 GMT

Droids are a perfect consequence of the "cash society", or capitalism. Capital - money, rich people - seeks to maintain power and control. Freethinking, independent people are too prone to upsetting the status quo. More importantly, they are expensive, since they are individuals instead of a bulk commodity. Engineering is the discipline of reducing production from that which requires a craftsman to that which a droid can do. Computer based systems, cash registers that make change, and countless other high-tech innovations exist solely for the purpose of de-skilling work. Converting production from a dignified act with deep psychological gratification to assembly lines and other droid jobs is a trend clear since the beginning of the industrial revolution.

What are the risks? People with droid jobs that read droid textbooks in school, electrotranquilize on droid TV, read droid newspapers, possess droid ideologies with mouthed droid slogans (A thousand points of light / peace with honor / etc.) lose their facility for critical thinking. This explains why subtle issues like electronic privacy, media monopolies and deregulation mania are now beyond the grasp of average citizens. Our computers think for us, and we can no longer ponder the advisibility of invading Panama / Grenada / Lebanon / Iraq / ... (Droids do make good soldiers, or should I perhaps say cannon fodder.) Droids lack the intellect to analyze the mainstream press and detect propaganda. The steady slip of Western "Civilization" into droidism is perhaps the greatest risk facing us all. We need to value intellect, culture and learning if we are to survive, and if our society is to preserve even a shred of respect for human dignity.

Re: But the computer person said it was OK! (Andrew, RISKS-11.21)

Robert Murphy <bobert@ceili.UUCP>
Thu, 7 Mar 91 12:17:59 PST

Nick Andrew's remarks on "droids" provides an apt name for a phenomenon I'm sure most of us run into with some frequency. Alas, far too many companies and managers prefer droid employees, even in the computer industry. How often have you encountered the following RISKy scenarios?

1. A company wants to create a technically challenging product, but the project has an insecure manager or martinet running the show who only hires droids who are not capable of doing the necessary creative work, so the project fails.

2. A company hires an expert, promising her that the company "wants to do it right". The new employee then discovers that this was only window dressing, and what they really want is a droid who looks like an expert. When the employee tries to exercise her expertise, she encounters bureaucratic obstacles and is eventually ordered to change her "uncooperative attitude." If she is not such an astute political operator as to force the right technical decisions in spite of the obstacles, then she will either leave or knuckle under, and the project fails.

---

cultural adaptation to droids

Bob Sutterfield <bob@MorningStar.Com>
Mon, 11 Mar 91 21:23:40 GMT

The emergence of the "droid" class has led to some interesting cultural adaptations. Someone already mentioned their strategy of asking for the droid's supervisor, then iterating until a human is discovered.

I have found that droids often expect to talk to other droids, so if one creatively molds one's behavior into the droid pattern, often significant advantages can be reaped. For instance, when trying to convince a droid to send me an XXX-component to replace a critical but broken XXX-widget here, I

have been known to resort to saying something like "I sure wish you could get that down to the shipping dock this afternoon rather than tomorrow morning. My boss is breathing down my neck and he doesn't like being told that XXX isn't working." This invariably elicits sympathy in the droid on the other end of the phone, who then tries to help out a fellow droid in trouble. In real life, I have considerable autonomy from my supervisors and whatever flexibility I really need to get my job done (very un-droidlike attributes), but there's no need to tell the droid that. Let the droid think that all the world's a droid, {s}he will feel good about doing something to help another droid, and I'll get my XXX fixed a day faster.

RE: de-skilling (Brantley, RISKS-11.20)

Eric Prebys, CERN-PPE/OPAL <prebys@vxcern.cern.ch>
Mon, 4 Mar 91 16:41:53 +0100

In his reply to Alan Wexelblat's "dumbing-down" letter, Peter Brantley makes two somewhat contradictory statements. The first -

>There have been many instances
>where computerization has forced the lay off of newly redundant personnel, but
>for those who receive or gain control of workplace automation, the story is
>different. They often experience a reskilling, or more explicitly, a
>redefinition of their job tasks, with even greater required skills.

is probably true in many cases, but he then goes on to say -

>The operation of machinery does not, and should not, require knowledge of
>appropriate intervention, as Alan suggests. Indeed, the very *point* of
>automation is to remove these tasks from the province of the worker.

I think that anyone who has had experience with building and/or programming automated systems would strongly disagree with this statement, if for no other reason than that it presupposes infallible systems with infallible users. Indeed, it could be argued that some of the most important "reskilling" required in a highly automated environment involves learning to recognize when "appropriate intervention" is required and what that intervention should be. In many cases, this falls under the heading of quality control, but the required attention to detail is much more difficult to maintain in an automated environment.

As an example, consider an automobile assembly line. In an old-fashioned (i.e. human) line it's difficult to imagine the workers leaving the steering wheel out of every one of the cars they make one day (although one occasionally hears stories like that); however, it doesn't take much imagination at all to picture a fully automated assembly line doing just that (say on Feb. 29 of it's first leap-year in operation), and the problem going unnoticed for some time. What is "appropriate" intervention in this case? While I wouldn't expect a worker to run down and start installing the steering wheels himself, I would certainly expect him to stop production until the problem was fixed---even if his Macintosh screen was still telling him everything was alright.

This is certainly an unrealisitic example, but the point is this: While automation does in general result in fewer errors and frees workers from menial tasks, one should not be lulled into a lethargic state. There is still a minimum level of knowledge about any given product/task that should be maintained. Automobile workers should still know that cars require steering wheels and salespeople should still know that making change requires a subtraction.

-Eric Prebys, CERN, Geneva, Switzerland

Computers and Stoopid Work

Steve Cavrak <cavrak@griffin.UVM.EDU>
Sun, 10 Mar 91 8:36:09 EST

Although I subscribe to the theory that it is cars that have made us stoopid (the more you drive, the dumber you get), I'd like to add the following to the readings on computers and the transformation of work:

Zuboff, Shoshana, @i(In the Age of the Smart Machine: The Future of Work and Power), Basic Books, New York, 1988.

The author makes the distinction between firms that "automate" and those that "informate". Her approach is both historical and sociological - including material from interviews with administrators, managers, and workers.

Sherry Turkel's The Second Self: Computers and the Human Spirit, Touchstone, Simon and Schuster, 1984, would suggest that computers in the right hands can make you smarter. Maybe computers are for kids; adults would be better off without them.

[The Zuboff reference was also noted by Professor Michael Mahoney, of the Princeton History and Philosophy of Science Program (mike@pucc.bitnet), as communicated by David M. Laur <dmlaur@phoenix.Princeton.EDU>. PGN]

Deskilling - reply to Peter Brantley (Re: RISKS-11.20)

<wex@PWS.BULL.COM>
Tue, 5 Mar 91 09:43:50 est

Brantley make some interesting assertions, but he and I fundamentally disagree. Quoted text is from his article in RISKS-11.20.

> it is questionable whether the service sectors have been the targets of a
> "dumbing."

Let's continue to use the word "deskilling" which is a more accurate description of the process. "Dumb" is a pejorative and I only used it as a reference to the discussions ongoing in today's society about the "dumbing down" of such things as news boadcasts, political discussion, etc.

That said, I think the process of deskilling is obvious. The article to

which I responded noted an incident, familiar to many of us, where a clerk was unable to tally or make change or do other normal clerkly activities while hir machine was down. This person is clearly less skilled than hir predecessors. Further, this deskilling results in a loss of service to customers and a loss of revenue to businesses. I hardly thought this a conten

---

Deskilling/Dumbing-down (Re: Brantley, RISKS-11.20)

Jeffrey Sorensen <sorensen@dino.ecse.rpi.edu>
Tue, 5 Mar 91 15:39:23 EST

Peter Brantley, Department of Sociology, University of Arizona, Tucson, on the topic of the "dumbing" of the workforce writes:

> If we fail to notice that the U.S. educational and social system
> does not support the acquisition of these skills, then we have done a grave
> disservice. This is not something particular to automation, but to our social
> system. Automation is a neutral force. Society is not.

While it is unclear how the U.S. educational system could teach the skills required for "automation", more importantly is that automation is not a neutral force. All technologies have characteristics that detemine the nature of their interactions with society. The technology itself determines who will use it, how it will be used, and its effects on individual lives. Even more important is that in the long run, technology determines what types of political forms will emerge to deal with it. To quote from Jerry Mander's interesting book _Four Arguments for the Elimination of Television_:

> "If you accept nuclear power plants, you also accept a techno-scientific-industrial-military elite. Without these people in charge, you could not have nuclear power. You and I getting together with a few friends could not make use of nuclear power. We could not build such a plant, nor could we make personal use of its output, nor handle or store the radioactive waste products which remain dangerous to life for thousands of years. The wastes, in turn, determine that _future_ societies [his emphasis] will have to maintain a technological capacity to deal with the problem, and the military capability to protect the wastes. So the existance of the technology determines many aspects of the society." p. 44

> [...] Workers were, are, and will be oppressed.

Many of the information processing skills that are becoming requisite in our moder society could be better termed meta-skills. Workers today must deal with the great many changes that are occuring at higher rates as new technologies emerge. It is this ability to adapt and learn new skill that is now highly sought in industry. But paradoxically, it is these same meta-skills that make much of the job of management redundent. Information technology allows people to exploit one another's experience and "borrow" the skills required for a specific task. It is possible to design equipment in a fashion that allows unknowledgeable people to operate and fix it, and this is largely the goal of graphical interfaces.

Jeff Sorensen sorensen@ecse.rpi.edu (518) 276-8202

---

deskilling (Brantley, RISKS-11.20)

Phil Agre <phila@cogs.sussex.ac.uk>
Mon, 4 Mar 91 12:33:56 GMT

Peter Brantley's article about deskilling in RISKS-11.20 makes a number of assertions that are not entirely uncontroversial. I would like to flag these here, for the sake of RISKS readers who are interested in the issues and are thinking of doing some further reading.

> The operation of machinery does not, and should not, require knowledge of appropriate intervention, as Alan suggests. Indeed, the very *point* of automation is to remove these tasks from the province of the worker.

This is not a very accurate account of the history. Large numbers of factory workers are, and have been for upwards of a century, in `machine tending' jobs. The prototype case of this was in textile factories, where a single individual would run have to about keeping a dozen or more knitting machines unjammed. Machines go wrong. Eliminating the need for human intervention may be the `point' of automation, in the sense of the managers' ideal, but in practice it is an ideal approached only slowly.

> ... as Braverman accurately noted, the age of craft work -- where you could send Joe to "bang on it a few times" to fix it are long gone.

This is a misleading gloss of Braverman's point. Braverman argued that the age of craft work did not simply drift into obsolescence but was actively brought to an end as part of the process of shifting control over the organization of work. To characterize craft work in terms of sending Joe to bang on things is a caricature, part of the very ideology that justified the whole process -- a process which could have gone in other directions.

> Braverman did not note that the craft work population of the U.S. was always *very* small.

Quite the contrary, an appendix to Braverman's book hotly disputes the assertion that craft workers were never numerous. His argument, briefly, is that statistical assertions to the contrary are based on projecting modern de-skilled job categories back onto the very different processes of work in earlier times. He gives the example of farm hands, whose jobs have grown steadily less skilled over time.

This is not to defend the simple de-skilling thesis, but simply to avoid a shift to an equally oversimplified opposite extreme. The picture is indeed complicated. RISKS readers who are interested in the subject should go hit the literature. The Thompson book I cited is a good place to start.

Phil Agre, University of Sussex

Re: High Tea at the Helmsley in New York City (Tashkovic, RISKS-11.23)

<dave@whoops.fps.com>
Mon, 11 Mar 91 17:17:04 PST

And not a very customer-friendly establishment! Using the computer as an excuse as to why something "cannot" be done is not acceptable, especially at a place like that where exceptional service is the commodity being paid for. The correct response to an excuse like that is "I wasn't aware the Gold Room was part of McDonald's. Please take care of it and don't bother me anymore." If they had had to write out a special receipt by hand that is what they should have done. $50 for tea for two and they're going to tell you the computer's dictating how you can pay. Indeed!

David L. Smith, FPS Computing, San Diego ucsd!celit!dave or dave@fps.com

---

Re: Medical image compression (Lane, RISKS-11.23)

Ian Clements <ian@lassen.wpd.sgi.com>
Mon, 11 Mar 91 08:24:39 -0800

Most physicians (radiologists) will not make a diagnosis based upon digital imagery transmitted to them via phone lines (or which has been compressed in any way). Why? Because a mis-diagnosis may result in malpractice. Most physicians realize that compression results in loss of information so they often wait until the film arrives or until they have a chance to review all the data before making a diagnosis.

Clearly, there are risks other than those associated with data compression which apply to medical imaging systems that rely on computers. An example; software in an MRI system depends on the correct orientation of the patient in relation to the magnetic field (for the purpose of labeling an image). What happens when the magnet is incorrectly installed?

Ian Clements ian@sgi.com 415/962-3410

Re: Medical image compression (Lane, RISKS-11.23)

<davidsen@crdos1.crd.ge.com>
Mon, 11 Mar 91 09:03:19 EST

We've had this discussion before. As a person who has had medical imaging and who has worked developing medical imaging software for CAT and ultrasound, I don't buy the idea that if the original image is not perfect it is okay to degrade it further.

bill davidsen (davidsen@crdos1.crd.GE.COM -or- uunet!crdgw1!crdos1!davidsen)

Apathy and viral spread

Rob Slade <p1@arkham.wimsey.bc.ca>
Sat, 09 Mar 91 21:05:01 PST

Recently, Stratford Software has started a new online information service called SUZY. (The service is active in Canada, and is in beta testing for users in the United States.) SUZY operates along lines similar to those of the Prodigy service and the PLC BBS network in that "vendor" supplied software must be used on both host and terminal; you cannot just dial up SUZY with your favourite communications package. This has allowed Stratford to market SUZY as the ultimate in "user friendly" services; the user does not need to know anything about protocols for connection, the "terminal" software deals with all network connections and everything from installation to email is done with a menu driven interface. (It is now even "rodent compatible.")

(Lest I be seen as too enthusiastic here, I suspect everyone on this group would find the lack of functionality somewhat restrictive. Long time net users will demand features it can't yet provide, but it certainly is the kind of system that any "naive" user could access without difficulty.)

I manage the data security/anti-viral topic area (referred to as an "Information Network", or "IN") called INtegrity. Any SUZY user can look at the information in the INs, but, as they "leave" the area, they are asked if they want to "join". This simply puts them on a mailing list that can be used to send announcements to the "members" of an IN. If they want to "join", they hit <ENTER>, if not, they hit <ESC>.

Using figures from a month ago, the number of SUZY users who have joined INtegrity stood at 170. Some others will have dropped in and looked around, but deliberately left themselves off the list when they left the IN. (We "INkeepers" have no access to that information.)

The number of accounts on SUZY a month ago at about 6000. However, research I have done indicates that less than 15% actually use the system more than once a month. Interestingly, this figure has remained unchanged since SUZY was released. That means that less than 900 accounts were "active" at the time.

What does this mean to you, and to data security? It means that less than 3% of all, and 20% of *active* SUZY users care enough about data security to join the anti-virus IN. This is the *real* reason that computer viri are so widespread today: people do not realize the danger.

Those of you who have studied viral characteristics, and virus protection and functions, will realize how easy it is to protect yourselves against most viri. But if the majority of users think they are safe, and do not take *any* precautions, then viri have a fertile breeding ground to grow and spread in. As my wife says, it shows not only how few people understand technology, but how few even understand the concepts of public health.

I have been careful about identifying my affiliation, and describing the situation for a reason. When I first posted this on VIRUS-L, I got flamed by someone who someone who said my observation was invalid because a) SUZY is a pay system, b) he knew of at least three BBSes where people were interested in viri and c) my IN wasn't any good anyway.

SUZY is a commercial system, and this is the reason I chose it for my figures. It is marketed to both home and business users, and therefore gives a better "cross section" of the "whole" user community, not just the "home users and hackers". It is also promoted as "the system for the rest of us" as Apple would say, and again provides access to novice as well as expert users. (Weighted a bit heavily to the novice side, but then so is the general user community, wouldn't you say?)

I know of a number of local BBSes that cater to interest in viral programs as well. I support three of them myself. But I selected those boards on the basis of their interest, and it would be very strange if the user population there represented the general population. By the sales figures, those who use a modem at all almost automatically put themselves in the upper 10% of computer users.

(Am I going to take John's advice about improving my IN? I'd be delighted. Unfortunately, it seems he doesn't use the system. Odd ...)

I am coming to find, though, that it is often the "experts" who give those of us who are working in this field the most trouble, vis this recent exchange:

Message #1678 - Anti-virus forum
Date : 07-Mar-91 19:24
From : Stephen Fryer

SF> I mostly have problems with the computers the instructors
SF> use; instructors are at least as good at spreading viruses
SF> like Stoned since many of them seem to think their more
SF> exalted status (socially and educationally) makes them
SF> immune to such things.

My response? Oh, yes. I've seen this all too often.

Actually, I'm not so sure that it's as much conceit, as a kind of frightened fatalism. They probably are aware that they don't know much about virus protection, but in this business everybody has to be an expert on everything, so they just ignore it and hope it will go away. Strange reaction in my view, but then again, how do they get the facts? Courses are few and far between, and most of the books are not very strong on how to protect yourself (besides being "technically" out of date the instant they go to press.) Forget the media. (InformationWeek printed only four articles on viri during 1990. Computing Canada published a "Computer Security" issue in November of 1990, and printed only two articles on viri, both so general as to be almost useless. I had submitted five articles to CC for that issue, and the one they picked was on how to "define" a computer viral program.)

But again, I agree with Stephen's assessment; it's the "experts" who are often the greatest problem. (Last government office I worked in, the first disinfection I had to do was on the system support operator's machine. He had infected himself while trying to do a disinfection for someone else! Recently, in teaching in a microcomputer lab at a local school board I found that two computers were infected. I informed the lab manager, with some difficulty, and returned the next week to find that not only were they not disinfected, but a third had joined them.)

I mean, with respect to information on computer viral programs you can't *give*
it away. Quite literally. Cheap courses I give through local school boards
get cancelled due to lack of registration. Mid-priced courses I run through
the Federal Business Development Bank just squeak through. It's the expensive
ones that the Center for Advanced Professional Development has me do that reach
the "break even" point for registrations two months before the course dates.
(So if you *have* to swap disks with someone, make sure he's wearing an
expensive suit. :-)

This is the first time since I started working with computers that the attitude
of the general public has really had me baffled. People must surely realize by
now that viri are real, not just the "scare tactics" of the security industry.
The two biggest problems the world faces today are ignorance and apathy. But
people don't know that, and they just don't care ...

Vancouver Institute for Research into User Security, Canada V7K 2G6
Robert_Slade@mtsg.sfu.ca (SUZY) INtegrity

Search RISKS using swish-e

THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

ACM Committee on Computers and Public Policy, Peter G. Neumann, moderator

Volume 11: Issue 27

Wednesday 13 March 1991

Contents

Incredible backlog of RISKS contributions -- Risks of RISKS again

RISKS Forum <risks@csl.sri.com>
Wed, 13 Mar 1991 17:21:44 PST

OK, folks, I have never before asked you to slow down in your contributions, and am not about to do so now. Perhaps the evident lag time will help to do that naturally. But the recent volume of mail to RISKS is horrendous -- on droids, dumbing-down, qwertyuiop, EMI (as of 2 March), warranties and free software (as of 28 Feb, with a double-size issue's worth of stuff still backlogged waiting for my immoderation), etc., all under consideration. (And BARFmail is on the increase again, for no apparent reasons, just the usual net flakiness, people moving, host names changing, FROM: addresses TO which I cannot even answer your mail, especially unregistered portions of UUCP, etc.).

I was away most of today and noticed that my backlog of UNSEEN NEW messages was over 100, and the backlog of UNSEEN messages was about almost twice that, just over the past few days. Thanks for all your enthusiasm!

On an old subject, I get complaints from some of you when I do NOT use draconian pruning shears, because you would like to rely on my moderation to be incisively oriented toward exciting and really interesting material, so that you do not have to wade through the less interesting stuff. But what is interesting to some may not be interesting to others. I also get queries from some of you when your message has not appeared after a while. I know I cannot please everyone, but I'll continue to try to do the best I can. I am currently batching heavy-response items together into self-contained issues, so that if you are bored with the topic you may simply ignore the entire issue.

I long ago gave up trying to acknowledge every message. If you really want to make sure a particular message got through or try to wedge it out of the queueueueueueueue, please feel free to do so. Otherwise, please just have patience. Thanks. PGN

New Utility to Unlock Passwords

"Martin Minow moved to LJO2-A2, RANGER::MINOW" <minow@bolt.enet.dec.com>
Tue, 12 Mar 91 08:45:47 PST

>From MacWeek, Mar 12, 1991: [edited for space].

"New Visions Limited Partnership last month shipped a new [Macintosh] password-recovery utility called MasterKey.

"MasterKey comes in three versions [for WingZ, Excel, and WordPerfect 1.0]. ... MasterKey is intended for use by law-enforcement agencies to access files belonging to drug criminals, embezzlers and terrorists; by companies to access files that disgruntled or terminated employees have locked; and by users to access their own files.

"Features ... include the ability to rever passwords from MS-DOS files, [and] an access code to prevent use by unauthorized users...."

I rather like the fact that they decided to password-protect their utility: maybe I should write a utility to break their password scheme!

Martin Minow minow@ranger.enet.dec.com

Medical image compromise

Roy Smith <roy@alanine.phri.nyu.edu>
Tue, 12 Mar 91 11:56:07 EST

Slightly off the original subject, but I noticed in a recent visit to a hospital that in the public hallway outside of the CAT/MRI scan area were open rack upon open rack of magtapes, no doubt containing images of patients. It struck me that anybody could just pick up a tape and walk off with it. Surely they would not be so sloppy with "official medical records". My guess is that it never really occurred to them that these tapes are part of the medical records, just as surely as the bit of paper charts the doctors scribble in are.

-- Roy Smith, Public Health Research Institute 455 First Avenue, New York, NY 10016 roy@alanine.phri.nyu.edu -OR- {att,cmcl2,rutgers,hombre}!phri!roy

[Clearly not an integrity concern, but it could be a privacy concern if some eager journalist stole a tape, or a denial of service concern if the tape goes astray. PGN]

MCI's Computer Said It Is NOT OK

Li Gong <li@oracorp.COM>
Tue, 12 Mar 91 17:56:09 EST

I wanted to subscribe to MCI's three major calling packages: Prime Time, Call Europe, and Call Pacific. I was told by MCI representatives that I couldn't do so because their computer couldn't handle the complicated billing computation. The maximum is two packages per account.

Li Gong, ORA Corp, 675 Mass Ave, Cambridge, MA

Examinations by Phone

James K. Huggins <huggins@zip.eecs.umich.edu>
Wed, 13 Mar 91 11:32:53 EST

With the recent discussion on voting-by-phone in RISKS, I thought the following (excerpted) article, taken from "U.: The National College Newspaper" might be of interest to readers.

"Test Taking Goes Touch-Tone": Seema Desai, _The_Daily_Pennsylvanian_ (student newspaper of the University of Pennsylvania)

At Governors State U., a wrong number can cost students more than a quarter. It can cost them their grade point averages. The small university near Chicago recently adopted a telephone system that lets students take multiple-choice exams over a touch-tone telephone.

Donald Fricker, a management professor who spent about two years developing the application, said students call a special number and respond to recorded multiple choice questions by pressing digits on their phones. The system, named Big Mouth, has been in operation since this fall, and four professor currently use it to administer exams. Fricker said more than 100 students in classes ranging from psychology to management have taken exams on the system, adding that most students have responded positively to the new technology. [student and faculty testimonial deleted]

Some students and faculty have raised concerns about abuse of the system. Currently, students have to enter their social security number to access the system. Students are on their honor not to cheat, Fricker said. And because students have only five seconds to answer, Scherzinger said cheating is difficult. [quote deleted]

In the near future, Big Mouth will have the ability to repeat questions and accept short essay answers. Fricker said he also plans to add more security measures to the system, including offering multiple versions of exams and giving each student a special security code. [...]

Despite some of the system's drawbacks, Scherzinger said he thinks it will gain wide acceptance in the academic community. "I personally believe that the system will come to every college within the next 10 years."

The RISKS here are abundant: students hiring other students to take their exams for them (a risk that is somewhat minimized by an in-person exam) using their identification number, students deliberately using someone else's Social Security number to flunk the exam for them, and students recording the exam as it is being given in order to distribute copies to their friends.

I hope Big Mouth never comes to Michigan.

Jim Huggins, Univ. of Michigan (huggins@zip.eecs.umich.edu)

[This is getting to be an old-hat topic. But it will recur. PGN]

Confident Extrapolation of Worst-Case Failures

Anthony E. Siegman <siegman@sierra.stanford.edu>
Tue, 12 Mar 91 11:39:51 PST

>From Henry Spencer at U of Toronto Zoology ...
> because we must rely on such extrapolation and we already do;
> the questions are how best to do such extrapolation and what
> form of testing must be done to permit confident extrapolation.

Surely it's also very important to assess the magnitude of the damage that could be done by overconfident extrapolation.

Failure of a large airliner due to some unanticipated worst-case behavior (e.g., the early Comets) will kill at most a few thousands (in the air and on

the ground).

(I suppose a really worst-case failure in which an airliner comes down in Yankee stadium could kill several tens of thousands; but one can at least estimate with fair confidence the probability that a falling airline will hit Yankee Stadium.)

[Shea, Hey, Willie?]

In any event one can accept this level of tragedy and then use it to improve the system. Indeed that's more or less how large-scale civil aviation has made progress. The ``confident extrapolation'' in this instance, based on several decades of experience, is really that unanticipated worst-case behavior probably WILL happen; and one is nonetheless willing to accept this risk.

Worst-case failure of a nuclear power plant in Sacramento, California, on the other hand, could render the entire San Francisco Bay Area uninhabitable for generations if not centuries (perhaps I'm exaggerating here, but it's hard to be certain). In any event, an really ``confident extrapolation'' that this worst-case event can't happen may be near to impossible; and past performance (Browns Ferry, Three Mile Island, Chernobyl) may lead one to have doubts about the ability (or wisdom?) of those who put such forth confident extrapolations.

This is NOT an anti-nuclear message; I merely wish to make the points that:

1) The conservative confident extrapolation, based on past experience, may be that in most cases a worst case failure IS LIKELY to happen.

2) The most crucial question then is not "Will it happen?", but "Can we live with it, if it does?" (or "when it does").

--AES

Re: A pulsar repulsed! (RISKS-11.25)

Matti Aarnio <mea@mea.utu.fi>
Tue, 12 Mar 91 23:35:20 EET

> The 1989 discovery of an apparent supernova-remnant pulsar, blinking 2000
> times per second, has now been attributed to electrical interference from a
> closed-circuit television camera used to operate the telescope in Chile.
> [Source: an AP item in the San Francisco Chronicle, 11 Mar 91, p.A8]

Interesting that this item has now surfaced thru AP. This was news item on Sky & Telescope magazine a few months back when it was debugged. (Reported around August-90?) What your extract doesn't tell is whether or not SFC mentioned it was a suspected OPTICAL pulsar -- which vanished next night. (No radio pulsar has been detected either.)

It is very difficult to measure small but fast variations on very low levels of light intensity.

Long lags from news to their appearance in newspapers seem to be common, also time lag and amount of errors correlate positively. Maybe feeding some

RISKS to papers like Datamation would help? (I doubt they know what ACM is..)

> I suppose it would have been much more obvious had it been blinking at 60
> cycles (or is it 50 in Chile?), although certainly less spectacular. A little
> like hearing a loud thumping in a quiet room and discovering it the pulse of
> your own heart beat?

Or faint ticking at 2Hz, and you start to suspect bugs until you notice your watch... Anyway, it tells that while we use complex systems we must be carefull to spot all possible interference sources before we jump to conclusions. (Aren't we always?)

About two weeks ago I saw on national TV news something telling that Australian radio astronomers had spotted an "ET" signal (me: immediate frown), but the way it was told on TV (as their "ending joke"), associated picture material etc., gave me conclusion: this is a red herring, forget it.
"Hey, lets tell this joke from Down Under about those Radio Astronomers..."
(Maybe 15 seconds total.)

Today I went to do some UNIX system maintenance at the University of Turku Astronomy departement. Professor asked if I had heard anything about those Aussies, because local commercial radio wanted to make a program about this ET signal, and to interview some local radio astronomer...

Our problem? No word about it from verifiable sources, thus do we dare to dip into USENET to fish out POSSIBLE information about it?
(I hope there is information, but I doubt it... Good luck for SETI anyway!)

/Matti Aarnio <mea@utu.fi>

EM solution for new buildings - risk solved?

"Olivier M.J. Crepin-Leblond" <UMEEB37@vaxa.cc.imperial.ac.uk>
Mon, 11 Mar 91 18:07 BST

I have read in this month's British Airways Business magazine that Pilkington's, the UK's glass manufacturer has attempted to tackle the problem of electromagnetic spying with a new "shielded" glass.

The glass sheets are similar to the ones usually mounted on new sky-scrapers, with a shiny surface. However, this metallic film can be tied to earth, thus providing shielding which stops any electromagnetic radiation from leaving the building. It is therefore impossible to hack inside information from outside by picking-up electromagnetic radiation. Solutions were very costly up to now, with actual physical shielding of the building using metallic plates etc.

Olivier M.J. Crepin-Leblond, Comms.Sys., Imperial College, London, UK.
disclaimer: I am NOT related to Pilkington Glass or British Airways in any way !

Cellular surveillance

Les Earnest <les@Gang-of-Four.Stanford.EDU>
Wed, 13 Mar 91 13:55:56 -0800

I am seeking information on current practices and prospects for the use of cellular telephone systems in surveillance of individuals.

1. Given that the telephone companies have traditionally facilitated the tapping of individual telephones by law enforcement agencies if a court order has been obtained, I would assume that most cellular telephone systems have been instrumented to provide this capability. True?

2. Given that cellular telephone systems must track each individual instrument as it moves between cells (by checking relative signal strengths at cellular receiving stations) and given that phones can be tracked even when they are not in use, it would be a simple task for the cellular computers to record a time log of the movements of any selected phone. Has this capability been included in the software of these systems?

3. By using signal strength information from more than one cellular receiving station it is possible to estimate the location of a given phone more accurately than just which cell it is in. With existing equipment and signal strength accuracy, what is the typical positional accuracy of this estimate?

4. Motorola's planned Iridium system is expected to provide global cellular telephone service via 77 satellites in polar orbits. What kind of positional tracking accuracy will that system be able to provide on individual cellular telephones?

Les Earnest, 12769 Dianne Dr., Los Altos Hills, CA 94022 415 941-3984
Internet: Les@cs.Stanford.edu UUCP: . . . decwrl!cs.Stanford.edu!Les

Cellular phone usage

<[anonymous]>
Mon, 11 Mar 91 12:05:23 XST

A recent poster questioned the cellular phone fraud loss figure mentioned in RISKS. He seemed to feel that 10 minutes/day/person would be a large amount of usage for cellular phones. In fact, this would be a very modest usage!

While many cellular phone calls are short, many are VERY long, with individual calls longer than an hour not at all rare. Many people sit on those things all day long, making call after call. Whether the duration and number of calls is related in any way to whether or not the user is paying for the call or committing "cellular fraud" is difficult to determine from the "outside", of course. But persons who have "accidently" tuned in cellular conversations will tell you that it is amazing how many of the calls are such things as long, intimate chats between couples, people with handheld phones chatting with others for hours on end, lawyers talking about cases, etc. Not to mention the drug and prostitution rings (the latter two groups are BIG TIME users of cellular systems--and may well be among the more likely to be operating modified, illegal phones).

There also seemed to be some concern that many of the calls would not have been made if the person weren't stealing the service. This is no doubt true, but there aren't many other obvious ways to quantify loss other than the unbillable amounts. The same could be said about toll fraud and intellectual property thefts.

Re: Re: Secret Service Foils Cellular Phone Fraud (RISKS-11.23)

Ed Hall <edhall@rand.org>
Mon, 11 Mar 91 18:13:24 PST

Who said anything about long-distance? A $5000 bill for cellular calls wouldn't be that hard to accrue for someone who spent a lot of time on the phone. Remember that you have to pay to *receive* as well as make cellular calls.

I can think of one occupation where a person might receive dozens of calls a day, and where the anonymity provided by the counterfeit chips would be a big plus. In fact, this particular occupation might also afford a ready connection to the underground market for such devices, and its practitioners wouldn't be likely to worry about their illegality. You've probably guessed the occupation I'm thinking of: drug dealing. Indeed, cellular phones have replaced pocket pagers as the major technological tool of the "upscale" retail illicit drug trade. Considering the size of the drug trade in a city like New York, $100 million in calls a year sounds like a reasonable estimate to a city-dwelling layperson like me.

-Ed Hall

Secret Service Foils Cellular Phone Fraud (bart, RISKS-11.23)

P.J. Karafiol <karafiol@husc8.harvard.edu>
Wed, 13 Mar 91 20:04:56 -0500

Let's be real for a second. When was the last time you made a phone call to a friend that was less than ten minutes?

It's very easy to talk for five minutes at a go. The few people I know who have cellular phones use them for an average of ten minutes a day, if they can afford it.

Someone who plunks down $5000 for a modified phone can afford it. Not because he has $5000 to plunk down, but because he has free phone service.

I'd make ten minutes of calls a day if they were free.

I'd make a couple of hours of calls a day if they were free.

I have friends all over the country. I can't afford to call them. But if I had a modified phone, I could. I would say, "Hey, I wanna talk to mike, let me get in the car ..."

Of course, I think using phones like this *is* theft, and not something I would do at all. But I'm trying to get across the salient facts here.

== pj karafiol

Telephone risks revisited (Griffith, RISKS-11.23)

W.A.Simon <alain@elevia.UUCP>
Tue, 12 Mar 91 18:07:52 EST

All of the listed features really are one: calling phone identifies itself or is identified for us by the telco. This one feature is used to provide n services. [...]

> Welcome to the age of Big Brother.

Big Brother is a state of mind which belongs to bureaucrats, in government as well as in private enterprises. It was always there. Technology is now such that their particular vice can easily be satisfied. But don't kid yourself, Big Brother was always watching. Instead of fighting it, why not setup social and legal structures which will negate the benefits of snooping? Examples:

* Let's make wiretapping legal; this way, we know and we expect our communications are monitored. We can always invest in cryptographic systems. And we can listen to the cellular calls of our politicians (:-).

* Our medical files are violated by law enforcers as a matter of routine. Employers are not far behind. Insurance companies are misusing this same information. Government agencies are unable to protect it against leaks. And, big insult, I am not allowed to see the file my own doctor keeps on my subject. Therefore I propose all medical files should be made public. If I am discriminated against by an insurance company for smoking pot, why should their president be sheltered from the public revelation that he is a drunk and a wife abuser?

* All of my past employers know about my checkered past. I know nothing about theirs. Why should their resume be confidential? I ask that human resource departments make all resumes public.

* Police and politicians keep tabs on our every move through passport controls and credit cards. But politicians travel with diplomatic passports and they use assumed names to protect their privacy. My credit history (yours too) is known by so many people that it would make little difference if it were made public. I ask credit records be made public and that borders be opened.

Etc...

What makes our privacy so fragile is that we value it; it makes us vulnerable to B.B.: being homosexual is a problem only as long as one has to hide the fact. In the same manner, if all our foibles and weaknesses are made public, right along those of our neighbours and friends, who is to cast the first stone? Who will need to snoop then? In other words, since we can't protect

privacy, let's replace it with the right to know. Technology would then work for us peons.

Alain Home+Office: (514) 934 6320 UUCP: alain@elevia.UUCP

Re: Apathy and viral spread (Slade, RISKS-11.26)

Steven King <king@motcid.UUCP>
12 Mar 91 19:20:55 GMT

Your data looks good, but I don't think your conclusions are well-founded. Let's assume that SUZY is a valid cross-section of the computer-using populace. Also, let's ignore the inactive users on the grounds that they're not participating in discussions on *any* topic. You claim this leaves us with only 20% of the active computer-using popluace that cares enough to talk about viri, implying that the remaining 80% are ignorant of the matter.

Well, count me in that 80%, though I'm *not* ignorant. I don't use SUZY, but I use other information networks such as Usenet and local BBSs. I'm pretty active on them as well. And I don't subscribe to VIRUS-L or any other anti-viral discussions. Why? Is it that I'm unaware of the threat of viri? Hardly. It's that I have a limited amount of time, and I prefer to spend it in other ways. I pick and choose my discussions carefully, tempering my decisions with real-world affairs like cooking dinner.

Yes, I'm aware of the threat of viri. Yes, I care about them. But I don't care enough to devote time to discussing the latest ones, or the latest theories on how to combat them. I suspect that you'll find a large number of people who fall into this category. While it's reasonable to say that only 20% of the populace care enough to discuss matters, it hardly follows that the remaining 80% is apathetic and ignorant. We're just off saving a different corner of the world...

Steven King, Motorola Cellular (...uunet!motcid!king)

Search RISKS using swish-e

THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

ACM Committee on Computers and Public Policy, Peter G. Neumann, moderator

Volume 11: Issue 28

Thursday 14 March 1991

Contents

BeeperScam

Jake Livni <JAKE@DBCLUA> <jake@mars.bony.com>
Tue, 12 Mar 91 18:58:27 EST

I just saw a news item describing the arrest, today, of someone in New York City on possible wire-fraud and mail-fraud charges. Apparently, he used a computer to dial common beeper exchanges and left a return phone number on as many beepers as he could. Those people who called the number heard a message stating that they were being billed $55.00 for this call. There weren't many more details in the report - except that the Secret Service didn't have much difficulty finding this guy.

Maybe that explains a strange return number my boss got a few weeks ago, I think a 900-number. I knew that some FAX-supply companies were sending out junk-FAXes to FAX-numbers but what could a beeper-supply company try and sell?!

On a slightly divergent note, should there perhaps be some kind of restriction

on phone numbers that cost umpteen-dollars after the first second of connect time? It's not so difficult for a misdialled call to cost plenty.

Jake jake@bony1.bony.com

[An anonymous RISKS reader noted that their company phone switches are protected from making outgoing calls on 900 and 540 numbers. However, their employees may use phones at customer sites in response to a page. Their New York office has alerted employees to this scam. They expect similar activities in other areas in the future. PGN]

The Mailing List Business

"Mary Culnan" <mculnan@guvax.georgetown.edu>
14 Mar 91 13:38:00 EST

In today's Wall Street Journal (3/14/91, p. A1;A8), there is an extended article describing the extent to which the mailing list business extends its tentacles into the details of our private lives. The article by Mike Miller not only provides extensive examples of individual lists which many people are likely to find offensive, but also provides information on some of the largest mailing list firms in the country and the ways they gather data about all of us. Evan Hendricks of the Privacy Times is quoted as saying, "You go through life dropping little bits of data about yourself everywhere. Most people don't know there a big vacuum cleaners sucking it up."

Specific lists cited in the article include:

* Metromail's "Young Family Index Plus" which lists about 67,000 new births each week compiled from clipped birth announcements, referrals from Lamaze coaches and names acquired from companies that deal in baby supplies

* America List Corp sells lists based on high school yearbook listings about virtually every high school class in the U.S.

* Benadryl bought names and addresses (based on phone numbers sold to them) of people calling an 800 number for pollen count information

* The Big 3 credit bureaus sell mailing lists based on aggregated credit data, e.g. "Credit Seekers Hotline" of people who recently applied for credit and are "prospects who want to make new purchases"

Finally, an Atlanta-based company which prepares marketing questionnaires asks if there has been a recent death in the family. The company's President is quoted, "Death has always been a negative life style change nobody thought could be sold, but I differ. I think it's a very good market."

The RISKS are clear. If you aren't aware that personal information is being collected, i.e. you thought you had an expectation of privacy, ignorance makes it impossible to exercise the options that exist for getting one's name taken off of lists. However, even these mechanisms are not foolproof if companies

are not committed to privacy on principle. One example was cited of a company who mailed to people who had signed up for a "delete me" list because these people would have uncluttered mailboxes.

[A lot of the info came from the same public sources I mentioned in my earlier RISKS posting and also in the handout I sent to the 10 or so people who wrote me. MC]

[Roger.Pick@UC.Edu (Roger Pick) also noted this article, headlined "Data Mills Delve Deep To Find Information About U.S. Consumers: Folks Inadvertently Supply It By Buying Cars, Mailing Coupons, Moving, Dying: Treasure for Direct Marketers." He highly recommends it. PGN]

Census Bureau Seeks Changes

<[anonymous]>
Tue, 12 Mar 91 12:37:37 XST

Today's AP reports that the Census Bureau is already asking for $10.1M next year for needed modernization of the census process for the year 2000. Census Director Barbara Bryant told the census and population subcommittee of the House Post Office and Civil Service Committee that "The increasing diversity in ethnic and language groups will certainly make data collection in the 2000 census more difficult."

Bryant said the bureau is considering changes such as the following:

* A "user-friendly short questionnaire" that would include only the questions needed to redraw voting districts. The agency hopes more people will fill out the census form if it is shorter.
* Distributing forms at public locations, much as tax returns are, and using computers to weed out duplicate mailings.
* Using new technologies to produce forms in languages other than English and Spanish.
* Allowing people to file their census forms by home computer directly into the agency's data banks.
* Obtaining information about people from other government agencies rather than from the people themselves.

Let your fingers do the walking thought the roadway information base

John 'Fast-Eddie' McMahon <mcmahon@TGV.COM>
Thu, 14 Mar 91 16:03:00 PST

In the 3/13/91 issue of the San Francisco Examiner, a columnist (I have forgotten the name) describes the new transportation department service where you can use your phone to dial up and request information on the status of a particular roadway. From a touch tone phone, you answer the prompt with the highway number.

It appears the default for any given road is a message which states that "no construction/detour information is available". This was the information that the columnist received when he punched in "480", the code for Interstate

Highway 480 in downtown San Francisco.

The problem is that I-480 (a.k.a. The Embarcadero Freeway) was closed after the 1989 Loma Prieta Earthquake earthquake and is in the process of being torn down. Anyone who reads a San Francisco newspaper know this. Obviously no one bothered to tell the computer...

John 'Fast-Eddie' McMahon, TGV, Inc., 603 Mission Street, Santa Cruz CA 95060
408-427-4366 or 800-TGV-3440 : MCMAHON@TGV.COM

How to deal with "DROIDS"

<MISS026@BOGECNVE.BITNET>
Thu, 14 Mar 91 19:05:53 -0600

The recent discussions on "droid" workers has prompted me to pass along a bit of "wisdom" that I've acquired from dealing with many "droid-related" problems.

Feel free to quote the following:

Re: EM solution for new buildings - risk solved?

Christopher Owens <owens@lust.uchicago.edu>
14 Mar 91 16:08:53 GMT

> ... which stops any electromagnetic radiation from leaving the building.
> ^^^
> It is therefore impossible to hack inside information from outside ...
> ^^^^^^^^^^

It appears that the author of the magazine article uses the term "any" to mean "some", and "impossible" to mean "more difficult". Clearly (bad pun) the stuff can't stop *all* electromagnetic radiation, else you couldn't see through it.

Christopher Owens, Department of Computer Science, The University of Chicago
owens@gargoyle.uchicago.edu (312) 702-2505

Computer Obtuseness File (Medical Division)

Anthony E. Siegman <siegman@sierra.stanford.edu>
Sun, 10 Mar 91 16:27:10 PST

My wife's father, elderly and ill, has had many medical bills lately. These bills are sent by the medical providers (doctors, hospitals, etc.) directly to Medicare, which pays part of the charges, leaving a balance to be paid by supplementary insurance or his personal funds.

Because so many patients in this situation have supplementary Blue

Cross/Blue Shield coverage, Medicare has set up an automatic forwarding procedure to transmit the unpaid portions of these bills directly to Blue Cross. My wife's father has supplementary coverage with another carrier, however, and no Blue Cross coverage; yet it turns out this automatic forwarding feature can be neither redirected to his carrier nor turned off.

For every single bill, therefore -- and there are dozens -- the unpaid portion gets forwarded to Blue Cross, which tries to process it and discovers he has no coverage. So after a suitable delay they mail him (really, us) a form letter (a separate one for each bill) saying they are unable to identify his coverage. There seems to be no way to turn this process off or short-circuit it.

--AES

Search RISKS using swish-e

Report problems with the web pages to the maintainer

Search RISKS using swish-e

THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

ACM Committee on Computers and Public Policy, Peter G. Neumann, moderator

Volume 11: Issue 29

Friday 15 March 1991

Contents

Paranoia and Telephone risks revisited (W.A.Simon, RISKS-11.27)

Larry Nathanson <lan@bucsf.bu.edu>
Thu, 14 Mar 91 22:24:13 -0500

> * Our medical files are violated by law enforcers as a matter of
> routine. Employers are not far behind. Insurance companies are
> misusing this same information. Government agencies are unable
> to protect it against leaks. And, big insult, I am not allowed
> to see the file my own doctor keeps on my subject.

This paragraph ranges from blatant misunderstanding to just dead wrong.
Medical confidentiality is being taken very seriously nowadays. I really can't

think of many reasons why a cop would want your medical file, (drug testing is generally not part of your record) and I certainly don't see any health professional allowing a cop access to medical records without a warrant. For one thing, it's unethical. And another, its illegal.

I don't see how insurance companies are "misusing" the medical information. They may be doing a lousy job of interpreting it, and their payments might not be fair, but if you want them to pay, you have to tell them what the doctor did. That's not poor use of information, not misuse.

Government agencies might not be able to protect your medical record against leaks, but that's not terribly surprising -- it's not their job. Last I heard, Bush was not deploying the Marines into every doctor's office. The medical record is part of the doctor patient relationship- thus it is the doctors responsibility to keep it private. It is the government's repsonsibility to hear the case, if you sue him for not doing so.

(Quoted without permission from _The Rights of Patients_, by George Annas. VERY highly recommended for anyone interested in their medical rights. George Annas is one of the top Health Law people in the country, and is quite a good speaker and author.)

Q: Does the patient have the legal right to see and copy the medical record?
A: The majority of states grant individuals a legal right to see and copy their medical records ... In most other states individuals have a probable legal right to access without bringing suit. ... On the federal level the Privacy Act of 1974 requires direct access in most circumstances.

Q: What should the patient do if denied access to the medical record?
A: Raise Hell. There is no valid, ethical, or legal reason to deny a competant patient access to the medical record. ... (exceptions of "would do harm...etc" listed.)

Q: Is the maintainance of confidentiality a legal or an ethical obligation of health care providers?
A: It is both. Historically, the doctrine was an ethical duty applicable only to physicians. Currently it is also the legal duty of physicians ... and it is becoming a legal duty of other health care practitioners, as well. (Quotes Hippocratic Oath, AMA Principles of ethics, ANA Code)

> Therefore I propose all medical files should be made public. If I am discriminated against by an insurance company for smoking pot, why should their president be sheltered from the public revelation that he is a drunk and a wife abuser?

Because technically, pot smoking is illegal, drinking to abuse is not, and wife beating only is, if she brings charges. What kind of insurance are you applying for, that requires a drug test?

> * All of my past employers know about my checkered past. I know nothing about theirs. Why should their resume be confidential? I ask that human resource departments make all resumes public.

Ummm.. because you are working for them, not vice versa???

> * Police and politicians keep tabs on our every move through passport control and credit cards. But politicians travel with diplomatic passports and they use assumed names to protect their privacy.

Whoa! While the general feeling on RISKS (mine too) is that technologies can ALLOW one to be tracked, I think postulating that such a system is officially in place and active is getting a bit paranoid. And why in the world do you think the politicians are going around incognito for their privacy? Where do you get this stuff from?

> What makes our privacy so fragile is that we value it.

Ah! Finally, we agree on one thing.

Smartening up coexists with dumbing down

"GRUMPY::RMEHLMAN" <rmehlman%grumpy.decnet@uclasp.igpp.ucla.edu>
14 Mar 91 21:59:00 PDT

The following is excerpted from Digital Review, March 11, 1991, p.16,
"Files Getting Bigger All the Time" by Bill Hancock:

> A customer called today and said that one of our network security products had set off a security alarm proclaiming that excessive data was being transmitted from one node to another. [...]
>
> It seems that the user of the offending microcomputer had a hard-disk head crash about a year ago and has been extremely diligent ever since about performing system backups between the microcomputer and the system with the file server software.
>
> Well, the user of the microcomputer received a CD-ROM optical disk player (read only) and thought it had to be backed up every night. The result? A 650MB CD-ROM was being backed up to the file server each night, and it was setting off the excessive data alarm in the network security product.

"US study discounts VDT-miscarriage link"

Martin Minow 15-Mar-1991 1009 <minow@ranger.enet.dec.com>
Fri, 15 Mar 91 07:26:26 PST

>From the Boston Globe, Mar 14, 1991: "Medical Notebook" by Judy Foreman (abridged slightly by MM):

"Government researchers say a new study settles a question that has worried women of childbearing age for more than a decade: Can using a video display terminal cause miscarriage?

"The answer is clearly no, according to the National Institute for Occupational Safety and Health in Cincinnati, which studied 730 pregnant directory assistance or general telephone operators, some of whom worked at VDTs [15% miscarriage rate] and some of whom did not [16%]."

... "The new study, published today in the New England Journal of Medicine, did find that three factors are linked to increased risk of miscarriage: heavy drinking, smoking and the presence of a thyroid disorder."

My comments: Brodeur's New Yorker articles quote a researcher who suggests that electromagnetic-field related miscarriages may occur at such an early stage of development that the woman doesn't realize she's pregnant. I suppose one could control for this by noting the number of months between "intent to get pregnant" and "missed period" (i.e., whether there were miscarriages in the first two weeks after fertilization). This is an extremely noisy measurement, and would probably require a much larger sample size to elicit reliable data. Also, both VDT and non-VDT operators might both work in an "electromagnetic-field-rich" environment inside a telephone office which would mask any differential effects of the VDTs.

My own suspicion, however, is that the researchers are correct and that whatever VDT-related effects exist are better explained by job-stress and general economic-related issues: the VDT offers a visible symbol, even if it is more of an effect than a cause.

Martin Minow minow@ranger.enet.dec.com
The above does not represent the position of Digital Equipment Corporation

Interesting analysis of drug poisoning risks

Jerry Leichter <leichter@LRW.COM>
Fri, 15 Mar 91 11:09:30 EDT

The following is extracted and summarized from an essay, "Sudafed's the Last Thing to Be Afraid Of", by Paul H. Rubin, former chief economist of the Consumer Product Safety Commission, soon to be a professor at Emory University. It appeared in the 13-March issue of the Wall Street Journal. Much of it concerns the specific risk of drug poisoning; but many of the same issues and arguments arise for all kinds of risks. Jerry

Two people have died after taking poisoned Sudafed. These murders, apparently due to a random act of wanton violence, are tragic but not unique. In the past decade, there have been at least six previous episodes of ... poisoning [and] perhaps 10 deaths.... These incidents can provide serveral lessons:

- As a society, we have trouble adapting to small risks. The number of deaths involved have been very small by any measure. There are more than two million deaths a year from all causes in the U.S. There are 5000 deaths ... from accidental poisoning,

and more than 20,000 ... homicides. If there continues to be one death per year from tampering, risk to a typical consumer is on the order of one in 30 million. This is 30 times smaller than the smallest risk that the [EPA], not a conservative body, will address. In the grand scheme of things, deaths from product tampering are a minute problem, whether relative to all deaths or to homicides.

Nonetheless, consumers have reacted strongly to these poisonings. By some measures, Tylenol has never fully recovered from the loss in brand value from two poisoning incidents [in 1982 and 1986].... [The recalls cost some $100 million; one estimate of actual losses to the maker, counting loss of market share and necssary price cuts, is on the order of $1 billion.]

Before mass communications, a person probably would learn of a hazard only if it harmed someone in the community. Such risks were likely to be sufficiently probable to be worth worrying about. Today, however, our intuitions about risk are not a good guide to action. We can learn of risks with minute probabilities. Indeed, the more unusual the death, the more newsworthy it becomes, and we may be more likely to learn about such risks than about more common and more significant risks, such as death from automobile accidents. The Alar episode teaches that we may even learn about nonexistent risks.

Because of the publicity given trivial risks, people incorrectly perceive that the world is becoming riskier. In reality, it is becoming ever more safe, and life expectancies are continuously rising. Life expectancy at birth in the U.S. was 59.7 years in 1930; by 1987 it had risen to 75 years. Moreover, death rates from accidents of all sorts are falling in the U.S.

- Businesses must respond to consumer perceptions, even if the perceptions are not objectively justified. [This is expensive - tamper-resistant packaging costs $50 to $75 million a year just for materials. Tylenol is no longer sold in capsules, a loss of convenience.] ... Ralph Nader and others who claim that businesses are indifferent to consumer risk have it exactly backwards. Businesses are exceedingly sensitve to consumer perceptions of risk, even when those perceptions are biased.

- ...[T]he tort system serves only to create additional injury, not to provide real benefits. There were at least four claims of $5 million each filed in the Tylenol matter, and at least one claim has already been filed against Sudafed. There is no negligence and no blame in either case, and nothing the manufacturers could reasonably have done to prevent the incidents. The only effect of such litigation is to raise the price [to consumers].

- Some harms may have no cure. Unfortunately, there is nothing feasible to do about product poisonings. After the Tylenol poisonings, many firms began using tamper-resistant packaging,

perhaps a rational response given the consumer fears generated by the poisonings. No package, however, is entirely tamper-proof.

We can see this clearly with the Sudafed murders. Like all over-the-counter medications, Sudafed was sold in tamper-resistant packaging - but tampering occurred. A walk through a grocery store or a drug store will quickly indicate that there are inumerable places where one could insert poison. (Remember the poisoned Chilean grapes?) A determined killer can always find something to poison.

In the case of over-the-counter drugs, tens of millions of dollars are already being spent on a hazard that experience tells us may involved one death a year. Regulatory agencies ... commonly estimate that it pays to spend $1 million to $2 million to save a life; upper-bound estimates are about $9 million. The tens of millions we are spending on packaging could save more lives if spent more efficiently - and, anyway, do not seem to be effective in saving even one life.

Some authorities suggest that consumers examine packages more carefully to determine if tampering has occurred. However, the risk is so small that this would not be a useful way to spend time. Time spent in other actions, such as buckling seat belts, would save more lives than time spent examining drugs.

- Government reactions are often counterproductive. After the first Tylenol incident, the [FDA] began to require tamper-resistant packaging.... As we've seen, this hasn't been effective (though, of course, it's impossible to tell if it's deterred less-determined poisoners.) While firms may decide to introduce such packaging themselves, there is no reason to mandate it by law. Now, as a result of the Sudafed incident, there have been calls for the FDA to ban capsules for all over-the-counter medications.... There are benefits to capsules, such as ease of swallowing, and it would be misguided to ban them.

The only appropriate government response to such incidents ... may be increased resources [to catch poisoners] and increased punishment.... The threat of execution is more likely to be effective ... than are increased requirements for packaging....

Most of us do not routinely wear bullet-proof vests, even though the chance of being shot by a mugger or being a victim of a random bullet in a drug war is vastly greater than the chance of buying a poisoned capsule. Public authorities and a responsible press should indicate the order of magnitude of risks, and allow people to take whatever precautions are appropriate. Unfortunately, sometimes there aren't any.

Drawing the correct conclusions from that Miami NTSB report

Donald A Norman-UCSD Cog Sci Dept <danorman@UCSD.EDU>
Thu, 14 Mar 91 21:45:19 PST

In previous issues of RISKS there was considerable discussion of the case of the missing o-rings on all three engines:

NTSB. (1984). Aircraft Accident Report -- Eastern Air Lines, Inc., Lockheed L-1011, N334EA, Miami International Airport, Miami, Florida, May 5, 1983 (Report No. NTSB/AAR-84/04). National Transportation Safety Board. Washington, DC

Sorry for not responding earlier, but I am in hiding this academic year.

I thought that the real impact of this report was missed by all the discussants. This is a classic RISK case example, and perhaps ought to be required reading. The incident has several unrelated phases, each all by itself a case story of hazard and risk. Here is a very brief review of the highpoints.

Part I: Maintenance of the engines.

A plug is removed from each engine to check the oil. The plug is magnetic, and by examining the metal particles on it, you can tell the state of the engine oil. Obviously, after removing such plugs, they have to be replaced. With a plug and an o-ring.

Item: all three o-rings were missing, one each from three engines.

Item: two different mechanics replaced the plug/o-ring combination on the three engines (the center engine is somewhat different than the two wing ones)

Item: they signed off the checklists correctly signing that they had installed the o-rings on the plugs, but without putting on the o-rings.

Item: they NEVER put on o-rings for as long as they had worked there, so they always (properly?) signed off the checklists saying they had put on o-rings because in fact, the o-rings were always already on. And you know those stupid forms that ask you to certify things that have no relevance. (My comment).

Item: the o-rings were already on because the supervisor, for years, got the parts from the storeroom, put on the o-rings, and left them in his desk.

Item: this one night -- out of many years -- the desk drawer was empty, so the parts had to be gotten from the storeroom. And the parts are separate, not attached together in the storeroom.

Item: the maintenance crew started the engines and looked for leaks, but didn't find any. (But it was night and the engines may not have been left on long enough)

---

moral so far: Never try to do favors -- if people then count on you and you fail once, severe problems can arise. So, the supervisor was partly to blame.

Don't sign off for something even if you have to to continue: insist on having the checklist changed, or something. Or having the supervisor sign off. (minor moral -- you could get yourself in trouble for following this moral: It would certainly be unfriendly behavior). So the mechanics were partly to blame.

Moral: How come the o-rings were not packaged with the plugs if they ALWAYS had to be installed on them? So the system was partly to blame.

Moral: If you invent a check (turn on engines and look for oil leaks), TEST IT! Leave out the o-rings or don't screw in the plug all the way and see if the leak can be seen. At night, with a flashlight (standing on a ladder, on tiptoes, peering into and around the engine?). So the maintenance procedures were partly to blame.

Moral: who is to blame? The system.

==========

part II

The crew discovered low oil pressure in one engine and shut it down. They then turned around to go back to Miami, even though they were more than 1/2 way to their destination. NTSB hints but doesn't say why. (They trust the mechanics at Miami better?)

When the other two engines showed low oil pressure, the captain sad my favorite phrase of all time:

It can't be true! Its a one in a million chance that all three engines would have low oil pressure at the same time.
I apologize that this is not a quote because my NTSB report is buried somewhere where I can't find it.)

The captain was right. And he was that one in a million.

A one in a million chance is NOT good enough. We have close to 8,000,000 departures a year in commercial aviation, one in a million means about 8 incidents a year.

People are notoriously bad at low probability events. And this is why it is hard to get engineers and designers to take safety seriously enough (That could never happen they say, meaning, one in a million. I heard someone say that elevators were very safe because there was less than one chance in 10,000 that it wold get stuck or break between floors. Yikes. That means I am guaranteed to be in one of them.

So the captain didn't trust the gauges and kept the engines going until they failed. (Even had he believed the problem, he didn't have much choice anyway.)

==========

Part III.

The communication between flight crew and cabin crew was close to zero. These are really two separate operations, one with high status, one with low, and crew don't bother to inform the cabin crew of everything. And, to be fair, they were rather busy.

So great panic in the cabin. passengers screaming, panicking. Cabin crew pretty scared themselves. Told to assume crash position far too early. No idea how much time they had.

Read the report.

==========

Yup, they got the first engine working again just barely in time, so they landed. And the engine then died on the runway.

=====

all accidents involve a complex chain of events. Never believe anyone who gives you "the reason" for an accident. I have never seen an industrial accident with a single reason. Remember that, RISKS, folks. And look for the subsidiary effects -- like how well the passenger side was handled.

As I said this is a classic study: I am amazed nobody else mentioned all the side effects.

Don Norman, Department of Cognitive Science 0515, University of California, San Diego, La Jolla, California 92093 USA dnorman@ucsd.edu dnorman@ucsd.bitnet

---

Known bug turns 25 years old?

<JERRY@HMCVAX.CLAREMONT.EDU>
Fri, 15 Mar 1991 00:09 PST

Bug celebrates its Twenty-Fifth Anniversary!

The March 31 issue of Aviation Week & Space Technolology discusses the X-31, a research aircraft intended to explore high angles of attack. The craft has a long fuselage, a delta wing, canards, and thrust vectoring paddles stuck in the engines exhaust. From the bottom, it looks vaguely similar to a thin space shuttle.

Here's a quote I found interesting:

"The Honeywell digital flight control system is derived from one used on the Lockheed C-130 high-technology testbed aircraft. ... The control system went into a revisionary mode four times in the first nine flights, usually due to a

disagreement between the two air data sources. The air data logic dates back to the mid-1960s and had a divide-by-zero that occurred briefly. This was not a problem in its previous application, but the X-31 flight control system would not tolerate it. This was fixed with software in January, and the problem has not reoccurred...."

So what does this mean? Have they had a known bug from 1965 which was never fixed? What is a divide-by-zero which occurs briefly?

Is the X-31 better or worse than its predecessor? Perhaps the previous application ignored divide-by-zeros and produced spurious results which were never noticed (except by grieving relatives?). The X-31 now proudly catches these errors. Or maybe the X-31 demands more accuracy and doesn't catch these errors and dies instead.

Or, perhaps the previous application had an error-handler which could recover and it's the X-31 engineers who never considered a divide-by-zero....

Jerry Bakin. Jerry@ymir.claremont.edu

RISKS in Dateline

<[anonymous]>
Thu, 14 Mar 91 12:18:27

My wife and I met through Dateline. This is easily the largest computer dating agency operating in the UK. It is commercially successful; has been running for over twenty years and claims to have the largest client list in the country. Their advertisements appear almost everywhere.

The anuual fee is about \pounds 100 at the moment (it was \pounds 70 when I joined four years ago) -- call it $200. For that you get a questionaire asking for personal characterisics (age, education, religion, etc); a personality test (complete the following doodles, do you prefer hiking to watching TV, and the like); and a section on required, desirable, neutral, disliked and rejected characteristics in prospective partners. After pattern matching (and they make a point of using fuzzy matching, though they don't use that term in their promotional literature) you will receive a list of 6 contact names and addresses and/or phone numbers. Further lists are available for a nominal fee -- a couple of pounds or so. (Incidentally, quite a few women reveal only their phone numbers, presumably as a mis-guided security precaution.. In every case but one, a trawl through the phone directory revealed an address. Not a computer-related risk, as I used the paper version.)

In my case, I was pretty tolerant on age differences. I was 30, I thought that women much younger or older than I would not likely be appropriate, so I put my REQUIRED age range as 24-36, i.e., plus or minus 6 years. My wife, for her part, had +3 years to -5 years.

My wife is now 40 and I am 33. We've been married 18 months.

In this particular case, a bug in Dateline's pattern matcher has been

beneficial. Whether that is a RISK or not is open to question.

[In case you were not reading carefully, the program did not adhere to the spec, violating the specified spread of 6 on his part and 5 on hers. Fuzzy matching, eh? Apparently the organization had advertised that it would be a stickler for specified constraints, but permitted "don't cares". So, who's counting, especially if it works. Maybe the real risk is in overspecifying your constraints. PGN]

"What the laws enforce" (RTM Conviction, RISKS-11.25)

Allan Pratt <apratt@atari.UUCP>
Tue, 12 Mar 91 18:08:57 pst

In a RISKS article about RTM's conviction being upheld, PGN writes: "It seems to me that there is still a significant gap between what it is thought the laws enforce and what computer systems actually enforce."

This is true in all parts of the law. A "Keep off the grass" ordinance need not be "enforced" by a fence to be legitimate. Laws provide punishments for violators; they don't prevent violations.

[My reponse not saved. His response to my response follows. PGN]

"Keep off the grass" is just a sign. A cop giving you a citation for walking on the grass is authority. There are better examples where there's no sign, and yet doing something is against the law. Giving a cigarette to a duck in Arizona comes to mind as one of those silly "did you know it's against the law to..." things. There's no sign saying, "Don't commit murder," either. If nobody catches you, you get away with it, but that doesn't make it right or legal. That's the point I was trying to make.

The article I was responding to said, "How can you say something is wrong and then not put up security barriers against doing it?" That statement implies that when you want to say something is wrong or illegal, you have to put up barriers against doing it. I think that logic is flawed.

-- Allan Pratt, Atari Corp. ...ames!atari!apratt [Standard disclaimer]

[WWWHOA! THAT IS *NOT* A QUOTE FROM RISKS-11.25. YOU ARE INVENTING A STATEMENT AND ATTRIBUTING IT TO SOMEONE ELSE, a classical example of SHOOTING A STRAW HERRING IN THE MOUTH. I did not even SUGGEST that you have to put up security barriers, merely pointing out that a gap exists, which can be addressed by a variety of means, technological, social, legal, ethical, etc. PGN]

What does "authorisation" mean? (RTM Conviction, RISKS-11.25)

Peter da Silva <peter@taronga.hackercorp.com>
Thu, 14 Mar 1991 03:29:23 GMT

Should the computer systems be required to enforce the law? Should an absence of protection imply authorization? If so, say goodbye to a goodly part of Usenet.

It's not so in the real world, you know. Am I allowed to steal my neighbor's lawnmower simply because he left it out?

(peter@taronga.uucp.ferranti.com)

Re: What does "authorisation" mean?

Peter G. Neumann <risks@csl.sri.com>
Thu, 14 Mar 1991 9:51:37 PST

I don't think that is the conclusion that should be drawn from the gap. But if the laws say that exceeding authorization is illegal and the computer systems require no authorization, then it seems to be a MISAPPLICATION of the law to say that Morris was guilty of exceeding authorization or misusing authorization or whatever... [with respect to the use of finger, the debug option, .rhosts, ...] [The laws could be a little sharper.]

Re: What does "authorisation" mean?

Peter da Silva <peter@taronga.hackercorp.com>
Thu, 14 Mar 91 23:16:29 CST

Only if you assume the computer system is solely responsible for enforcing the authorization. Is that a valid assumption? Do you want it to be?

[Of course not. See my foregoing comments on Allan Pratt. PGN]

Search RISKS using swish-e

THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

ACM Committee on Computers and Public Policy, Peter G. Neumann, moderator

Volume 11: Issue 30

Monday 18 March 1991

Contents

"The Trigger Effect" and Coke robot...

"Dwight D. McKay" <mckay@ecn.purdue.edu>
Fri, 15 Mar 1991 13:33:26 -0500 (EST)

Having just gotten into work after being stranded at home with no power for two days due to ice storm here in the midwest, I am reminded of the reliance we all place on basic services.

While I've not lost phone service (thank you AllTel!) nor Gas, but I had no electricity. This meant I had no heat as my furnace needs electricity to sense temperature, run the air circulation fan and even start the gas burning (it's pilot light-less). Our kitchen is all electric so that was out, and so on.

Even when power was restored, the ordeal was not all over. How many clocks, and embedded computers do you have around your house? I had to replace half a

dozen "backup" batteries, reset various devices which have no memory without power, etc.

A very worthwhile description of this "technology trap" we are placed in my depending on basic services like electricity is episode 1, "The Trigger Effect" of James Burke's PBS series "Connections". It covers in fairly good detail the sequence of events and problems caused by the early 60's east coast blackout. I'd recommend it as good video for Risks readers to watch or to show to others. The video has started some very interesting conversations concerning the risks of high technology with everyone I've shown it to.

BTW - Have any of the rest of you seen the drink dispensing robot Hardee's has in some stores now? It appears to be directly tied into the same network as their cash registers and fills drink orders while the cashier takes your money. I can see it now, "Sorry, we cannot give you a drink right now, our computer is down." Sigh...

Dwight D. McKay, Purdue University, Engineering Computer Network (317) 494-3561
mckay@ecn.purdue.edu --or-- ...rutgers!pur-ee!mckay

Strange numbers on your beeper

Esther Filderman <ef1c+@andrew.cmu.edu>
Fri, 15 Mar 91 16:29:12 -0500 (EST)

The article about the beeper scam reminded me of something that occured to me two weeks ago.

When my beeper went off in the middle of a Saturday afternoon I was not phased by the strange number that appeared, figuring that it was a coworker calling from home. When I called the number I got a real surprise: I reached US Air's pilot scheduling number!

The person I spoke with told me that the database of beeper numbers was very out of date. When I mentioned that I had had my beeper for over six months she responded that she had once called a number a year out of date.

Meanwhile, some poor pilot was wondering when her/his next flight was....

Esther C. Filderman, System Manager, Mercury Project. Computing Services,
Carnegie Mellon University ef1c+@andrew.cmu.edu

Re: "What the laws enforce" [RTM] (RISKS-11.29)

<TK0JUT1@NIU.BITNET>
Fri, 15 Mar 91 15:47 CST

I rather liked PGN's comment that "that there is still a significant gap between what it is thought the laws enforce and what computer systems actually enforce." It's parsimonious and incisive. I interpreted it to mean simply that the law has not caught up to changing technology, and old, comfortable legal

metaphors are inappropriately applied to new, qualitatively different conditions. Calling simple computer trespass (even if files are perused) a heavy-duty felony subjecting the offender to many years in prison does not seem productive. I may walk on your grass and pick your flowers, even if there is a prohibitive sign. But, it is unlikely there would be a prosecution (informal sanctions, yes, but not a prosecution), and if there were, it would unlikely be a highly publicized felony that subjects me to federal felony charges, even though an ecological federal interest might be claimed.

The point seems to be that emerging computer laws are archaic. Neither those who write the laws nor those who implement them have a clear understanding of what is involved or at stake. When mere possession (not use, but possession) of "forbidden knowledge" can be a felony (as it is in California), we must begin to question what the law thinks it's enforcing. One can oppose trespass while simultaneously opposing Draconian attempts to stomp on those who tread tackily in our once-pastoral fields. And, at the moment, I suggest that it's law enforcement agents who are the greatest danger to the computer world, not hackers. Why? Because "there is still a significant gap between what it is thought the laws enforce and what computer systems actually enforce."

[Thanks! PGN]

Voice Recognition Experiment

Dave Turner <dmturne@ptsfa.pacbell.com>
Fri, 15 Mar 91 15:49:44 PST

The following was excerpted from comp.dcom.telecom. Although it appears to be a legitimate study, the unscrupulous could reap vast rewards.

>The Oregon Graduate Institute of Science and Technology is building a
>huge database of voices as part of a project to develop voice
>recognition for US West directory assistance.
>
>They want to be able to classify sounds according to regional
>differences, and they need thousands of samples of speech to do this.
>
>Call 800-441-1037 (I assume this is nationwide ... it may not be) and
>follow the voice prompts. They will ask your last name, where you are
>calling from, and where you grew up, and then ask you to pronounce
>several words and recite the alphabet.

This could be used for vocal forgery.

By combining the requested words, alphabet and, possibly, numbers a digital vocabulary could be produced for everyone who participated in the study. Once this is available, a "bad guy" could use it to place phone calls using anyone's digital voice. If the hardware were fast enough, the called party could be fooled into believing that he/she is talking to the individual whose voice is being used. The addition of credit card numbers and expiration dates for each "voice" will allow fraud that is hard to dispute; after all, it's your word (voice) against his.

Including your name, location and other personal information in this study could be a big mistake.

This sort of risk is made easier by duping people to provide samples of their voices but a determined "bad guy" could obtain the same information by recording a ordinary phone call and processing the data later.

`Sendsys' forgery - denial of service?

Doug Sewell <DOUG@YSUB.YSU.EDU>
Friday, 15 Mar 1991 20:25:20 EST

I don't get many SENDSYS requests in control, so they tend to stick out. I've also learned by experience that even limited hierarchy or limited distribution will result in a disruptive amount of e-mail (how did I know that over 400 sites got some bit.* - I suspected 100, tops). Many of them are big (UUNET's was several thousand lines long), and they trickle in for days.

Having said this, one I got today stuck out as being rather unusual.

Someone forged a sendsys to rec.aquaria, misc.test, and alt.flame, in the name of one of the 'celebrities' in those circles. Distribution was unlimited. This type of prank amounts to a significant denial-of-service attack, IMHO. In this case, it may also mean bodily injury for the perpetrator, if he's caught.

(If you want to know who, go look in alt.flame).

Doug Sewell, Tech Support, Computer Center, Youngstown State University, Youngstown, OH 44555 doug@ysub.bitnet doug@ysub.ysu.edu

---

Re: Medical privacy and urine testing (Larry Nathanson, RISKS-11.29)

<wex@PWS.BULL.COM>
Mon, 18 Mar 91 13:42:25 est

The issues surrounding urine testing are something I have been researching heavily for over a year, more as they began to affect my life more extensively. While I generally agree with Nathanson's assertions, he does make one important error:

(drug testing is generally not part of your record)

This is true some of the time, but misleading. The discussion revolves around privacy and one of the concerns about urine testing is that testing agencies (gov't, companies and the military) generally require you to sign a form detailing any and all prescription medications you are taking. In many cases, the testing agencies require the testee to produce the actual prescriptions, and may call the prescribing doctor to confirm the validity of the prescriptions.

This information is clearly part of your medical record and it seems an invasion of privacy to require the employee to reveal that s/he is taking {birth control pills, AZT, insulin, anti-depressants, etc.}.

In each case, access to prescription information reveals an enormous amount of medical information which is customarily assumed to be private.

--Alan Wexelblat phone: (508)294-7485
Bull Worldwide Information Systems internet: wex@pws.bull.com

Long-lived bugs

Pete Mellor <pm@cs.city.ac.uk>
Mon, 18 Mar 91 10:30:54 PST

Jerry Bakin's item in RISKS-11.29 <Jerry@ymir.claremont.edu> about the 25 year-old known bug reminded me of some stories about fairly ancient unknown bugs.

I was told by a colleague, who was a computer engineer, about a UK site which required its operating system to be enormously reliable. (They were so highly secret that I was not supposed to know that they existed, so he couldn't provide much in the way of supporting detail.) They had learned the hard way that each new version brought with it its own crop of new bugs, and so had stayed resolutely out of date for many years. Running a stable job mix and not updating, they eventually achieved 4 years of failure-free running. At the end of that time, a new, serious, bug was discovered. This had lain dormant all that time.

The Air-Traffic Control system at West Drayton has recently been replaced. The previous system had been in use for many years. A software engineer who had studied this system told us that a new bug was recently discovered in a piece of COBOL code which had not been changed for 20 years.

Such anecdotes could be dismissed, except that they are supported by careful research. E.N. Adams in "Optimizing preventive service of software products", IBM Research J., 28, (1), pp 2-14, 1984, describes investigations into the times to detection of bugs in a widely used operating system. He found that over 30% of all bugs reported caused a failure on average only once every 5000 running years.

Peter Mellor, Centre for Software Reliability, City University, Northampton Sq., London EC1V 0HB +44(0)71-253-4399 Ext. 4162/3/1 p.mellor@uk.ac.city (JANET)

A cautionary tale [long] [On the Midway in a 3-ring SRCus?]

John DeTreville <jdd@src.dec.com>
Mon, 18 Mar 91 15:59:57 PST

This is a cautionary tale about a software failure that RISKS readers might

find interesting. I wrote down this description soon after the failure, in as much detail as I could, because it made such an interesting story. I've listed some possible lessons at the end, and readers are welcome to add their own.

Around 5:00 p.m. on Friday, February 16, 1990, much of the distributed environment at Digital's Systems Research Center (SRC) became unavailable. Although no machines crashed, most user operations failed with authentication errors and users could get almost no work done. Some quick diagnostic work determined the problem: the contents of the distributed name service had become corrupted. Lengthier detective work determined the long sequence of accidents that caused the corruption.

I should point out to start that at no point during this episode did the name service itself fail. The design and implementation of the name service were both quite solid. All the failures were elsewhere, although they manifested themselves in the name service. SRC is purposely dependent on our distributed name service because it has numerous practical advantages over the alternatives, and because it has given us very reliable service over an extended period. (Failures of unreliable systems aren't very instructive!)

First, some necessary background. SRC's research software environment is called Topaz. Topaz can run stand-alone or layered on top of Ultrix, Digital's product version of Unix. We built Topaz at SRC, and while the research ideas that we test in Topaz may influence Digital's product directions, Topaz is not a production system. Once every year or two, SRC exports snapshots of the Topaz environment to a few universities that we maintain close ties with. We collect the components of an export release, then bring the snapshot up on an isolated testbed and verify that its elements work together and do not accidentally depend on anything not in the release.

Part of the information in SRC's name service is the user data traditionally stored in /etc/passwd. For administrative convenience, we still maintain /etc/passwd files, and although Topaz accesses the name service instead of /etc/passwd, administrative daemons track any changes in /etc/passwd (via a "dailyUpdate" script). For example, if users leave Digital, administrative procedures delete them from /etc/passwd; once dailyUpdate runs, all mention of them is removed from the name service.

On with the story. A few months before, Lucille Glassman had built our most recent export snapshot. To test it, she put together a testbed environment in the machine room, using a small VAX named "midway" as an Ultrix-based Topaz server machine.

The export testbed ran on a small Ethernet disconnected from SRC's main network. The testbed environment had its own name service, and midway had its own /etc/passwd. Midway's /etc/passwd wasn't very large--about a dozen users--and so its name service didn't hold many names. But that was intentional; it was just a testbed.

Since the testbed environment was disconnected from SRC's main network, software snapshots were brought over to midway via a disk that was dual-ported between midway and bigtop, a large Ultrix server machine on SRC's main network. The disk appeared in each system's /etc/fstab (the file system table); it was moved from system to system using the /etc/mount and /etc/umount commands.

Lucille would mount the disk on bigtop, copy /proj to the disk (/proj holds the Topaz environment), then unmount it from bigtop and mount it on midway as /proj.

Later, after the export was completed and the tapes had been sent out, Richard Schedler and Lucille did some cleanup on midway. They turned off its Topaz servers, including the name server. They also edited midway's crontab, which runs various commands at various times, not to run dailyUpdate; there was no need for it. But they didn't reconnect midway to the network as an ordinary Ultrix machine; they left it isolated on the testbed network.

Here comes the amusing part. It turns out that on the version of Ultrix running on midway, /usr/lib/crontab is a symbolic link to /etc/crontab. The cron daemon reads from /usr/lib/crontab, but the file physically resides in /etc/crontab. Knowing this, Richard and Lucille edited /etc/crontab to remove the call to dailyUpdate.

The first thing that went wrong was that, at some point earlier, this symbolic link had been broken, and /usr/lib/crontab had been replaced with a copy of /etc/crontab. Most people at SRC use the Ivy text editor, which runs as a single server per user, creating a window per file. Since Ivy runs with the user's permissions, you can't use it to edit files like /usr/lib/crontab, which you can't ordinarily write. Users get around this limitation by editing copies, then moving the copies back as super-user. This is an error-prone operation, and we believe that at some time someone fumble-fingered the last step.

So when Richard and Lucille edited /etc/crontab, it had no real effect; cron kept on using the old /usr/lib/crontab. Every day, midway ran dailyUpdate. But dailyUpdate tried to run a program from the Topaz environment on /proj, and the dual-ported disk holding /proj had been claimed by bigtop, so midway couldn't access it, and dailyUpdate silently failed every day. Also, midway was still disconnected from the network.

The second thing that went wrong was that midway got reconnected to the network. Someone threw a local/remote switch on a DELNI Ethernet connector. This happened some time in the previous few months. (A few months after this writeup circulated internally, we found out what had happened; someone had been fixing a broken workstation on the testbed network, and tested it by rejoining the networks rather than moving the workstation's network connection.)

On Friday, 2/16/90, at 11:00 a.m., SRC had a power failure during heavy rains. This was the third thing to go wrong. When power came back, bigtop and midway both came up. Midway came up faster, being a smaller system. This was the first time in months that midway had booted while bigtop was down, and midway got to claim the dual-ported disk.

Friday at 5:00 p.m., midway successfully ran dailyUpdate. It contacted SRC's name service, and made the name service contents consistent with its abbreviated /etc/passwd. Soon afterwards, when the authentication caches expired on their workstations, most people found themselves unable to do anything that required authentication: log in, run programs, even log out.

(Richard and Lucille and I didn't notice anything wrong at first, because we were listed in midway's /etc/passwd. But Lucille received mail from the name service saying that root@midway had just made a bunch of changes, and I got calls from people asking, "What does it mean when it says, `Not owner'?")

So Lucille and I went to the machine room (dodging the person installing some new locks), and looked at midway's /etc/crontab. Everything looked fine; no mention of dailyUpdate there. (It was much later we discovered the call to dailyUpdate was still in /usr/lib/crontab). Although we didn't know what had made dailyUpdate run, Lucille rethrew the DELNI switch to isolate midway from the network so it couldn't happen again.

(If the person installing new locks had been a little ahead of schedule, we probably wouldn't have been able to get into the machine room, since we didn't have keys yet.)

Lucille then ran dailyUpdate against a real copy of /etc/passwd, to get things to the point where everyone could log in. She discovered that there's an upper bound to the number of additions that dailyUpdate can make to the name service at once. This had never been a problem before, but it was a problem now. (Midway's dailyUpdate didn't have any problem with the same number of deletions.) Lucille finally coaxed dailyUpdate to run. Unfortunately, restoring information isn't as easy as deleting it, and even with a lot of hand editing, things still weren't great at 7:00 p.m., when Lucille and I both had to leave.

Richard had left long before, as had Andrew Birrell, our main name server expert, but Lucille sent them mail explaining what had happened, and asking whether they could fix it. Ted Wobber and Andy Hisgen, two other name server experts, were both out of town for the weekend.

When I got back at 10:30 p.m., I found the mail system was broken, probably as a result of the name service problems, so Lucille's mail hadn't been delivered and no one had done anything since 7:00 p.m. (The file system holding server logs had also overflowed, because of all the RARP failures caused by the name server outage.) By the time I brought the mail system back up, it seemed too late to phone anyone at home, so, after confirming that no one else was fixing things at the same time, I started to restore the name service contents from the previous night's incremental dumps.

The name servers hold their state in VM, but keep stable copies in a set of files that they write into a directory from time to time. I found backup copies of these files on bigtop from incremental dumps made at 6:00 a.m. Friday. Fortunately, bigtop's name server had written a full set of files to disk between 6:00 a.m. Thursday and 6:00 a.m. Friday, or this wouldn't have worked. We didn't dump these directories on the other name servers, named "jumbo" and "srcf4c"; we had figured we didn't need to, since the contents are replicated. Even so, extra dumps might have come in handy if bigtop's dump had been unusable. We've now started dumping these directories on jumbo too, just in case.

(I had to do this restore before 6:00 a.m. Saturday, since the incremental dumps are kept on disk, and each day's incremental dumps overwrite the previous day's.)

So I reconstructed an appropriate directory for bigtop's name server, but couldn't do the same for jumbo or srcf4c. I killed all three name servers, installed the restored state on bigtop, and restarted bigtop's name server. At this point, SRC had a name service, but it wasn't replicated.

I left the other name servers down, because the overnight skulkers would make the name servers consistent, and bigtop's old information would lose to the more recent information in the other servers. I sent out a message describing the state of the world and went home, figuring that things weren't really fixed, but that nothing bad could happen before I came in Saturday morning.

Saturday morning, SRC had two more power failures during more rain. Jumbo, bigtop, and srcf4c all went down. Srcf4c has an uninterruptible power supply, but the batteries had probably gone flat, so it went down during each power failure.

When power was restored, bigtop's name server came back up, but so did jumbo's and srcf4c's. I had only killed the running instances of the other servers, not uninstalled them, since I was tired and thought it wouldn't matter overnight. Ha! Jumbo's server rebooted automatically after the power came back. Perhaps as a result of the flaky UPS, srcf4c did not reboot, but a helpful passer-by rebooted srcf4c by hand. He hadn't read the electronic message I'd left, since he couldn't log in, and, in any case, figured that some inconsistency was better than total unavailability while waiting for jumbo and bigtop to check their disks and finish booting. Compounding Saturday morning's confusion, I got to SRC later than I had planned, not wanting to travel in the rain.

At this point, users had a 2/3 chance of getting their data from a bad name server, and the bad servers were slowly propagating their contents to the good one.

Fortunately, I had kept copies of the directory I had reconstructed on bigtop the night before (plus the contents before I overwrote it, plus copies of everything else I could find; I had known I was tired). Even more fortunately, Andrew and Richard agreed to come in. We killed all the servers, reset bigtop's contents and restarted its server, then Andrew used magic name service commands to erase the name service replicas on jumbo and srcf4c and create new ones, copying their contents from bigtop. And that fixed everything.

Many thanks to everyone at SRC who helped understand the problem and to fix it. Thanks also to Jim Horning, Cynthia Hibbard, and Chris Hanna for reviewing this writeup.

What were the lessons? Some might be:

1) Things break Fridays at 5:00 p.m., especially if it's a long weekend. (Although SRC as a whole didn't get that Monday off for President's Day, many people weren't back by then. Perhaps some were trapped in the Sierras after heavy snows and an avalanche closed the roads.)

2) The name service had been so reliable that there were few experts available

to fix it. I'm not an expert, but I knew how it worked because I once released a faulty garbage collector that caused some name servers to lose data and eventually crash; I had done penance by fixing it.

3) You're always ready to fight the previous war. When I discovered the name server problems, my first reaction was that it was another garbage collector bug (even though the collector had been stable for about a year). Discovering that garbage collection had nothing to do with the problem wasted some time.

4) Ivy's inability to edit protected files may not be a big problem on the average, since those few users for whom this is a problem can work around it, but the workarounds can be dangerous. Moreover, these users didn't complain about this limitation to the Ivy developers; they devised the workarounds on their own.

5) After midway's /usr/lib/crontab got overwritten with a real file, it's unfortunate that Richard and Lucille followed the link in their heads and edited /etc/crontab, instead of editing /usr/lib/crontab and letting midway follow the link. Although a very similar situation had occurred two years earlier, neither one expected it to happen again.

6) SRC's name service allowed only one instance of the name service on the same network, virtually inviting this sort of collision of namespaces. Since then, Digital has developed product-quality name servers without this limitation, but we were running our own earlier experimental software. This limitation was probably a mistake waiting to strike, but it's a sort of mistake that's commonly made.

7) Although there are plenty of locks on the machine room, someone toggled the DELNI. Perhaps some network connectors should also have been unscrewed (and hidden). Again, this wouldn't have been a problem if we'd been using Digital's product software.

8) While the export snapshot was being built, Lucille was very careful to keep midway isolated from SRC's main network. Afterwards, she watched midway for a couple of days, making extra sure that it wasn't exporting its /etc/passwd contents. But she didn't watch it for months. Perhaps she should have reinstalled Ultrix on midway, deleting all old state.

9) Using dailyUpdate to keep the name service consistent with /etc/passwd seems cumbersome and error-prone. We may move toward a scheme where the name service drives /etc/passwd instead, since even catastrophes like this one would not lose information.

10) When I fixed things Friday night, I knew I was tired. As a result, I was very careful; I made copies of everything that might be overwritten. They might well have been overwritten even if I hadn't been tired, and I mightn't have had the copies.

As I said at the beginning, the name service itself did not fail. However, some other parts of the environment were not as well thought out, and the end result was a loss of data held in the name service. Moreover, the experimental name server's limitation to one instance per network made it especially susceptible to failure caused by accidental network reconfiguration.

John

Search RISKS using swish-e

Report problems with the web pages to the maintainer

Search RISKS using swish-e

THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

ACM Committee on Computers and Public Policy, Peter G. Neumann, moderator

Volume 11: Issue 31

Tuesday 19 March 1991

Contents

Untested mods to amusement rides...

Peter da Silva <peter@taronga.hackercorp.com>
16 Mar 91 23:41:35 CST (Sat)

Recently at Astroworld they decided to do a mod to their new ride, the "Condor", for its initial public performance. They were giving a bunch of reporters the first shot, so they decided to make it stop at the top to give them plenty of time to take pictures.

Apparently they didn't test the change before the big day, because it went up then got stuck halfway down, and it took 20 minutes of coaxing before they got the press off.

Since this ride involves swinging people around at 40 MPH, it could have been a *lot* worse! Astroworld officials insist that thanks to daily safety checks there was never any danger, but I think we've all heard that before.

The true risks of computerized voting

Hank Nussbacher <HANK@VM.BIU.AC.IL>
Sun, 17 Mar 91 12:34:42 IST

The following is a true story that happened on Wednesday March 13. Tel Aviv University decided to hold this year's student elections via computer. 23 voting stations were set up, a VAX/VMS system was dedicated to the one day project and a special voting program was developed.

Since every faculty had different students running for office and since different students would arrive at the polling booth, the menu screen was designed with a dynamically built vote selection. The menu would list 20 or so candidates and the student would select their choices at the bottom. The computer would then display the following menu with the selected choices in positions 21, 22, 23 ... of the initial menu. The user could either accept their choices by pressing enter or go back to the main menu.

When the user hit enter, the number of choices selected were to be extracted from positions 21, 22, 23, etc and placed into the vote file. By mistake, the program always took positions 1, 2, 3 from the original menu. When the voting was done and the tallies were counted it was spotted that in every faculty the people listed in the 1st, 2nd and 3rd positions were the ones that always won. A quick check of the program showed the flaw. A single line of code with an incorrect initial pointer destroyed 3,000 votes.

The test data that was run through the program did not catch this flaw since the checking was done by name and not by number and since there were dozens of names involved, no one took the time to double check that indeed the names voted for the most were indeed the ones who won.

This week, Tel Aviv University will be doing a manual re-vote.

Hank Nussbacher, Israel

California, driving, and privacy, again

Chris Hibbert <hibbert@xanadu.UUCP>
Tue, 19 Mar 91 11:19:48 PST

The California Department of Transportation (CalTrans) has been studying Automatic Vehicle Identification (AVI) systems, which would be used to automate the charging of tolls on bridges and highways throughout California. They've

asked for comments on a proposal titled "Compatibility Specification for Automatic Vehicle Identification Equipment". The specification calls for an active transponder that could be installed securely on vehicles. When it is queried the transponder responds with a radio burst that would contain, among other things, the VIN issued by the vehicle's manufacturer. This is a first-rate RISK to privacy.

The system makes it possible for highway authorities (and anyone else who can build or buy a reader that meets the spec.) to track the movements of anyone who signs up in order to get faster service at tollbooths. The most plausible charging system using this kind of reader requires that records be kept long enough for disputes to be resolved. As we have seen here before, those records (or their backups) can be examined with a subpoena or with the cooperation of the vendors. (CalTrans would probably pay the vender of the system to maintain the records, though that's not discussed in the spec.)

Other RISKS evident in this preliminary spec include the RISK of over-specification. The stated accuracy requirement is "incorrect transaction decodings and encodings shall not exceed 1 in 20,000". The box is required to work without change in accuracy over a temperature range of -40 to +180 degrees Fahrenheit; with vehicle spacing as close as 15 feet; at all speeds up to 100 mph; and with up to "6 inches of dry uncompacted snow," "2 inches of salt water ice or slush," or "1 inch of dirt sand or salt" obstructing the path between a transponder and reader.

There are quite a few alternative designs that don't require an identifier that is traceable to an individual. At the low end there are low-tech low-discrimination systems like color-coded or bar-coded monthly window stickers (with many people getting the same sticker each month.) These allow charging a monthly fee and charging a price based on number of occupants and time of day (require paying manually in a separate lane on days when the car is less full or traveling at rush hour.) They don't support charging based on the amount of use within a month.

A more sophisticated system would use unique (but not traceable to individuals) identifiers. The user has an anonymous account to deposit money into and money would get deducted each time past a toll collector. No one has to maintain an association between account numbers and people's names. New Orleans apparently uses this kind of a system. Drivers get individual boxes, and pay into anonymous accounts. If anyone can give me more details about this system, I'd appreciate it.

The most sophisticated system might have active transponders in the car that themselves maintained records about how much money had been deposited. The toll collector would send a packet asking the box whether it had enough money and then to deduct the current charge. When the box indicated it was running low, it could be recharged like a Pitney-Bowes postage meter. This scheme would obviously require much more security in the box and reasonably sophisticated encryption mechanisms in order to make sure that the same packet couldn't be used more than once to pay for trips, etc.

Any AVI system design that requires that records be kept to do billing or resolve disputes allows tracking of individual movements. This would lessen our individual privacy, which in California at least is protected by the state

Constitution.

Comments on the proposed specification can be sent to Les Kubel, Office of Electrical and Electronics Engineering, California Department of Transportation, 5900 Folsom Boulevard, PO Box 19128, Sacramento, CA 95819. I have a scanned copy of the proposed specification. You can get a copy from me or from that same address. You can also call and ask for a copy at (916)739-2245. I wasn't able to find out what deadlines have been set when I talked to Les.

Chris

Can't stop auto-withdrawal

Rick Simkin <rsimkin@dlogics.dlogics.com>
Mon, 18 Mar 91 8:20:39 CST

Some banks offer a service which pays bills directly out of your checking account. This service is started with a single authorization for each company which will have this privilege. This could be considered a risk all by itself--NO customer action is required for the bank to pay out whatever the creditor bills. If there's an error in billing, the customer finds out only when the bill comes, with the annotation "Paid by bank draft." At this point, the money is already gone--there's no way to withold payment in the case of a dispute.

But I discovered a more alarming risk this month: at the bank I have in mind, this service, once started, continues forever. Although direct drafts can be authorized by a signature given to the bank, they can't be stopped that way. Instead, the customer has to tell the billing party, "Stop removing money from my account," and keep doing so until the billing party stops. The bank employee blamed this setup on the computer.

Maybe the bank's programmers studied under the Sorcerer's Apprentice?

Rick Simkin, Datalogics, Inc., 441 W. Huron St., Chicago, Illinois 60610-3498
uunet!dlogics!rsimkin rsimkin@dlogics.com +1 312 2664437

Re: Let your fingers do the walking...

Chris Thomas <thomas@sono.UUCP>
Mon, 18 Mar 91 09:12:50 PST

John McMahon mentions the California Department of Transportation (Caltrans) road-information service, and how it failed to have any information on the quake-damaged Embarcadero freeway.

Some experimentation with the system reveals two facts:

- the default condition is that "the route you have selected is reported open with no driving restrictions"; and

- there is no check to verify that the input is an actual
  highway number in California. (Unless someone has created
  a highway 9999 without telling anyone!)

Since Caltrans filed paperwork to have the Embarcadero officially removed from the state system (sometime in 1990, I believe), highway 480 "no longer exists", and Caltrans thus has no information about it.

Compare this with the information provided for another quake-damaged freeway, I-280. The message correctly identifies the mile-long closure.

Chris Thomas thomas@sono.uucp (415) 969-9112 x2994

Re: About Risks in Believing AI Gurus (M.Minsky) (RISKS-11.19,21)

Bob Frankston <Bob_Frankston%Slate_Corporation@mcimail.com>
Wed, 13 Mar 91 15:19 GMT

There are risks of unthinkingly believing various philosophies be they AI, religion or other maintstream philosophies. It is not clear what the particular risk is in the case of Minsky. I view him as a source of questions not final answers.

Our understanding of what "intelligence" is minimal. I wouldn't expect computers to be the same as humans short of synthesizing people from DNA. But the idea of a symbiotic relationship between computers and people both with highs levels of intelligence (whatever that is) is not that far fetched.

Klaus Brunnstein's claim: "In my analysis, it is this kind of misconceptions that are an esssential reason for contemporary computer accidents - misconceptions of scientists (uncritically following paradigms and unverified assumptions), top- and medium-level-misconceptions, misimplementations, misunderstandings on the users' side, conscious use of side effects and other misuse..." seems to trivialize real issues in systems design and engineering.

Re: Telephone risks revisited (RISKS-11.27)

Kian-Tat Lim <ktl@wag.caltech.edu>
Thu, 14 Mar 91 19:44:35 GMT

I'm sure many people will point out the similarity of this scenario to that in John Brunner's 'The Shockwave Rider'.

Kian-Tat Lim (ktl@wag.caltech.edu, KTL @ CITCHEM.BITNET, GEnie: K.LIM1)

[Actually noone else did, but I am always amused at how many of our current risks were in some way anticipated by Brunner. PGN]

Re: Pilot Error - an impartial assessment? (RISKS-11.)

The Polymath <hollombe@ttidca.tti.com>
12 Mar 91 21:12:58 GMT

Twenty-some years ago, when I worked for the L.A. County Engineer, Aviation Division, I got FAA accident reports across my desk almost daily. Without doing any statistical analysis, one relationship seemed to stand out: If the pilot's dead, it's his fault.

Plus ca change ...

Jerry Hollombe, Citicorp, 3100 Ocean Park Blvd., Santa Monica, CA 90405
(213) 450-9111, x2483 {rutgers|pyramid|philabs|psivax}!ttidca!hollombe

---

Re: Drawing correct conclusions from Miami NTSB report (RISKS-11.29)

The Polymath <hollombe@ttidca.tti.com>
19 Mar 91 02:30:35 GMT

While the analysis of danorman@UCSD.EDU (Donald A Norman-UCSD Cog Sci Dept) is probably true in the broadest sense, I can give a single "reason" for the accident: The need to have an o-ring in the first place. Had the plugs been designed to not require an o-ring, the accident wouldn't have happened.

Is such a design reasonable? Very much so. The Boeing 727 is designed to operate without gaskets or o-rings. All joints where you would expect such are simple metal to metal (or so I was taught in mechanic's school, some 22 years ago. I admit I've never actually been that intimate with a 727).

The unfortunate fact is, it's cheaper to build and maintain a design requiring gaskets and o-rings. The acceptable tolerances are much looser.

Possible moral: You get what you pay for.

Jerry Hollombe, Citicorp, 3100 Ocean Park Blvd., Santa Monica, CA 90405
(213) 450-9111, x2483 {rutgers|pyramid|philabs|psivax}!ttidca!hollombe

---

Re: "What the Laws Enforce"

Nancy Leveson <nancy@ICS.UCI.EDU>
Tue, 19 Mar 91 07:37:30 -0800

The analogy here is not a good one. A more reasonable analogy is someone breaking into your home or business and perusing your personal files. "Breaking and Entering" IS a felony. After the Morris attack that precipitated this discussion, I lost three days of work because the computers had to be turned off and "cleansed." I don't consider that the equivalent of picking flowers on my lawn but of someone breaking into my home, trashing the place, and making it unlivable until I spend three days away from work cleaning it up. Considering the number of lives and careers nationwide that were disrupted, it is not unreasonable that this was highly publicized or that our society would

want to strongly discourage such behavior by making it a crime and not a misdemeanor. Although such laws may not discourage true criminal behavior, they do discourage potentially destructive "play" by essentially law-abiding people.

In fact, personal and business privacy and property is extremely important in a complex, crowded society such as ours. Many science fiction horror stories about future societies involve the invasion of personal privacy -- whether it is by the government or my fellow citizens matters little to me. A society that values my privacy less than the curiousity of others about my personal property is not a pleasant one to consider. And yes, there are serious and important societal costs involved. Right now, I am being hampered in my attempts to work on an important system that may save lives (or cost them if done wrong) because a company with which I need to deal has had to severely restrict outside computer access because of security fears. Draconian security measures to prevent frivolous access and pranks (in situations where it would not otherwise be necessary because there is nothing of value to steal) will hurt us all and cost our society untold dollars and perhaps worse. What about the kids who broke into the Sloan-Kettering Cancer Center and fooled around with the patient records, changing some as a result? It would be surprising to me that readers of Risks that value privacy highly would consider invasion of privacy a misdemeanor on the same level as walking on the grass.

Telecommunications Risks

Nigel Allen <ndallen@contact.UUCP>
Sun, 17 Mar 91 19:50:21 EST

Many telecommunications-related risks discussed here might also be of interest to readers of the Telecom Digest, which is distributed within Usenet as the comp.dcom.telecom newsgroup. If you would like to submit a telecommunications-related article to the Telecom Digest, send it to telecom@eecs.nwu.edu. If you have access to Usenet newsgroups, you can read the Telecom Digest as the comp.dcom.telecom newsgroup; if not, you can be added to the mailing list by sending a message to telecom-request@eecs.nwu.edu.

I'm not the moderator of the Telecom Digest; Patrick Townson is.

> [Occasionally someone kindly forwards RISKS-relevant TELECOM stuff to me, and Patrick sometimes picks up RISKS stuff. I'm not sure he is prepared to handle the enormous volume of TELECOM RISKS that I am currently experiencing, but for those of you who also are reading TELECOM, that might be a better place for some of the more detailed stuff. However, RISKS cuts across all disciplines and technologies, and I think it is important that its perspective be as inclusive as possible -- precisely because the risks themselves transcend artificial boundaries and because the lessons to be learned do also. Thanks, Nigel. Peter]

Report problems with the web pages to the maintainer

Search RISKS using swish-e

THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

ACM Committee on Computers and Public Policy, Peter G. Neumann, moderator

Volume 11: Issue 32

Thursday 21 March 1991

Contents

A further lesson from DeTreville's cautionary tale (RISKS-11.30)

<wex@PWS.BULL.COM>
Thu, 21 Mar 91 14:57:16 est

One important lesson that John might have noted was:
- Use Paper and Pencil.

Long ago I learned that people will try to fix obvious problems before they read their email. Therefore, whenever I report a serious problem by email, I

also leave handwritten notes taped to the appropriate doors and keyboards so that anyone who sits down to fix the problem will see my note and be aware that something is not as they expect.

Of course, this is not perfect, as physical notes are sometimes not seen or are ignored, but it has saved me many times when email didn't work or wasn't read until "too late."

--Alan Wexelblat, Bull Worldwide Information Systems phone: (508)294-7485

Another anecdote about automatic transfer systems

Ken Mayer <ken@visix.com>
Wed, 20 Mar 91 12:25:25 -0500

Several years ago, when I began working for a new employer, I was given the option of direct deposit for my weekly paycheck. I also opted to have a certain amount of money transferred to my savings account from my checking account on a monthly basis. Due to a clerical error, the automatic transfer started one month earlier than I expected causing undo embarassment when many of my checks bounced. When I complained (not only was I billed overdraft charges, I had to pay a returned check fee at my other bank, one of my credit card carriers and the electric company), the bank droid shrugged her shoulders and said (basically), "Tough luck, bozo."

Infuriated, I immediately closed my account and took my business elsewhere.

Here's where things get interesting: Even though the account was closed, the automatic transfer was not turned off! Every month for the next two YEARS I received a statement from this bank from hell that my account was overdrawn, my automatic savings transfer did not go through and I will be billed for insufficient funds. Every quarter I got a letter stating the my account balance was negative and I should call the local branch to straighten it out. Speaking with the bank the bank manager, I got a lot of apologies, and explanations how the computer needed the right incantation and he didn't know it. (He really was a nice fellow, it was just that this particular bank's data processing system was written before electric power was popular.)

The letters stopped coming when I moved to another state.

Ken Mayer, Technical Support Engineer, Visix Software Inc. 703.758.8230
...!uunet!visix!ken ken@visix.com

Re: "What the laws enforce" (TK0JUT1, RISKS-11.30)

CDC Contractor Bob Johnson;SCSS; <robjohn@logdis1.oc.aflc.af.mil>
Wed, 20 Mar 91 11:35:39 -0600

Begging your pardon, but there is a great difference between trespassing on my property and breaking into my computer. A better analogy might be finding a trespasser in your high-rise office building at 3 AM, and learning

that his back-pack contained some tools, some wire, a timer and a couple of detonation caps. He could claim that he wasn't planting a bomb, but how can you be sure? As a prudent office-building-owner, wouldn't you call in the police bomb squad, and deny access to the tenants until the whole building had been inspected and been declared safe?

My system has over 2,000 users, and well over 70,000 files. When we have a breakin (and we have had a couple), how much time is it going to cost me to do a complete audit of the operating system executables and configuration files, have all the users change their passwords and inspect their files for damage, analyze the intruder's activity and plug the security hole, document the intrusion for law enforcement agencies, and pursue prosecution (if we so decide)? Just counting the direct cost of manpower, the sum involved is many thousands of dollars. Under federal law (as I understand it) - any breakin that causes more than $5,000 of damage is a FELONY. This includes the incidental costs mentioned above. I am for making the penalties for computer trespass extremely painful to the perpetrator. Perhaps in this fashion we can encourage these people to find a more productive use of their time, and can avoid the cost of cleaning up and verifying our systems after these events.

Most administrators who've had to clean up and audit a system of this size probably think that a felony rap is too light a sentence. At times like that, we tend think in terms of boiling in oil, being drawn and quartered, or maybe burying the intruder up his neck in an anthill.

Re: "What the laws enforce" (Leveson, RISKS-11.31)

<TK0JUT1@NIU.BITNET>
Tue, 19 Mar 91 16:23 CST

In RISKS 11.31, Nancy Leveson takes exception apparently to my "analogy" of computer hacking to trespassing on grass and argues with passion that computer trespass is uncool. Sorry, but that analogy wasn't mine, and I was responding to it. The point isn't whether we approve or disapprove of hacking or computer trespass. Most of us agree it's at best tacky, at worst dangerous. Most of us agree that some social response is needed to both proactively and reactively curtail trespass and other predatory behavior in all its forms. The question is what are the most appropriate legal responses to computer trespass and what are the problems with current attempts to invoke criminal penalties for it?

Those of us who have followed the recent secret service cases are concerned with the application of comfortable legal definitions to new forms of offense for which those laws may not be appropriate. The current metaphor of hacking as "home entry" and applying sanctions comparable to B&E seem neither accurate nor just. Equating credit card fraud and other forms of rip-off with hacking only adds to the confusion. By accepting the trend to apply former metaphors to new conditions, we risk setting precedents that affect how computer behavior, access to information, and other emerging problems faced by computer hobbyists will be handled in the coming decades.

Few objected to the enactment of RICO laws, and fewer still to the laws allowing confiscation of property of drug suspects. The attitude seemed to be

that harsh measures were justified because of the nature of the problem. Yet, those and similar laws have been expanded and applied to those suspected of computer abuse as we see in the cases of Steve Jackson Games, RIPCO BBS, the "Hollywood Hacker," and others have been raided under questionable circumstances. The Hollywood Hacker illustrates some of these problems. Stuart Goldman, an investigative journalist, appears to have been set up and caught accessing the computers of the Fox network by using an account to which he apparently was not fully authorized. In a media event-type raid (Fox cameras were present), the SS and Los Angeles police raided him in March '90, took his equipment, and he faces a five year sentence for what appears, according to the indictment, to be at worst a trivial offense, at best a peccadillo for which an apology, not a sentence, is appropriate.

I'm wondering: What does law think it's enforcing? What is the appropriate metaphor for computer trespass? What distinctions should be made between types of offense? Please remember, nobody is justifying trespass, so continual harangues on its dangers miss the point. I am only suggesting that there is a greater risk from misapplication of law, which--like a virus--has a historical tendency to spread to other areas, than from computer hackers. It's easier to lock out hackers than police with guns and the power of the state behind them, and we have already seen the risks to people that result from over-zealous searches, prosecution, and sentencing.

[Still trying to be semianonymous? PGN]

Re: "What the Laws Enforce" (Leveson, RISKS-11.31)

Ernesto Pacas-Skewes <skewes@CAD.MCC.COM>
Wed, 20 Mar 91 12:14:58 CST

> ... Although such laws may not discourage true criminal behavior, they do
> discourage potentially destructive "play" by essentially law-abiding people.

They also discourage potentially constructive "play" by essentially law-abiding people. Knowing that you will be severly punished if you (maybe unintentionally) hurt somebody else tends to discourage initiative. Knowing that you are in an environment where you cannot hurt any body else tends encourage it. Your caution is also affected in opposite directions. The relative benefits of (and relation between) initiative and caution are debatable, the key, as with most anything else, is to strike the "right" balance. Many other qualities and values come into place, I am only trying to illustrate that severe laws by themselves don't cut it, and that laws that are "too" severe may even be counterproductive.

> In fact, personal and business privacy and property is extremely important
> in a complex, crowded society such as ours.

Completely agree, I would even remove the complex and crowded society.

> ... an important system that may save lives (or cost them if done wrong)
> because a company with which I need to deal has had to severely
> restrict outside computer access because of security fears.

I fail to see how doing it right or doing it wrong is related to the access to secured data unless doing it right means doing it on time. If the right/wrong doing is determined by the accessing of secured data there may be a major hole in that system.

> ... Draconian security
> measures to prevent frivolous access and pranks (in situations where it would
> not otherwise be necessary because there is nothing of value to steal) will
> hurt us all and cost our society untold dollars and perhaps worse.

The value, I think, is determined by whoever decides to impose the draconian security measures, if there is none, why bother? Well ..., maybe a lawyer would be able to find the "appropiate" value, and envolving lawyers almost always hurts and may cost untold dollars.

The draconian security measures imposed by the company you refer to, at least warn you that somebody already places value on the data you need to access and these measures may very well save you from getting bitten by the severity of the laws that you are rooting for. You request the data, the company's system gives it to you, the company's lawyer finds out you got the data and decides you are a good money maker, you pay more for crimes than for misdemeanors. Or is the lack of protection and implied authorization?

I value my privacy, I try to protect it (if the law helps, even better).

Ernesto

Re: California, driving, and privacy, again (RISKS-11.31)

Caveh Jalali <caveh@csl.sri.com>
Tue, 19 Mar 91 14:53:38 -0800

The major concern I have about Automatic Vehicle Identification (AVI) systems is that they might make life too easy for our friends at the law enforcement agencies. Photo radar is bad enough -- now our car could turn into a credit-card-on-wheels for anyone who needs to balance their budget for that month! instead of taking a picture, the camera would simply emmit the query signal, and record your car's ID. The speeding ticket, parking ticket, etc... could be in the mail before you even realize you did anything illegal.

Re: California, driving, and privacy, again (Hibert, RISKS-11.31)

Flint Pellett <flint@gistdev.gist.com>
20 Mar 91 17:43:18 GMT

Sometimes people can't seem to see the forest for the trees. If the roads were paid for out of general funds like income tax money, (where there is already a mechanism and bureaucracy in place for collecting it) then there would be no need to build expensive toll booths, invest in transponders for cars, or bar code readers and a new sticker every month, or any of that other stuff: you wouldn't have to hire people to maintain the equipment and install it and collect the money. You could actually spend all the money that is going toward

that technology and bureaucracy building roads instead! And nobody would have to complain about waiting in line at the toll booth ever again! (But wait: then people might be able to see how much tax they are really paying!)

IMHO: the main RISK this is demonstrating isn't the risk to privacy involved in having toll booths able to track your movements, it's the risk of inventing technology that is going to create more problems (and expense) when we wouldn't need that technology at all if we just addressed the social and political problems (taxes that are too high, so we disguise them as tolls, etc.) we started with. But technological problems seem to be easier to solve than political ones.

Flint Pellett, Global Information Systems Technology, Inc., 1800 Woodfield Drive, Savoy, IL 61874 (217) 352-1165 uunet!gistdev!flint

---

Re: California, driving, and privacy, again

Jurjen NE Bos <jurjen@cwi.nl>
21 Mar 91 10:10:08 GMT

There is still a better solution:
- The user is fully anonymous
- The box is the car is owned by the user, not by the government
- The user has smart card containing his money
- Opening the smart card only allows limited damage to the system
- Fast payment (20 ms) over IR
- extendible to phones, public transport, shops, etc

The system is called SmartCash and is developed by our neighbors, DigiCash.

Re: Pilot Error - an impartial assessment? (Hollombe, RISKS-11.31)

Christopher Stacy <CStacy@STONY-BROOK.SCRC.Symbolics.COM>
Tue, 19 Mar 1991 17:09-0500

> If the pilot's dead, it's his fault.

In a regulatory sense, this would generally be true, because the Federal Aviation Regulations are written that way. That is, the FAR's can be interpreted to basically say, "it's always the pilot's fault." In a legal sense, sometimes the aircraft manufacturer or someone is held partly or totally responsible. NTSB reports almost always cite multiple contributing factors, often putting some of the blame on controllers, airline practices, poor FAA regulations, and pilots. There is almost always something the pilot "could have" done, if he had thought of it, and such things are at least useful hindsight. Those are three common ways for finding fault, and they often come up with different answers. "Fault" is a slippery concept, and it's risky make broad generalizations about a complicated domain, based on simple bottom-line analysis that don't make their motivations explicit.

Fast Food and locked cash registers

Jonathan Leech <leech@cs.unc.edu>
21 Mar 91 17:10:46 GMT

In RISKS-11.30, Dwight McKay says ``I can see it now, "Sorry, we cannot give you a drink right now, our computer is down."'' A similar incident happened to me a few weeks ago. While getting lunch (loosely speaking) at Taco Bell, a fire down the street cut power. I happened to be about to pay at the time. Not only could they not take any further orders, they couldn't accept payment as the cash register would not open. At least I got lunch for free.

RISKS of digital voice forgery exaggerated

Fernando Pereira <pereira@research.att.com>
Wed, 20 Mar 91 14:45:31 EST

It is the opinion of colleagues of mine working on speech recognition and speech synthesis that the risk suggested by David Turner of digital voice forgery from small speech samples is negligible. As everyone knows who has dialed up a modern voice mail system or directory assistance service, sentences constructed by concatenating prerecorded words sound very unnatural. More sophisticated methods, which to some extent handle co-articulation (interword transitions), require much greater amounts of speech data, and they still fall far short of natural speech, particularly in the correct modeling of speech durations and intonation. My colleague David Talkin says: ``It is MUCH more likely that a human mimic could listen to the short passages and subsequently perform successful voice forgery.''

Fernando Pereira, 2D-447, AT&T Bell Laboratories, 600 Mountain Ave,
Murray Hill, NJ 07974

Report on ACM's position on privacy (in response to Lotus Marketplace)

<SIMONS@IBM.COM>
Tue, 19 Mar 91 18:50:11 PST

The following statement was passed by ACM Council and will be issued as a press release:

> Whereas the ACM greatly values the right of individual privacy;
>
> Whereas members of the computing profession have a special responsibility to ensure that computing systems do not diminish individual privacy;
>
> Whereas the ACM's Code of Professional Conduct places a responsibility on ACM members to protect individual privacy; and
>
> Whereas the Code of Fair Information Practices places a similar

responsibility on data holders to ensure that personal information is accurate, complete, and reliable;

Therefore, be it resolved that

(1) The ACM urges members to observe the privacy guidelines contained in the ACM Code of Professional Conduct;

(2) The ACM affirms its support for the Code of Fair Information Practices and urges its observance by all organizations that collect personal information; and

(3) The ACM supports the establishment of a proactive governmental privacy protection mechanism in those countries that do not currently have such mechanisms, including the United States, that would ensure individual privacy safeguards.

==========

Here is some information on how to join ACM.

The RISKS forum is an ACM sponsored activity. ACM is also getting more involved in the kinds of issues represented by RISKS and the above statement. If you support these activities and are not currently a member of ACM, I urge you to demonstrate your support by joining. You can obtain a membership application from any issue of CACM. If you can not get ahold of CACM, you can obtain an application from:

ACM, P.O. Box 12114, Church Street Station, New York, NY 10257

The costs are:
$71 Voting Member (You are asked to have a Bachelor's degree,
equivalent level of education, or four
full-time years of experience. The Bachelor's
does not necessarily have to be in computer science.
I don't know if it has to be in a related area.)
$71 Associate Member (No membership requirements)
$21 Student Member (You must be a registered student at an accredited
educational institution, and a faculty member must
certify your status.)
$66 Joint member of the IEEE-Computer Society
$57 Member of one of the following overseas computing societies
ACS (Austraila), AFCET (France), AICA (Italy) BCS (United Kingdom)
BIRA/IBRA (Belgium), CIPS (Canada), CSZ (Zimbabwe), GI (Germany),
HKCS (Hong Kong), ICS (Ireland), IPA (Israel), IPSJ (Japan),
NGI (Netherlands), NZCS (New Zealand), SCS (Shanghai).

Spouse members:
Voting Members 1st person + CACM $71 2nd person, no CACM $48
Student Members 1st person + CACM $21 2nd person, no CACM $14

$35 Retired members (Annual income from part time and consulting work
does not exceed $2500; age + years of ACM membership
must exceed 75)

One can also join a SIG without joining ACM. While that would be less expensive than joining the SIG and ACM, it would not be as effective in demonstrating support for the activities listed above.

Barbara Simons, National Secretary, ACM

ISM Workshop Announcement

Brian S. Hubbard <hubbard@TIS.COM>
Wed, 20 Mar 91 15:42:55 -0500

Sponsored and Administered By: TIS, TRUSTED INFORMATION SYSTEMS, INC.
In Coordination With: DIS DEFENSE INVESTIGATIVE SERVICE

The 1991 Industrial Security Manual:
A Workshop on Satisfying NEW Requirements
For Site Approval of Automated Information Systems
Washington, D.C., 7-9 May 1991
Los Angeles, California, 14-16 May 1991

In order to process classified information using automated information systems (AISs), a contractor site must receive approval by the Defense Investigative Service (DIS). The requirements for such site approvals are stated in Chapter 8 of the Industrial Security Manual (ISM), DoD 5220.22. At the invitation of DIS, Trusted Information Systems, Inc. participated in the development of the 1991 Industrial Security Manual which was promulgated by the Director of DIS in January 1991. This revision of the ISM reflects the requirements of DoD Directive 5200.28. The process of receiving site approval has been administratively streamlined; however, the requirements themselves have been made technically more sophisticated and exacting. The revised requirements also offer a more realistic approach to addressing threat and risk. Part of this latest revision requires contractors to meet the requirements of DoD 5200.28-STD, the Trusted Computer System Evaluation Criteria or TCSEC, commonly known as the "Orange Book".

In order to explain the new requirements of the ISM and their application to specific processing environments, Trusted Information Systems, Inc. in coordination with the DIS is sponsoring and administering a comprehensive three-day workshop. This workshop is being developed by developers of the new requirements.

Lecturers include Stephen T. Walker (TIS), Carole Jordan (Defense Investigative Service), Marvin Schaefer, Charles P. Pfleeger, William C. Barker (TIS)

For further information, contact Brian at hubbard@TIS.COM or Trusted Information Systems, Inc., Attn: WORKSHOP COORDINATOR, 3060 Washington Road, Glenwood, MD 21738, Phone: (301) 854-6889 FAX: (301) 854-5363

Search RISKS using swish-e

Report problems with the web pages to the maintainer

Search RISKS using swish-e

THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

ACM Committee on Computers and Public Policy, Peter G. Neumann, moderator

Volume 11: Issue 33

Friday 22 March 1991

Contents

A billion here, a billion there... [$B column omitted]

Saul Tannenbaum <SAUL_SY@hnrc.tufts.edu>
Fri, 22 Mar 91 00:05 EDT

The following Editors' Note appeared on Page 3 of the New York Times, Thursday, March 21:

> Because of a computer typesetting misadjustment, the Money Market Funds table appearing in Business Day each Thursday since February 14 has carried incorrect figures for the total assets of some funds and for their yields. The asset figures have omitted the billions column for amounts of $1 billion of more; a fund, for example with assets of $12.345 billion would have been shown with $345 million. In addition, since Feb. 21, the column labeled 7-day yield has actually shown the 7-day effective yield, a higher figure.

> Readers reported the erros soon after they first occurred, but through an editing laps, the table continued to appear while repairs where awaited.
>
> A corrected format begins today on page d9. It includes both the 7-day yield and the effective 7-day yield, but omits the assets.

At least Fortran would have printed *'s....

Saul Tannenbaum, Manager, Scientific Computing, USDA Human Nutrition Research Center on Aging at Tufts Univ., STANNENB@HNRC.TUFTS.EDU STANNENB@TUFTS.BITNET

Sprint says NO to increased account security

Lauren Weinstein <lauren@vortex.com>
Thu, 21 Mar 91 13:15:41 PST

There have been reports in various forums recently of various concerns regarding U.S. Sprint's new policy of allowing access to almost all (1+ long distance dialing) customer account balances based only on 10 digit phone numbers (previously, account numbers had been needed to obtain such information). Account balances for all phone numbers with 1+ service selected to Sprint, except for those customers connected to Sprint by high volume leased line facilities (e.g. T1) are apparently accessible via the system.

Concerns have been expressed about misuse of this data by outside organizations, competitors, or even other carriers looking to target the "big" customers. Certainly most people have been assuming that the amount of their long distance bills was not "public" information.

I have been following this rather closely, and over the last several weeks have had a complaint working its way up the chain in Sprint. As a user of Sprint (as well as other carriers) I personally feel that account balance information should be private between the carrier and the customer. If reasonable protections cannot be provided for that information in automated systems, customers should at least have some method for "opting out" of the automated account system itself.

Sprint has been very good about staying in touch about this issue. The "end of the line", so to speak, has been Ms. Rochelle Richter at the Sprint Executive Offices. She's an "Executive Analyst" in the offices of the President of Sprint (Mr. LeMay) and the Sprint CEO (Mr. Esrey). She tells me that they have been informed of the concerns I expressed over this system. The number for the Sprint Executive Offices where Ms. Richter (or the other persons mentioned above) can be reached is (800) 347-8988. Ms. Richter also discussed the issue with the gentleman in charge of the development and management of the automated system itself, Mr. Rick Shield at (816) 276-6242.

I'm sorry to report that Sprint at this time does not view the privacy issues involved as a problem. They do plan to add a requirement that users enter their zipcode as well as their 10 digit number, apparently viewing the zipcode as a security measure. I assume that most of us agree that the addition of the

zipcode does not represent any real security improvement, since it is trivially available to anyone who wants it in most cases.

The Sprint view is that they have had very few complaints from customers about the system (she claims only two), that they don't see what the concern is about account balance information, and that they haven't heard of any similar systems causing problems for the customers or the companies providing information.

She invites those with concerns about this issue to contact her directly at the toll-free 800 number above. She made it clear that unless they get significant numbers of complaints from customers, there is currently no intention for any change other than the "zipcode" requirement mentioned above. She also invites comments to herself or Rick Shield from persons who have documented evidence of the privacy/security problems which could result from such systems.

If any of you are Sprint customers and *are* concerned (either as an individual or as an organization) about the privacy issues involved with this system, or even if you are a non-customer and can offer Sprint some insight into the issues involved, I would suggest that each of you take Ms. Richter up on her offer and express your views, so that Sprint will have more opinions on which to base any future decisions about their system.

--Lauren--

"What the laws enforce" (Jim Thomas, alias TK0JUT1, RISKS-11.30)

<P.E.Smee@gdr.bath.ac.uk>
Thu, 21 Mar 91 18:10:42 GMT

>... One can oppose trespass while simultaneously opposing Draconian attempts
> to stomp on those who tread >tackily in our once-pastoral fields.

There is a very tricky balancing act involved, though, and I don't believe that the 'physical trespass' analogy holds very well. Seen from the point of view of the person whose system is being hacked, the amount of time and manpower required to 'resecure' a system after it's been hacked is approximately the same regardless of whether the 'hacker' committed destructive acts, or simply logged in and straight back out. It takes a long time to make sure that data integrity has been preserved, and that no trapdoors or trojan horses have been left behind. Thus, from the point of view of the victim, even 'harmless hacking' results in a great amount of damage.

As for 'forbidden knowledge', what does that include? I'd regard it as VERY serious if someone has, for example, a plaintext list of usernames and passwords for our system, even if they haven't used it. You never know when they will. They've effectively got a gun at your head.

I confess to having difficulties with all this, for which I don't have an easy answer, because I do hold the (officially forbidden, here) belief that 'hacking' (in the most general sense) can provide a very valuable educational experience for the hacker -- and we are supposed to be an educational institution. At the same time, though, I deeply resent the time I lose whenever I've got to help clean up after one -- even if, after a week of

investigation, we find that nothing harmful has been done. I would certainly like to find a solution for all this.

Re: "What the laws enforce" (Johnson, RISKS-11.32

Mike Godwin <mnemonic@eff.org>
Thu, 21 Mar 91 16:24:05 EST

>...He could claim that he wasn't planting a bomb, but how can you be sure?

This is an insupportable analogy. Few breakins have as much evidence of malicious intent as Bob's example here. There is no way to "be sure," as Bob correctly points out. But it takes minimal understanding of the "cracker" subculture to determine that very few have malicious intent.

It is a premise of our legal system that criminal prosecutions be based on a culpable mental state on the part of the person who is convicted. If kids or anyone else damages a system accidentally and/or non-maliciously, the proper legal remedy is civil litigation. (An even better remedy, of course, is to be nonnegligent as far as maintaining attractive nuisances go. In the case of the Atlanta hackers, for example, the touted E911 document was copied from a computer that was accessed through an account with a null password. The kids got 14 to 21 months.)

> As a prudent office-building-owner, wouldn't you call in
>the police bomb squad, and deny access to the tenants until the whole
>building had been inspected and been declared safe?

If your office was entered after you took too few measures in maintaining building security, it's a little late to show prudence when the mad bomber has already shown up, I'd think.

>When we have a breakin (and we have had a couple), how much time is it
>going to cost ...

It costs much less to practice good security in the first place.

> Just counting the direct cost of manpower, the sum involved is many
>thousands of dollars.

It is perfectly appropriate to sue to recover this amount. This is a civil proceeding, not a criminal one, however. Or did you think that the purpose of the criminal-justice system was to save you litigation costs?

> I am for making the penalties for computer trespass extremely painful ...

Nothing disturbs me more than people who blithely call for more and harsher criminal laws. It is apparent when one studies the criminal justice system in this country that we prefer to criminalize some activities rather than make responsible policy decisions. More than a million people are in jail (the highest rate of imprisonment in the world, when I last checked), yet we don't want to build new jails for them.

Oh, yes--*much* wiser to send some 19-year-old kid to prison on the basis of a bankrupt theory of deterrence than to make sure he doesn't get in in the first place.

And let's remove the requirement of criminal intent for conviction, shall we? Let's expand the criminal law to include anything and everything that is inconvenient, or that we don't like.

>Most administrators who've had to clean up and audit a system of this size
>probably think that a felony rap is too light a sentence. At times like that,
>we tend think in terms of boiling in oil, being drawn and quartered, or maybe
>burying the intruder up his neck in an anthill.

It is precisely this kind of mentality that was so common, once upon a time, in concentration-camp guards. It is amazing to me that one can admit this sentiment in public without embarrassment.

Mike Godwin, Electronic Frontier Foundation (617) 864-0665 mnemonic@eff.org

---

Re: "What the laws enforce" (Johnson, RISKS-11.32)

Neil Rickert <rickert@cs.niu.edu>
Thu, 21 Mar 1991 22:42:45 GMT

>Begging your pardon, but there is a great difference between trespassing
>on my property and breaking into my computer...

Begging your pardon, but there is a great difference between logging into a computer using an account with no special privileges, and being found in a high-rise with wire and detonators.

Let me describe a couple of experience from my past. They occurred in the 1970s. At that time I had an account on our campus (the campus I was at then) mainframe. The account had no special privileges. I was a faculty member, and not part of the computing services staff.

Experience 1: While using a feature of the editor, I noticed a suspicious discrepancy. Exploring this, it looked like a security problem. To test this, I attempted to submit a job under the identification of one of the Systems Programmers. Actually I submitted an essentially null job (IEFBR14 for those who recognize this name). My submission was successful. I immediately reported it to the System's Programmer, who fetched the output of his (my) job, and immediately set to work to remove this misfeature from the editor.

Experience 2: While using a software debugging system, I noticed a suspicious feature. Exploring it, I discovered I could change the contents of a register used by the system when in a highly privileged state (Supervisor State). The bit I actually changed was an insignificant bit with no purpose, but I could equally have changed any register and gained control of the system.

> I again reported this to the Systems programmer, who immediately set to work documenting it so as to report it to the vendor.

What is the relevance of these experiences?

Simply this. If the same circumstances occurred again, I would take the same action. I would consider it unethical NOT to act as I did.

Yet, some people in these discussions of intrusion, etc, would define my actions as computer crime, punishable by lengthy prison terms. Sure, in the circumstances, they would probably exonerate me based on my motives. But still their definition of computer crime is wrong. It is a head in the sand approach which pretends that if we just punish the 'criminals' the problems will go away. They won't.

Neil W. Rickert, Computer Science, Northern Illinois Univ., DeKalb, IL 60115
+1-815-753-6940 <rickert@cs.niu.edu>

Old Soviet spacecraft loss attributed to software

<henry@zoo.toronto.edu>
Thu, 21 Mar 91 23:10:09 EST

An interesting report from Bart Hendrickx of Belgium in the April issue of Spaceflight, based on a newly-published Soviet book about unmanned Mars exploration (Yuriy Markov, "Kurs Na Mars", Mashinostroyeniye, Moscow 1989). In part, he writes:

> As is known, one of the three Soviet [Mars] probes readied for the 1971 launch window got stranded in Earth parking orbit and was renamed Cosmos-419. It now turns out this was intended to become Mars' first artificial satellite. Unlike its companions Mars-2 and 3, which were combined orbiter/landers, Cosmos-419 merely consisted of an orbiter. The resulting weight reduction would have allowed it to fly a faster trajectory and reach Mars orbit ahead of America's Mariner-9, clinching another major first for the Soviet space programme. The probe failed to leave Earth orbit due to a "most gross and unforgivable mistake" made by programmers during the input of code-numbers into its on-board computer.

(No further details, alas.)

Henry Spencer at U of Toronto Zoology

Fake Cashpoint duped Customers

paj <paj@gec-mrc.co.uk>
22 Mar 1991 11:42:58-GMT

A report on the back page of the 21 March Computer Weekly describes a home-made

box with a keyboard which was placed on a cashpoint machine in Hove, England. It seems that four customers put their cards in the box and typed in their PINs. The machine then recorded the PIN and kept the cards. The intention appears to have been to remove the box and use the cards and PINs to extract money from real machines. A fifth customer became suspicious and called the police.

Jean Paul English was arrested and plans for the box were found in his home. He told police that he made the machine out of curiosity. When tried at Lewes Crown Court he denied two charges of forgery but admitted to one specimen charge of stealing a cash card. The fake ATM did not fall within the definition of an `instrument' in the 1981 forgery act.

This relates somewhat to the `droid' discussion last week in RISKS. Its not just in shops and customer service departments that the droid mentality shows up. It does not seem to have occured to the first four customers that the box might not be official or that it could be removed (and hence could not contain cash). I suppose they just expected to get their cards back from it.

Paul Johnson, GEC-Marconi Research +44 245 73331 paj@gec-mrc.co.uk
UUCP:<world>!mcvax!ukc!gec-mrc!paj

Solutions Incorporated FaxGate software

<jwn2@qualcom.qualcomm.com>
Fri, 22 Mar 91 08:17:23 -0800

>Sender: "QuickMail (CE Software) Users" <QM-L@YALEVM.YCC.Yale.Edu>
>From: Peter Furmonavicius <PETER@YALEVM.YCC.Yale.Edu>
>Subject: Solutions Incorporated FaxGate software
>
>Recently, I mentioned our use of facsimile networking software called
>FaxGate, from a company called Solutions Incorporated. I would like to
>warn anyone considering the use of this package about a potentially
>serious security problem. FaxGate prepends the lines from the "Address"
>portion of the Special Address dialog box to every fax that it transmits.
>However, this is where the user must specify the phone number for the
>outgoing fax that they wish to be sent. So what's wrong with that?
>Well in lots of sites I'm sure, users that wish to send non-local
>faxes must append their phone credit card numbers or local toll
>authorization numbers to the outgoing 'long-distance' phone number.
>And this would consequently get printed at the remote site where the
>fax is sent! We have found this to be unacceptable and are therefore
>discontinuing our use of this software until the problem is corrected.
>If anyone has any further comments or corrections (or circumventions),
>let's hear them. Thanks.
> Peter

Long-dormant bugs

Martyn Thomas <mct@praxis.co.uk>
Fri, 22 Mar 91 15:27:18 GMT

All the theoretical work on software reliability demonstrates that there should be very many paths which are rarely executed, in most software.

That is why we are so concerned about the difficulty of establishing the probability of failure of software, when the target probabilities are very low.

We should therefore *expect* reports of bugs showing up after a very long time. It is evidence that the problems we identify are real.

There isn't much software out there which has been running for 20+ years - but the amount is growing very quickly. We can expect an increasing number of anecdotes about long-dormant bugs, until they become commonplace and not worth remarking.

Martyn Thomas, Praxis plc, 20 Manvers Street, Bath BA1
1PX UK. Tel: +44-225-444700. Email: mct@praxis.co.uk

Search RISKS using swish-e

THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

ACM Committee on Computers and Public Policy, Peter G. Neumann, moderator

Volume 11: Issue 34

Monday 22 March 1991

Contents

Re: A cautionary tale

David Shepherd <des@inmos.com>
Mon, 25 Mar 91 10:54:06 GMT

The problems with a rogue machine updating name service tables at SRC sounds similar to problems I experienced when we were changed our internet address to a class B address. On the relevant friday evening alll machines in the company (then about 100 assorted Suns etc and a few microVaxes) were to be taken down updated at the same time. This included about 4 SparcStations at our manufacturing plant at Newport 30 miles away which is linked to our network. Our system adminstrator here told the adminstroator in Newport that the switch would take about half an hour so their machines should be shutdown between 6 and 6:30 and these would be updated over the weekend. Needless to say the switch took longer (it didn't start till after 6:30 in any case) and when I tried to reboot the SparcStation in my group half of them failed as they decided to take they NIS information from a NIS server in Newport (i.e. one 30 miles away rather than just down the corridor - they had never done this

before!) which now contained old internet addresses which were completely wrong.

After several reboots to try and get the machines to choose a Bristol NIS server, which failed, I gave up and left the computer support staff to get things sorted out over the weekend, which, fortunately, they did.

It is very infuriating to know that you cannot boot your systems because of a rogue machine which you cannot switch off because its 30 miles away!

david shepherd: des@inmos.co.uk or des@inmos.com tel: 0454-616616 x 529
inmos ltd, 1000 aztec west, almondsbury, bristol, bs12 4sq

Re: What the laws enforce

"Michael J. de Mare" <demarem@clutx.clarkson.edu>
Sat, 23 Mar 91 15:27:40 EST

P.E.Smee@gdr.bath.ac.uk expressed concern that it would be inappropriate to excessively punish hackers in spite of the amount of work required to check the system even after simple trespass because the hacking has educational value. I think that it has value to the systems administrater as well as the hacker do to security flaws revealed (although I have noticed that there tends to be hesitation in correcting such flaws be- cause the fixes tend to take a certain degree of flexibility out of the system). I think that in spite of the benefits, the costs make instances of hacking intolerable.

I think that sites that are uncomfortable with dealing strictly with hacker should set up a machine specifically for hacking into. The idea being that anything on it should be considered at risk, but anyone who does there hacking on other machines will be dealt with very severely. The hacker would get whatever educational value exists without imposing large amounts of work, cost and inconvience on others, the system administraters could discover weakness by monitering the hacking system. The catch is that there is an overhead cost in purchasing and maintaining the system which institutions would, justifiably be hesitant to pay.

Mike

Re: "What the laws enforce" (Godwin, RISKS-11.33)

Gene Spafford <spaf@cs.purdue.edu>
25 Mar 91 04:27:23 GMT

Mike Godwin makes the point that intent is part of the usual process of applying criminal law, and that the usual "hacker culture" (an oxymoron?) does not condone or encourage malicious intent. Perhaps that is true, but that does not convince me of anything -- it's like saying that the majority of car thefts are done by kids with no intent to keep the cars, so auto theft should be a minor crime. The act is what is illegal, not the intended result (although the results may result in other charges, like vehicular homicide). The intent portion is demonstrated by breaking in to something/some place that the

offender has no permission to access.

I must defer to Mike on questions of law as he has a law degree and is (I assume) a member of the bar in some state(s). However, my understanding is that cases where people only intended to frighten or intimidate another but had their plans go awry do happen. The intent may have been simple hooliganism (say, assault or malicious mischief at worst), but the charges that result may be battery, manslaughter, arson, or any number of other more serious charges. The intent involved was that of doing something criminal, even if the result was not what was intended; the charges are filed on the act, not on the claimed intended act.

The same should happen with computer breakins. The intent part is satisfied if it can be shown that they intended to access the system and knew they were not authorized to do so (via an authorized account or standard public mechanism). There is no question that the intruders know they are straying into territory they should avoid.

I don't think Neil Rickert's related experience is the same. He possibly exceeded his authorized access locally and reported it. That isn't the same as trespassing from outside. I'm assuming he knew something about the local security policy and had some legitimate access to begin with. Those are perhaps cases to be decided in a civil case, as per Mike's comments.

The problem comes from people who do not have legitimate access of any type. They intrude on systems without authorization and may (or may not) cause the owners difficulties. If I discover that people have broken into my office or my home, it is up to me to determine if they have altered the locks or stolen my coin collection. If I decide not to check, that is up to me. However, that doesn't alter the fact that breaking and entering has occurred, and is a chargeable offense, does it?

I'm not entirely clear on the law here, but I believe that the act (breaking and entering) is the same crime even if I fail to lock my door, correct? Isn't it the case that turning the doorknob and pushing open the door is considered "breaking" under the law? My insurance company may raise my rates or fail to reimburse me if I failed to use the lock, and as Mike noted, I can pursue civil action to recover the damages. I bear the costs and consequences of my carelessness. But the intent of the intruders is shown by their presence without authorization, with the door being locked or not.

I also don't think the "attractive nuisance" argument makes any sense. Suppose I own a Ferarri, and I lock the doors, then some kids steal it for a joyride. Are the thieves excused because the car would be considered an attractive nuisance and I didn't hire an armed guard to protect it 24 hours a day? I hope not! If I use standard locks on something generally accepted to be private property, I should have protection of the law. If I forget to lock the doors some night should not excuse the theft of the car, even if the thieves return the car with a full tank of gas. Again, my insurance rates may go up or fail to pay for damage if it can be shown that I failed to lock the car, but that does not result in the case being thrown out of court, does it?

Whether or not the majority of break-ins have been largely benign in intent *so far* does not mean they will continue to be so, or that

they are not sometimes damaging in ways not envisioned by the culprits. I agree that intent of malicious damage should make the charges more severe. However, I do not believe the lack of such proof means the break-in by itself is a minor crime. There is *no* ethically sound reason for people to break into systems they know they do not have permission to access. Likewise, such activity should not be treated lightly by the legal system.

Gene Spafford, NSF/Purdue/U of Florida Software Engineering Research Center, Dept. of Computer Sciences, Purdue University, W. Lafayette IN (317) 494-7825

Re: What the laws enforce (Rickerts, RISKS-11.33)

Joe Morris <jcmorris@mwunix.mitre.org>
Mon, 25 Mar 91 12:21:05 EST

[...]
>Yet, some people in these discussions of intrusion, etc, would define my
>actions as computer crime, punishable by lengthy prison terms. [...]

This isn't a valid situation to compare to a breakin by hackers:

(a) Your exploitation of the security exposure was limited to verifying that it did in fact exist.

(b) You were aware of the identity of the responsible manager (here, the sysprog) and, having verified that the exposure existed, sent that person sufficient information to identify and confirm the existence of the exposure.

(c) However unintended, the account *does* have special privileges in the security exposures.

Last, AND (IMHO) MOST IMPORTANT:

(d) You were authorized to be on the system, you were using the account issued to you for its intended usage, you became aware of the security exposure as a result of using your account for its intended purpose, and the computer center could identify you as the warm body behind the usage.

By definition, a user who logs into an account has access to the files authorized to be modified by that account. If the warm body who has logged into the account isn't the authorized user, that fits a working definition of "special privileges": access authority which the user should not be given but which is available.

Several years ago one of my VMS operators managed to crash the VMS system so hard that it took us two days to get everything back up to a stable production status. If this had occurred due to some unknown and unauthorized outsider's actions I would have had to expend a huge amount of resources to verify that no damage had been done to

the system itself or the users' data files, and I would treat the event as vandalism. Since the individual who triggered the failure was known to us, was an authorized and trusted user of the system, and there was a completely reasonable logic behind his actions there was no reason to distrust the integrity of the VMS system itself. (Reliability, of course, is a different issue. Thanks, DEC.)

Several other contributors to RISKS-FORUM have pointed out that much of the cost of electronic intrusions is in the work required to identify what (if any) files have been tampered with. Too many observers don't seem to understand that this is a major consequence of an intrusion, regardless of the actual damage which might or might not have been done by the intruder.

An apt comparison would be the recent cases in which Sudafed capsules have been tampered with. Sure, it's likely that only a few capsules actually have cyanide in them, but if you were the manufacturer or seller would you really want to sell them unless you had checked each capsule for tampering? How about the Tylonol (sp?) tampering a few years ago?

You want to have some fun? Go down to your local drug store and break the anti-tamper seals on some Sudafed boxes, then put the boxes (no cyanide, please...) back on the shelf. You haven't stolen any property, and (you claim) you haven't put poison in anything...but don't be surprised when the cops invite you to take a guided tour of the local jail unless you work for the drug store and discovered that the seals were broken during shipment.

One of the standard RISKS of computerized systems is that of unreliable data being used in automated systems. An unauthorized user, not accountable to the owner of a system, who deliberately enters a system and is in a position to corrupt data makes that data unreliable and thus of significantly reduced value to its owner. That's vandalism, and that in turn is a crime.

Re: What the laws enforce

"Neil Rickert, N Illinois U, CS" <rickert@cs.niu.edu>
Mon, 25 Mar 91 12:23:12 -0600

>This isn't a valid situation to compare to a breakin by hackers:

Maybe it isn't valid in your eyes, or in my eyes. But the question is not how you or I see it, but how lawyers, jurors and jurists, most of whom know zilch about computers, will see it. And they are wording and interpreting some of these laws in very scary manners.

-Neil Rickert

Re: "What the laws enforce" (Godwin, RISKS-11.33)

"Mike Gore, Institute Computer Research - ICR" <magore@watserv1.uwaterloo.ca>

Mon, 25 Mar 91 00:02:38 EST

>Oh, yes--*much* wiser to send some 19-year-old kid to prison on the basis of a
>bankrupt theory of deterrence than to make sure he doesn't get in in the first
>place.

Yet is prevention our *only* concern ? I fully agree that a better theory of deterrence should be sought as well as making it harder for someone to break-in. Yet if we only focus at fixing the system to make it harder to break-in we may fail to address another, and perhaps even much bigger, problem of what leads some people to think breaking in is such a minor social trespass in the first place. (Not to mention other issues that may be ignored in the process)

There is a risk here, that in trying to solve "the problem" that we distil everything down to single issue and or one source of blame.

Mike Gore, Technical Support, Institute for Computer Research
UUCP: uunet!watmath!watserv1!magore

---

re: "What the Laws Enforce" (Godwin, RISKS 11.33)

CDC Contractor Bob Johnson;SCSS; <robjohn@logdis1.oc.aflc.af.mil>
Mon, 25 Mar 91 01:20:47 -0600

> It is precisely this kind of mentality that was so common, once upon
> a time, in concentration-camp guards. It is amazing to me that one
> can admit this sentiment in public without embarrassment.

I'm one who likes to "stir the pot" once in a while - play the "devil's advocate", so to speak. I was intending to bring out the "other viewpoint", that taken by many government and commercial installations. A very real problem with breakins is that the collateral damage usually outweighs the actual damage. I purposely took the stance I did in order to balance out the discussion. Sometimes I feel that we computer professionals tend to take the distanced, analytical approach a bit too often. If I offended, I apologize. I certainly didn't expect it would elicit such a venomous response. However, I'd wager that Mike would harbor (albeit secretly) quite similar sentiments were he placed in the role of an administrator resecuring a system after it was compromised.

> It costs much less to practice good security in the first place.

Mike should talk to my superiors. They already think I'm completely paranoid. If I practiced any better security, it would be a full time job.

> ... Few breakins have as much evidence of
> malicious intent as Bob's example here...it takes minimal understanding
> of the "cracker" subculture to determine that very few have malicious intent.

Ok. Perhaps the malicious slant clouded the issue. I was trying to point out (through analogy) that we can't trust a hacker to truthfully tell us what

he/she was doing. I do feel that I have more than a minimal understanding of the "cracker" subculture, and I'm not inferring that phreakers/hackers (on the whole) are malicious. A royal pain, yes. Malicious, no.

> If kids or anyone else damages a system accidentally and/or non-maliciously,
> the proper legal remedy is civil litigation...It is perfectly appropriate
> to sue to recover this amount [cost of resesuring the system-bj]. This is
> a civil proceeding, not a criminal one, however. Or did you think that the
> purpose of the criminal-justice system was to save you litigation costs?

Perhaps Mike has a very valid point - maybe we should be asking for better civil laws instead of criminal ones. However, the laws that we have used to prosecute our intrusions are federal criminal laws. If congress can't get a good enough handle on computer crime to draft effective and timely laws, how are we going to prosecute these cases in local civil courts? And, most cases cross interstate boundaries, which makes them federal jurisdiction anyway. Perhaps we should try to prosecute crackers as federal civil cases? On what legislation and precident should we build our cases?

> It is apparent when one studies the criminal justice system in
> this country that we prefer to criminalize some activities rather than make
> responsible policy decisions.

Probably because our legislators feel that the laws should "scare the H*ll out of 'em", and that'll keep them from breaking the laws. The better way to address adolescent and post-adolescent system cracking would be some combination of education, instruction in ethics, and providing some other means of satisfying their curiosity. Unfortunately, even then there would be those thrill-seekers who would keep doing it. And there ARE malicious crackers (probably very few, but if they're good, they don't get caught). I guess we're still stuck with criminal laws, unless someone comes up with a workable way to overhaul the criminal justice system in America.

> More than a million people are in jail (the
> highest rate of imprisonment in the world, when I last checked), yet we don't
> want to build new jails for them.

Irrelevant.

> Oh, yes--*much* wiser to send some 19-year-old kid to prison on the basis of a
> bankrupt theory of deterrence than to make sure he doesn't get in in the first
> place. And let's remove the requirement of criminal intent for conviction,
> shall we? Let's expand the criminal law to include anything and everything
> that is inconvenient, or that we don't like.

Egad. Ranting a bit, aren't we? Must've touched a raw nerve or something. Purposely connecting to a system, ignoring posted warnings, and hacking into it by whatever means has been shown, in court, to signify criminal intent. And, I know of no 19-year-old kid who has gone to prison for computer cracking. A year or two of suspended sentence, some monetary reparations, confiscation of equipment, and a few hundred hours of community service are the typical sentences handed out to date. Face it, federal judges realise that these kids aren't hardened felons - many even have their records expunged if they adequately live up to their sentences.

For the record, I support much of the work of the Electronic Frontiers Foundation. I am very concerned about issues of privacy, ethics, and misuse of power and authority during investigations. However, like Clifford Stoll in "The Cukoo's Egg", I have been forced to expand my views to accomodate "the other side" - ie: the establishment. This problem is one which is not going to be solved soon or easily, and one which must be brought into open forums for indepth and thoughtful discussions. Does anyone have any ideas for attacking this problem? Myself, I favor mandatory computer classes in schools, with instructions on ethics, data ownership, and the applicable laws. Perhaps coupled with some sort of industry sponsored program or competition for "gifted computer students" - to give them something to work for. But this still doesn't address the social pressures that entice kids to enter the phreaking/hacking subculture in the first place...

Bob Johnson, Control Data Corporation (contractor to...)
Tinker Air Force Base, Oklahoma

---

re: "What the Laws Enforce" (Rickert, RISKS 11.33)

CDC Contractor Bob Johnson;SCSS; <robjohn@logdis1.oc.aflc.af.mil>
Mon, 25 Mar 91 01:24:11 -0600

> Begging your pardon, but there is a great difference between logging into a
> computer using an account with no special privileges, and being found in a
> high-rise with wire and detonators.

(Neil describes a couple of system security holes he found and investigated, and notes that he felt ethical and proper in doing that.)

> Yet, some people in these discussions of intrusion, etc, would define my
> actions as computer crime, punishable by lengthy prison terms...still
> their definition of computer crime is wrong. It is a head in the sand
> approach which pretends that if we just punish the 'criminals' the problems
> will go away. They won't.

I feel Neil was justified in doing what he did, and did the right thing. As a valid user, he checked into the problem and reported it to the proper authority. Had he been of a "cracker" mindset, he would have kept the knowledge to himself and shared it only with a few select friends. Had he used this newfound knowledge for personal gain, that would have (IMHO) been computer crime.

As Neil points out, there is a real problem classifying types of illicit usage of computing equipment. Consequently - it all gets called computer crime. Ergo, Neil's activities could be construed by some as a crime.

As another example - a while back, there was a documented hole in the uucp software in AT&T System V Unix. A couple of otherwise-responsible unixoids dialed up a well-known uucp phone number at the AT&T factory in Oklahoma City where the 3B's and 5B's are built. The system they called into is connected to the entire AT&T computer network - even back to Bell Labs.

The unixoids in question exercised the security hole, gained root access, poked around enough to determine that they were actually root, created a file with a message documenting the hole (created as root), and mailed a message to 'root' telling where to find the file. They considered it to be a public service, and they didn't break or change anything.

Recently, we hired one of the administrators who worked at AT&T during that time. It seems that the next day, the proverbial fecal matter hit the air movement inducer. The resulting crackdown and resecuring effort extended far beyond the one machine, and must have cost AT&T tens of thousands of dollars in manpower and programming.

Did they, in fact, do a public service - or did they commit computer crime? Was there a better way to bring the security hole to the attention of AT&T? Some have noted that hole was well-known for at least three years, and that Berkeley had closed the hole in the BSD versions soon after it was found. Apparently, "rubbing their noses in it" convinced them to fix it - a patch was distributed very soon thereafter (according to my sources).

Bob Johnson
Control Data Corporation (contractor to...)
Tinker Air Force Base, Oklahoma

Re: "What the laws enforce" (Rickert, RISKS-11.33)

"David A. Honig" <honig@ICS.UCI.EDU>
Mon, 25 Mar 91 17:37:06 -0800

>. high-rise with wire and detonators.

Which made me think: Given the presence of serious security holes in basically every operating system, is there such a thing as "an account with no special privileges", esp. for someone who's already found a way to break into a system?

I think the "you find someone in your high rise at 3AM with batteries, timers, and detonating caps" analogy might be amended to say, "you find someone in your high rise at 3AM who manages to destroy his backpack before you get to him, such that you have no clue what was in it and only his word as to his intentions..."

Security - break-ins and punishment

Chet T Laughlin <chetl@sparc19.tamu.edu>
24 Mar 91 23:11:28 GMT

I am somewhat puzzled as to how one can press for prison terms when the system that was entered is not even being protected by the administration and/or where there has been no demonstration of malicious intent toward the system or users. Maybe an example from "The Inner Circle" will help illustrate my confusion...

It seems that a teenage boy and one of his friends decided to trespass on Air

Force property. I believe the base was NORAD headquarters under the mountain. Now, they were caught and held in a room until their parents showed up. They were guarded by a soldier approximately 2-4 years older than they were. Their parents picked them up, both sets of authorities scolded them, and they were taken home. The Air Force knew exactly *how much of a threat* they were and I would quess, exactly *why* they were there - all those "do not enter signs." (EOE end-of-example)

Now. Some 14 year old hacker-wanna-be stumbles into my system after seeing an account name on the net. He/she quesses there is no password and makes that 1-1quintillion lucky chance. They stumble around trying "man this-that-the-other" "catalog" "help" "who" "dir" etc. Now, this isn't too hard to detect. A simple program that keeps track of who performed intro commands and which ones and when should flag this type of bumbling intruder. And its my fault for letting the system users have no password at all to start with.

Maybe this seems long winded, but pressing for time behind bars for this (strawman) seems overkill. Now, perhaps if I can demonstrate a DESIRE TO DESTROY or MALICIOUS INTENT I could see otherwise.

Chet Laughlin chetl@sparc21.tamu.edu

Re: Thumbs and authors ... (Wonnacott, RISKS-11.24)

"Herman J. Woltring" <UGDIST@NICI.KUN.NL>
Mon, 11 Mar 91 09:23 MET

Joking apart, current US legislation does no longer require a readable Copyright statement: with the ratification of the Berne Author's Rights / Copyright convention a couple of years ago by Uncle Sam, such formalities are no longer required for Copyright to apply in the USA. For e n f o r c i n g copyright in a US court of law, US citizens (both natural and legal persons) must, however, register their claim with the US Copyright Office within, I believe, a reasonable period from legitimate, first publication. Non-US citizens do not have to do so under Berne in order to maintain their rights in the USA.

I'm not sure what would constitute `(first) publication' of a finger print... And what about a father or mother forbidding his/her offspring to `copy' themselves via an unfavoured marriage or other relationship? Can (s)he ask the court to impound and destroy the illigitimate copies? I'm sure that the Fair Use doctrine (US Copyright Act, Section 107) would outlaw such a request.

At any rate, the US Constitution introduces Copyright `to promote the useful arts and sciences', while continental European Author's Right Law ("Droit d'Auteur") is more subjectively concerned with the reputation and, secondly, commercial position of the natural author who must be protected from pirating publishers or unethical co-authors trying to modify his/her work against his/her wishes.

This more subjective orientation, by the way, explains why the common "work for hire" rule under Anglo-American Copyright does not apply in many European jurisdictions: while an employer will usually be able to claim exploitation

rights (under Labour Law if not under Copyright Law), he will have a hard time in claiming moral rights such as the right to determine whether and when to publish, and the right to modify a work, especially if the work made under employment has the author's personal character. For `objective works' (computer programs?), moral rights are less problematic.

Herman J. Woltring, Eindhoven, The Netherlands (Studycommittees on s/w & chips protection / Computer crime, Netherlands Society for Computers and Law)
Brussellaan 29, NL-5628 TB EINDHOVEN, The Netherlands Tel. +31.40.480869

Search RISKS using swish-e

THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

ACM Committee on Computers and Public Policy, Peter G. Neumann, moderator

Volume 11: Issue 35

Friday 29 March 1991

Contents

Soviet Space Station [PGN Excerpting Service]

"James H. Paul" <0002296540@mcimail.com>
Fri, 29 Mar 91 21:11 GMT

REUTERS 03-28-91 05:40 PET
SOVIET SPACE STATION AVOIDS DOCKING DISASTER BY 40 FEET

MOSCOW, Reuters - The Soviet space station Mir came within 40 feet of a collision with a cargo module which would almost certainly have killed the two cosmonauts on board, Soviet television reported Thursday. Ground control staff noticed only seconds before impact that computers which should have been

docking an unmanned Progress-7 cargo module onto Mir were in fact steering it on a collision course. [...]

The cargo module was only 65 feet from impact when an alert ground controller watching television pictures of the docking had to make a snap decision to override the computers and change Progress-7's course. Rockets deflected the module, which had already failed to dock once last week, so that it passed within 40 feet of the space station and narrowly missed protruding antennae and solar panels. [...]

The space station's next crew will have to make more extensive repairs to a faulty antenna which was found to be the cause of the near miss. [...]

Tribe proposes computer freedom/privacy amendment to US Constitution

Paul Eggert <eggert@twinsun.com>
Wed, 27 Mar 91 09:26:05 PST

Here are excerpts from the Los Angeles Times, 1991/03/27, pages A3 and A12. The issues are familiar to Risks readers, but awareness has spread to the non-computer legal community, and it's worth noting how their reactions are reported in the mainstream press. On page A12 the article runs in parallel with the continuation of the day's biggest story, whose page one headline reads ``High Court Allows Forced Confessions in Criminal Trials ... A key pillar of constitutional law is upset.''

-- Paul Eggert

Computer Privacy Amendment Urged

Rodney Hoffman <Hoffman.El_Segundo@Xerox.com>
Wed, 27 Mar 1991 19:44:07 PST

Writing in today's 'Los Angeles Times' (p. A3), Henry Weinstein reports on one of the keynote addresses from this week's Conference on Computers, Freedom, and Privacy, sponsored by Computer Professionals for Social Responsibility.

According to the article, renowned constitutional scholar Laurence Tribe called for a 27th Amendment to the US Constitution "in order to preserve privacy and other individual rights threatened by the spread of computer technology.... to cope with the many questions raised by the advent of 'cyberspace,' a place without physical walls, or even physical dimensions, where an increasing amount of the world's communication and business -- ranging from ordinary letters to huge global transfers of money -- is taking place, via computer and telephone lines."

Further quotes from the article:

"The existence of such a place creates all sorts of potential problems, Tribe noted, because the nation's constitutional order historically has carved up the social, legal and political universe along the lines of 'physical places' which, in many situations, no longer exist. There is a 'clear and present danger' that the Constitution's core values of freedom, equality and privacy will be 'metamorphosed into oblivion' unless policy-makers come to grips with

the ramifications of technological change, Tribe said...."

"The proposed new amendment would provide that the Constitution's protections for free speech and against unreasonable searches shall be fully applicable, regardless of the technological method or medium used to transmit, store, alter or control information. The point, he said, would be to make it clear that the Constitution, as a whole, 'protects people, not places.'... [N]ormally wary of Constitutional amendments, ... he said the computer revolution has created 'substantial gray areas' that need to be addressed."

"Lance Hoffman, a George Washington University professor of computer science [And occasional RISKS contributor. And no relation to me! -- RH] said, ... 'We're casting about, because we're in a new age in our technological development, an age where a person can spend $1,000 and buy the computer equivalent of a Saturday Night Special and take down a large computer system.'"

More on Computers, Freedom, and Privacy

Peter G. Neumann <neumann@csl.sri.com>
Fri, 29 Mar 91 14:47:47 PST

The Conference on Computers, Freedom, and Privacy (Tuesday through Thursday of this week, sponsored by CPSR and cosponsored by and in-cooperation with numerous other organizations including ACM groups and committees) at which Professor Lawrence Tribe spoke (see previous messages) had a broadly based interdisciplinary audience, including law enforcers, lawyers, developers, vendors, marketers, computer scientists, (nonpejorative-sense) hackers, as well as crackers, whackers, and snackers (pejorative-sense hackers), trackers, backers, flackers (journalists), claquers, EFF-ers Kapor and Barlow, and a video crew one of whom was fresh from the Academy Awards Monday evening. Very few quackers (who duck the hard issues) or slackers. It was one of the most enjoyable meetings I have ever attended. All of my notes on the first two days seem to have been lost somewhere in the hotel (I was keeping my comments on the back of a bunch of laser printout pages that I happened to have with me), so my plans to write a detailed summary for RISKS have been scratched unless someone found the pages and saved them. I hope that some other RISKS reader will do so. There were a lot of RISKSers there, and a lot of valuable discussion, including various people arguing -- for DIFFERENT REASONS -- why they did or did not think the proposed amendment was a good idea. Also, a formation meeting was held for a U.S. Privacy Council, hoping to help privacy and privacy legislation in the U.S. catch up with various other countries. I hope that the organizers of that Council will provide details in RISKS.

[Peter Marshall: Re: Privacy Updates]

Brinton Cooper <abc@BRL.MIL>
Mon, 25 Mar 91 22:19:27 EST

Perhaps someone is listening after all! Brint

----- Forwarded message # 1:

Subject: Re: Privacy Updates
Keywords: CallerID/Privacy/Legislation
From: Peter Marshall <halcyon!peterm@sumax.seattleu.edu>
Date: Thu, 21 Mar 91 11:52:24 PST
Organization: The 23:00 News and Mail Service

In Washington, HB1774, setting up a joint committee on privacy and information technology, passed the House Tuesday on a 98-0 vote and is now in the Senate Law & Justice Committee, which has not yet set a hearing date on the bill. Also in Washington, HB1489, on Caller ID, which had previously passed the House, will have hearings in the Senate Energy & Utilities Committee at 10 a.m. next Tuesday and Thursday. In that other Washington, Sen. Leahy has set up a task force on CallerID; the Kohl "blocking bill" has been re-introduced, and Rep. Markey has introduced HR1305, which although it merely requires per-call blocking of CallerID, also restricts re-use and disclosure of ANI-delivered information without informed consent.

Peter Marshall
halcyon!peterm@seattleu.edu
The 23:00 News and Mail Service - +1 206 292 9048 - Seattle, WA USA

Legion of Doom's "Terminus" sentenced

Rodney Hoffman <Hoffman.El_Segundo@Xerox.com>
Wed, 27 Mar 1991 10:40:59 PST

According to a story by Henry Weinstein in the 23 March 'Los Angeles Times', computer consultant Leonard Rose pleaded guilty to federal felony wire fraud charges for stealing UNIX source code and distributing Trojan horse programs designed to gain unauthorized access to computer systems. He will serve a year in prison.

Rose, known as "Terminus", was alledgedly associated with the Legion of Doom "hacker group". In 1990, the Secret Service seized much of his computer equipment.

Court allows appeal over computer error

Martyn Thomas <mct@praxis.co.uk>
Thu, 28 Mar 91 18:01:35 GMT

A UK computer company was fined #21,000 for misdeclaring #71,000 of VAT (turnover tax). The misdeclaration occurred because software errors in an accounts package led to May invoices being included in a tax return which should have only included invoices up to April.

An appeal tribunal allowed the appeal against the fine, on the basis that the company had shown reasonable care in preparing the return, and was not aware of the bugs.

Martyn Thomas, Praxis plc, 20 Manvers Street, Bath BA1 1PX UK.
Tel: +44-225-444700. Email: mct@praxis.co.uk

RISK of being honest ["surplus" FBI data]

Peter Kendell <pete@tcom.stc.co.uk>
Tue, 26 Mar 91 08:46:01 GMT

>From the Guardian newspaper, London, 26 March 1991

Secret FBI files sold off inside $45 surplus computers

FBI informants given secret identities after testifying against the Mafia and other criminals may be at risk after the US Justice Department sold its computers without clearing the data banks.

Last summer, Charles Hayes, of Lexington, Kentucky, paid $45 (about 25 pounds) for a surplus computer from the local Justice Department office. When he plugged it in, he found himself reading sealed grand jury indictments and the confidential report of an FBI investigation into organised crime. The computer contained information on FBI informants and witnesses who had been given new identities.

When Mr Hayes informed the Justice Department, it sued him for return of the equipment, which came from the US Attorney's office.

The federal government's watchdog office said it knew of many similar cases and urged the department to recover the rest.

Agent Cooper, your secret is out! Seriously, though, what kind of incentive for honesty is it when someone points out to a goverment agency that they have made a serious security breach and they respond by suing him?

It would have been nice if the article had told us whether action had been taken within the Justice Department to prevent future cock-ups.

Peter

[It struck me that I'd missed the greatest RISK in the story about the surplus computers holding highly confidential information.

That is, that the Lexington Justice Department thought that, by recovering the computers with the sensitive data stored in them, they could also recover the data. I suppose the computers had removable media? PK]

USSR BBSList

"Selden E. Ball, Jr." <seb@lns61.tn.cornell.edu>

23 Mar 91 09:05:00 EST

Gentle folk,

Many people are doubtless already aware of this, but it came as a bit of a surprise to me.

It is now possible to direct-dial computer bulletin boards in the USSR and eastern European countries. Many of them are already on FidoNet. The following list of BBSs was recently posted to a widely read news group.

The potential transmission speed for computer viruses is increasing faster than your favorite comparison. sigh.

Selden Ball
seb@lns61.tn.cornell.edu

From: LNS61::WINS%"<KIDSNET@vms.cis.pitt.edu>" 22-MAR-1991 18:56:05.24
To: SEB
Subj: USSR BBSList

Return-Path: <KIDSNET@vms.cis.pitt.edu>
Received: from vms.cis.pitt.edu by lns61.tn.cornell.edu with SMTP ;
Fri, 22 Mar 91 18:55:52 EST
Date: Fri, 22 Mar 91 17:07 EDT
From: KIDSNET MAILING LIST <KIDSNET@vms.cis.pitt.edu>
Subject: USSR BBSList
To: kids-l@vms.cis.pitt.edu
Message-id: <A00DB88427FF407349@vms.cis.pitt.edu>
X-Envelope-to: seb@lns61.tn.cornell.EDU
X-VMS-To: IN%"kids-l"

Date: 15 Mar 91 23:01:15 EST
From: Frank Topping <76537.1713@CompuServe.COM>
Subject: USSR BBSList

I thought some teachers might be interested in this - they're growing like wildfire & connectivity opportunities abound!

-frank

.....
|Area : K12Net Sysops
|From : Serge Terekhov 15-Mar-91 00:05:00
|To : All 15-Mar-91 17:28:42
|Subj.: Full list of USSR BBSes!

Known USSR Bulletin Board Systems
Version 10c of 3/13/91
Compilation (C) 1991 Serge Terekhov

BBS name	Data phone	Modem	FIDO addr

```
PsychodeliQ Hacker Club BBS    +7-351-237-3700  2400      2:5010/2
Kaunas #7 BBS                  +7-012-720-0274  ?         -
Villa Metamorph BBS            +7-012-720-0228  ?         -
WolfBox                        +7-012-773-0134  1200      2:49/10
Spark System Designs           +7-057-233-9344  1200      2:489/1
Post Square BBS                +7-044-417-5700  2400      -
Ozz Land                       +7-017-277-8327  2400      -
Alan BBS                       +7-095-532-2943  2400/MNP  2:5020/11
Angel Station BBS              +7-095-939-5977  2400      2:5020/10
Bargain                        +7-095-383-9171  2400      2:5020/7
Bowhill                        +7-095-939-0274  2400/MNP  2:5020/9
JV Dialogue 1st                +7-095-329-2192  2400/MNP  2:5020/6
Kremlin                        +7-095-205-3554  2400      2:480/100
Moscow Fair                    +7-095-366-5209  9600/MNP  2:5020/0
Nightmare                      +7-095-128-4661  2400/MNP  2:5020/1
MoSTNet 2nd                    +7-095-193-4761  2400/MNP  2:5020/4
Wild Moon                      +7-095-366-5175  9600/MNP  2:5020/2
Hall of Guild                  +7-383-235-4457  2400/MNP  2:5000/0
The Court of Crimson King      +7-383-235-6722  2400/MNP  2:50/0
Sine Lex BBS                   +7-383-235-4811  19200/PEP 2:5000/30
The Communication Tube         +7-812-315-1158  2400/MNP  2:50/200
KREIT BBS                      +7-812-164-5396  2400      2:50/201
Petersburg's Future            +7-812-310-4864  2400      -
Eesti #1                       +7-014-242-2583  9600/MNP  -
Flying Disks BBS               +7-014-268-4911  2400/MNP  2:490/40.401
Goodwin BBS                    +7-014-269-1872  2400/MNP  2:490/20
Great White of Kopli           +7-014-247-3943  2400      2:490/90
Hacker's Night System #1       +7-014-244-2143  9600/HST  2:490/1
Lion's Cave                    +7-014-253-6246  9600/HST  2:490/70
Mailbox for citizens of galaxy +7-014-253-2350  1200      2:490/30
MamBox                         +7-014-244-3360  19200/PEP 2:490/40
New Age System                 +7-014-260-6319  2400      2:490/12
Space Island                   +7-014-245-1611  2400      -
XBase System                   +7-014-249-3091  2400/MNP  2:490/40.403
LUCIFER                        +7-014-347-7218  2400      2:490/11
MESO                           +7-014-343-3434  2400/MNP  2:490/60
PaPer                          +7-014-343-3351  1200      2:490/70
-----------------------------!----------------!----------!------------


|--- Maximus-CBCS v1.02
| * Origin: The Court of the Crimson King (2:50/0)

.....

Frank Topping, sysop
Sacramento Peace Child - NorCal K-12Net Feed (916)451-0225 (1:203/454)

conference moderator:
"The Educational Exchange Conference" - "OERI" BBS  (800)222-4922

operated by: Office of Educational Research and Improvement - (OERI)
U.S. Dept. of Education, Washington, D.C.
```

A Consciously Chosen Risk

<[anonymous]>
Sat, 23 Mar 91 12:40 xxT

Even in time of personal loss there are lessons learned that might be helpful to others. In this case I'm not exactly sure what the lesson is, but the RISK is readily apparent. My mother-in-law died recently and my wife and I have the burden of handling all the financial and legal details. Among those were notifying Social Security, two state-run pensions, and two insurance carriers (Blue Cross and the Medicare carrier.) All of the details were handled over the phone -- we did not have to send in any proof of death or even just a letter. (It happens that one of the state pensions has someone who reads the obituary column and had already started the necessary action for that account, but presumably they don't read every small town newspaper.) In all cases all we had to give was her name and social security number.

The RISK is obvious: if one wanted to harass someone who was dependent on social security and pensions all one would need do is phone in and pose as some relative and announce their death. (getting the SSN shouldn't be hard.)

When I realized during my first call (to Social Security) what the situation was I asked the person I was talking to about it. He replied that they had quite consciously decided to place as little extra burden as possible on what are usually still grieving relatives, even though they knew the risk involved. He pointed out that had there been survivors' benefits involved (which there weren't), proof would have had to be supplied. It should also be noted that in each case a letter will be sent to the address of record, so if there were a harassment it would presumably be discovered quickly. I'm not too sure however that the way that is handled is not without its flaws: one of the places we called asked if they had the right address; since in all cases the address had already been changed to ours I don't know if the others would have asked or given us an opportunity to change it to prevent the letter from going to the last known address. (We also stopped the telephone service the same way, supplying only the phone number and confirming the name and address.)

Compass 1991 Program [EXCERPT. EMail to jchernia for details.]

<jchernia@NSF.GOV>
Mon, 25 Mar 91 12:38:00 EST

COMPASS '91
6th Annual Conference on Computer Assurance
National Institute of Standards and Technology, Gaithersburg, MD
June 24-28, 1991

Sponsored by IEEE National Capital Area Council &
IEEE Aerospace and Electronic Systems Society

COMPASS '91 PRE-CONFERENCE TUTORIALS, Monday, June 24th

0900 Registration for Tutorial 1
1000 Tutorial 1: Safe Systems--A Disciplined Approach
John McDermid, University of York
John Cullyer, University of Warwick
1200 Lunch; Registration for Tutorial 2
1300 Tutorial 1: Safe Systems--A Disciplined Approach (continued)
Tutorial 2: Software Safety Analysis--Linking Fault Trees and Petri Nets
Janet Gill, Patuxent River Naval Air Test Center
1700 Close of tutorials

Safe Systems--A Disciplined Approach

Professor John McDermid, University of York, and Professor John Cullyer, University of Warwick, will discuss the integration of formal methods into the life cycle development of safety-critical software. Professor McDermid will discuss the safety life cycle and the safety analysis of software. Professor Cullyer will discuss the integration of formal methods during the requirements and specification phases, design phases (including hardware), and the verification and validation phase. Finally, Professor McDermid will discuss the skills, education and training required to apply formal methods to safety-critical software.

Software Safety Analysis--Linking Fault Trees and Petri Nets

Independently, fault trees and Petri nets serve limited evaluation purposes in safety-critical systems. This tutorial presents a technique for converting and linking fault tree analysis (FTA) with Petri net modeling and vice versa. This technique permits the analyst to determine if a software fault can be reached be analyzing the software in detail with FTA.

COMPASS '91 PROGRAM, Tuesday, June 25th

0800 Registration
0900 Opening Remarks, General Chair, Lt. Col. Anthony Shumskas,
Office of the Secretary of Defense, Department of Defense
0915 Honorary Chair Address
0930 Keynote Address, David L. Parnas, Queens University
1030 Break
1100 Conference Topic Panel: Educating Computer Scientists for the Year 2000
Chair, John Cherniavsky, National Science Foundation
David L. Parnas, Queens University
Peter J. Denning, NASA Ames Research Center
William L. Sherlis, DARPA
John A. McDermid, University of York/British Computer Society
Bruce Barnes, National Science Foundation
Raymond Miller, University of Maryland
1245 Lunch
1345 Panel (continued)
1515 Break
1545 Questions from the audience to panel members

1830 Cocktail Reception/Banquet (Holiday Inn)
The Accidents of Life--From Conception to Our Last Moments
John Cullyer, University of Warwick

COMPASS '91 PROGRAM, Wednesday, June 26th

0800 Registration
0830 Computer Related Risk of the Year: Weak Links and Correlated Events
Peter G. Neumann, SRI International
0915 SESSION 1: EUROPEAN ECONOMIC COMMUNITY '92 PERSPECTIVES
Chair, John Cullyer, University of Warwick

Computer Software and Aircraft
J. Peter Potocki de Montalk, Airbus Industrie

Some Results From DRIVE
Thomas Buckley, University of Leeds

1015 Break
1045 SESSION 2: HOW INDUSTRY TRAINING IN COMPUTER ASSURANCE CAN BE IMPROVED THROUGH EDUCATION
Chair, Diane Jachinowski, Nellcor
Peter G. Neumann, SRI International
J. Alan Taylor, British Computer Society
Claire Lohr, Lohr Systems
William Junk, University of Idaho
1245 Lunch
1345 SESSION 3A: CERTIFICATION AND SAFETY OF CRITICAL SYSTEMS
Chair, Michael Brown, Naval Surface Warfare Center

Certification of Production Representative/Production Software Intensive Systems for Dedicated Test and Evaluation
Lt. Col. Anthony F. Shumskas, Office of the Secretary of Defense

Interrelationships of Problematic Components of Safety-Related Automated Information Systems
Morey J. Chick, General Accounting Office

A Case-Study of Security Policy for Manual and Automated Systems
Edgar H. Sibley, James B. Michael, and Ravi Sandhu
George Mason University

1515 Break
1545 SESSION 3B: CERTIFICATION AND SAFETY OF CRITICAL SYSTEMS (CONTINUED)

Safety Criteria and Model for Mission-Critical Embedded Software Systems
R. A. Gove and Janene Heinzman, Booz Allen, and Hamilton

A Case-Study on Isolation of Safety-Critical Software
Edward A. Addy, Logicon, Incorporated

1830 Birds of a Feather Meeting (Holiday Inn)
Presentation: Software Development Methods in Practice

J. V. Hill, Rolls-Royce and Associates Limited

COMPASS '91 PROGRAM, Wednesday, June 26th

0800 Registration
0830 Day's Keynote: High Assurance Computing
H. O. Lubbes, Naval Research Laboratory
0900 SESSION 4A: FORMAL METHODS
Chair, Andrew Moore, Naval Research Laboratory

Report on the Formal Specification and Partial Verification of the VIPER Microprocessor
Bishop Brock and Warren A. Hunt, Computational Logic, Incorporated

Using Correctness Results to Verify Behavioral Properties of Microprocessors
Phillip J. Windley, University of Idaho

Estella: A Facility for Specifying Behavorial Constraint Assertions in Real-Time Rule-Based Systems
Albert Mo Kim Cheng, University of Houston; and
James C. Browne, Aloysius K. Mok, and Rwo-Hsi Wang,
University of Texas at Austin

1000 Break
1030 SESSION 4B: FORMAL METHODS (CONTINUED)

Design Strategy for a Formally Verified Reliable Computing Platform
Ricky Butler and James L. Caldwell, NASA Langley Research Center;
and Ben L. De Vito, Vigyan, Inc.

Specifying and Verifying Real-Time Systems Using Time Petri Nets and Real-Time Temporal Logic
Xudong He, North Dakota State University

Developing Implementations of Estelle Specifications Using the PEDS Toolkit
William Majurski, NIST

1245 Lunch
1345 SESSION 5: US AND INTERNATIONAL SPONSORED INITIATIVES
Chair, H. O. Lubbes, Naval Research Laboratory

NIST: Workshop on Assurance of High Integrity Software
Dolores R. Wallace, D. Richard Kuhn, NIST, and
John Cherniavsky, National Science Foundation

NASA Langley: Research Program in Formal Methods
Ricky Butler, NASA Langley Research Center

1445 Break
1515 SESSION 6: RISK CONTAINMENT PLANNING AND QUALITY MEASUREMENTS

Chair, Michael Brown, Naval Surface Warfare Center

Planning and Implementing and IV&V Program in a Large Scale DoD Software Development Program
Florence Sippel and Kevin Mello, Naval Underwater Systems Center

Quality and Security, They Work Together
Richard Carr, Marie Tynan, NASA Headquarters; and
Russell Davis, PRC, Inc.

Data Collection and Descriptive Analysis: A First Step for Developing Quality Software
Anita Shagnea, Kelly Hayhurst, and B. Edward Withers,
Research Triangle Park

Fault Locator and Weighting System
Jeffrey Bulow, General Electric, Syracuse

1715 Closing Remarks

Friday, June 28th

0830 - 1400 Forum: US and International Standards for High Integrity Systems (DoD, Government, and Industry)
Chair, Dolores Wallace, National Institute of Standards and Technology

[The packet was very long, including registration and hotel information. You may get the complete version from John, or even from me. PGN]

Search RISKS using swish-e

THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

ACM Committee on Computers and Public Policy, Peter G. Neumann, moderator

Volume 11: Issue 36

Monday 1 April 1991

Contents

Another type of password attack

Gene Spafford <spaf@cs.purdue.edu>
Mon, 01 Apr 91 17:20:00 EST

[Forwarded with permission of andie@umd.edu, this represents one of the most amusing attempts at a breakin in recent memory. This reminds me of the confidence scam where people call elderly marks and ask them to cooperate in a bank investigation by withdrawing a large sum of money. Spaf]

- ------- Forwarded Message

Date: Mon, 01 Apr 91 17:05:55 -0500
From: ssw (Samuel S Wagstaff)
To: spaf
Subject: scam [ssw (Samuel S Wagstaff): scam]

>From andie@ada.umd.edu Mon Apr 1 15:22:14 1991
Date: Mon, 1 Apr 91 15:20:25 EST
From: "Diane J. Donaldson" <andie@ada.umd.edu>
Subject: PLEASE READ THIS NOW

There has been a recent attempt to break in to our system.
Sudip Bose received the following letter:

- ---

>From root@hilda.umd.edu Mon Mar 25 19:13:34 1991
Date: Mon, 25 Mar 91 19:12:58 EST
From: "Operator" <root@hilda.umd.edu>

This is the system administration:

Because of security faults, we request that you change your password to "systest001". This change is MANDATORY and should be done IMMEDIATLY. You can make this change by typing "passwd" at the shell prompt. Then, follow the directions from there on.

Again, this change should be done IMMEDIATLY. We will inform you when to change your password back to normal, which should not be longer than ten minutes.

Thank you for your cooperation,

The system administration (root)

- --

Fortunately, he realized it was a fake and told me about it. If anyone else received one of these messages, PLEASE LET ME KNOW IMMEDIATELY!!!! In case you don't know already, I NEVER need to have anyone change their password so that I can fix "security faults". I can change your password myself if I have to. Again, if you have ever received or ever do receive a message of this sort, let me know so I can try to track down the person doing this. Thanks!

djd

- -- End of Forwarded Message

Re: Another type of password attack

Peter G. Neumann <neumann@csl.sri.com>
Mon, 01 Apr 91, 15:15:15 PST

I first saw this message on 25 Mar 91, but did not get around to running it in RISKS. (I am still backlogged.) In light of the date today, I include it now. However, it could have been a real hoax, not a prank, and I imagine there were people who were taken in. I heard of several reports of original appearances, spoofed out of different root addresses. So, what will the day bring us this year?

For those of you who have been requesting information on back pranks, see my Inside Risks column in the April CACM, which should be out forthwith. (Fourthmonth.) I honor the best spoofs of the past, particularly Piet Beertema's 1984 NOT-BY-Chernenko Spoof (ACM SIGSOFT SEN July 1984) and Chuq von Rospach's 1988 NOT-BY-Spafford Spoof (SEN July 1988 and RISKS-6.52, 1 Apr 88). Apparently the NOT-BY-Spafford Spoof is making an annual reappearance again today. PGN

[By the way, as of a few hours ago, I am now running on a SPARCstation. There are a few differences, so I won't be surprised if this RISKS mailing exhibits some of them...]

PBS presents 3 hours of RISKS

<oberman@ptavv.llnl.gov>
31 Mar 91 17:38:45 GMT

This week PBS is running a 3 hour program on the subject of risks. It's title is: "Living Against the Odds" and is hosted by Richard Lewis. My TV suplement gives the following blurb:

"Specialists seek a perspective on life's many risks, from voluntary dangers like gambling and rock-scaling to natural disasters, accidents and hazardous environments."

It is on Wednesday, April 3 in San Francisco, but, being PBS, the date may differ in other areas.

R. Kevin Oberman Lawrence Livermore National Lab. [or oberman@icdc.llnl.gov]

[I hope PBS uses some of the stuff they got from The Risks Forum, but I think the slant of the program is rather different. PGN]

PBS special: Living with Risks

William Ricker <wdr@wang.com>
Mon, 1 Apr 91 17:39:59 EST

[...] It won't dwell specifically on automated or even technologic risk, but on risk acceptance and the risks of everyday life.

It *might* increase public understanding of risk assessment and risk acceptance.

Bill Ricker wdr@wang.com

NOVA (TV) broadcast: "We know where you live" Tues @ 8 KCET

"David A. Honig" <honig@ICS.UCI.EDU>

Fri, 29 Mar 91 17:51:07 -0800

on tech & privacy

Correction Re: Terminus

Rodney Hoffman <Hoffman.El_Segundo@Xerox.com>
Sun, 31 Mar 1991 14:49:11 PST

In RISKS 11.35, I summarized a short article from the 23 March 'Los Angeles Times' about Leonard Rose's guilty plea. Two corrections:

1. The article said, "The Baltimore indictment asserted that he was associated with a group of computer hackers known as the 'Legion of Doom.'" I used that as part of my "Subject:" line for the RISKS posting.

I've now heard from several people that Leonard Rose was NOT a member of the Legion of Doom, and never claimed to be. (It may still be true that the indictment says he is.) The 'Washington Post' also ran the story of Rose's sentencing on 23 March, but published a correction on 26 March saying he was not a member of the Legion of Doom. I have not spotted any correction published in the 'Los Angeles Times.'

2. The LATimes article said, "Under the plea agreements, ... Rose ... will serve a year in prison." My RISKS posting omitted the reference to the plea agreements. The one-year sentence (actually, two concurrent one-year terms) is apparently the prosecutors' recommendation. Rose's formal sentencing is scheduled for May.

[Corrections via Craig Neidorf, and, indirectly, Brendan Kehoe and Bob Izenberg. Anyone interested in more details may write me. -- RH]

[See also two other items, noted for completeness to ensure that the message gets through... PGN]

Re: Len Rose (Hoffman, RISKS-11.35)

Mike Godwin <mnemonic@eff.org>
Sun, 31 Mar 91 16:03:20 EST

[...] This is actually incorrect. Rose pled guilty to two counts of unauthorized possession of UNIX source code. Rose did not plead guilty to "distributing Trojan horse programs designed to gain unauthorized access to computer systems."

"Rose, known as "Terminus", was alledgedly associated with the Legion of Doom "hacker group"."

Federal prosecutors are unwilling to abandon the allegation that Rose was a member of the Legion of Doom. He was not, however, and the counts to which he pled guilty have nothing to do with any known Legion of Doom activities, real

or alleged.

--Mike

Mike Godwin, (617) 864-0665 Electronic Frontier Foundation mnemonic@eff.org

---

Re: Len Rose (RISKS-11.35)

<TK0JUT1@MVS.CSO.NIU.EDU [still trying to be anonymous!]>
Fri, 29 Mar 91 23:33 CST

In RISKS DIGEST 11.35, Rodney Hoffman <Hoffman.El_Segundo@Xerox.com> writes:

Why, oh why, does this trash persist? Despite media distortion, prosecutorial hyperbole, and inane headers such as Hoffman's ("LoD's Terminus"??--c'mon!!), the following are demonstrable facts:

1) Len Rose was never associated with Legion of Doom, period. The Washington Post's story of March 23, which was based on an alleged link between Len and the LoD, contained numerous blatantly false statements, and the Post retracted the LoD connection. The retraction destroyed the basis of the Post's story, but the damage was done. Rose became involved in Secret Service investigations because of the infamous E911 files published in Phrack. Rose was raided, and although he was not associated with the E911 files, the SS agents found him in possesion of unlicensed copies of of AT&T's Unix source code and login.c

2) The continued attempt to link Len to LoD, despite overwhelming evidence that there was no link, frames this case as one of computer security. Face it! The government (Messrs Cook, Foley, Willcox, et. al.) wanted this case to be about something it wasn't. This case was about unlicensed software, *not* about computer security. Possession of AT&T source code, in this context, simply meant that Len had a copy of Unix that he was not licensed to have and that he allegedly received it from and shared it with others who allegedly were not authorized to have it. Len pleaded guilty to two federal counts (one from Maryland, one from Illinois) under Title 18 s. 1343:

> Sec. 1343. Fraud by wire, radio, or television
>
> Whoever, having devised or intending to devise any scheme or artifice to defraud, or for obtaining money or property by means of false or fraudulent pretenses, representations, or promises, transmits or causes to be transmitted by means of wire, radio, or television communication in interstate or foreign commerce, any writings, signs, signals, pictures, or sounds for the purpose of executing such scheme or artifice, shall be fined not more than $1000 or imprisoned not more than five years, or both.

3) A not-so-trivial point: login.c required root access. If one had root access, there was no need to hack into a system because one was already there. Yet, despite the nature of the plea, the allegations of the indictment, and the facts of the case, some irresponsible prosecutors and media types (not to mention hysterical headers such as Hoffman's) insist on sending the message

that Len was a "hacker" who posed a potential threat to the nation's computer security. At least one computer security consultant indicated that he used login.c to log passwords as a way of protecting security, not subverting it. I have yet to hear even a marginally literate Unix type claim that, despite prosecutors' claims in press releases (where they try to create meanings and images that they couldn't do at court), login.c is a realistic "hacking device." But, this is moot, because--I'll put it in caps--THE CASE WAS ABOUT SOFTWARE, NOT ABOUT SYSTEM SECURITY.

Len Rose accepted a guilty plea in an attempt to make the best of a situation in which there could be no winners on either side. He was under pressure to fight the case from those who had access to all the evidence and felt he could "win," and to accept a plea from those who felt he had committed a transgression and should be punished. Len's wife and two small children were in the middle. He made the decision that he felt would balance the needs of justice with those of his family and help him move on to a future in which he could rebuild his life. Let's not, despite all evidence to the contrary, continue this "hacker image" that was not at issue in Len's plea nor in the spirit or letter of the statutes defining his transgressions.

More "Sun Devil" indictments

Rodney Hoffman <Hoffman.El_Segundo@Xerox.com>
Sun, 31 Mar 1991 18:21:00 PST

According to a story by Henry Weinstein in the 30-Mar-91 'Los Angeles Times,' Arizona authorities have arrested Baron Monroe Majette, 19, also known as "Doc Savage," and charged him with three counts of fraudulent schemes and three counts of conspiracy.

The charges outlined in the article are (a) falsely posing as an employee of Toys R Us to illegally gain access to a telephone conference call line for calls worth $8,100, and (b) using a computer to illegally gain access to TRW Credit's database and extracting names, addresses, SSNs, credit histories, and other data, then using the information to create false billing addresses, obtain credit cards, and make purchases exceeding $60,000.

This arrest is a result of the federal - state Operation Sun Devil raids in May, 1990. From the end of the newspaper article: "Dale Boll, deputy director of the Secret Service's fraud division, defended the operation but said the agency would have done some things differently. He added that several new cases will be filed in coming months."

TRW report shows who else is interested

"David A. Honig" <honig@ICS.UCI.EDU>
Fri, 29 Mar 91 17:54:44 -0800

A friend of mine just bought a car. As he was talking to the person reviewing his finances, that person mentioned that Arrowhead (the bottled water supplier) was doing a check on my friend. (He was starting up bottled water delivery

service (and they ran a credit check!!))

It surprised both him and I that the names of recently-interested report-receivers would be printed with your credit report. This seems like an invasion of privacy. Does anyone know more?

Search RISKS using swish-e

THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

ACM Committee on Computers and Public Policy, Peter G. Neumann, moderator

Volume 11: Issue 37

Wednesday 2 April 1991

Contents

An ancient method for assuring software quality

Martin Minow 01-Apr-1991 0000 <minow@ranger.enet.dec.com>
Sun, 31 Mar 91 21:03:08 PST

Is it possible that the solution to the software quality crisis was discovered in Korea in the 15th century? The following is from Daniel J. Boorstin, "The Discoverers" quoting, apparently, Kim Won-Yong, "Early Movable Type in Korea" (1954):

> "The supervisor and compositor shall be flogged thirty times for an error per chapter; the printer shall be flogged thirty times for bad impression, either too dark or too light, of one character per chapter."

Boorstin continues, "This helps explain both the reputation for accuracy earned by the earliest Korean imprints and the difficulty that Koreans found in recruiting printers."

Martin Minow minow@ranger.enet.dec.com
[The date of submission of this is a coincidence, of course.]

> [This gives a new meaning to the concept of making a good impression.
> Both the Imprints of Darkness and Imprints of Lightness are evil!
> Kiss either one and he (distractedly) turns into a Flog.
> But if they succeed, they can have a moveable type feast.
> Strongly typed, at that. PGN]

Risks of using your telephone Calling Card in a COCOT

John R. Covert <covert@covert.enet.dec.com>
2 Apr 91 16:21:37 GMT

I cannot vouch for the accuracy of the following story, which I heard yesterday. There does seem to be substantial risk here:

According to the story, a company which leased COCOTs (Customer Owned Coin Operated Telephones) to businesses in New York, Chicago, and Los Angeles was discovered to have turned all 1000 of their phones into Calling Card thieves.

The scheme was simple: The phones, like most COCOTs, are located inside or outside small businesses. The business contracts with the leasing company for maintenance of the phones; as part of the contract the leasing company obtains a percentage of all money collected by the phone, paid by the small business out of the receipts in the coin box. In addition, the leasing company pays the business a percentage of the money collected by Alternate Operator Services (AOSs) for calls billed to Calling Cards.

The COCOTs include a modem used by the COCOT operator to call into the phone in order to set rate tables and to collect usage data for accounting purposes. This COCOT operator had modified the accounting program to collect and report the calling card numbers used by people placing calls from the phone. The calling card numbers (AT&T, Sprint, and MCI) were then sold to drug dealers and resulted in over ten million dollars in fraudulent calling before the pattern was discovered and the owners of the COCOT service company were arrested.

Police recommended using cash, not calling cards, from all telephones not bearing the identification of the local phone company.

/john

Computers and evidence

<smb@ulysses.att.com>
Mon, 01 Apr 91 22:15:07 EST

There's a fairly sensational murder trial going on now in New York that may be of interest to RISKS readers. Of course, I'm not referring to the more mundane attractions of the trial -- plenty of sex, a seedy private eye, and all manner of fascinating behavior -- but rather to some conflicting pieces of evidence

that the prosecution and defense have introduced.

The entire case is circumstantial, so every item counts. To demonstrate that the defendant called a particular gun store the day of the murder, the district attorney introduced a printout made from MCI's microfiche copies of phone bills. Sure enough, the call was listed. The defense countered with what it claimed was the original of the phone bill. That call wasn't shown, but a call to the defendant's mother was shown, at a time that would provide an alibi for the time of the killing.

The prosecution countered with a billing systems expert who claimed that MCI bills for the month in question should include a particular slogan; this one lacked it. Another MCI employee said that he had reviewed the original tapes in question, and the gunshop call was there, but not the alibi call. The defense attorney was astute enough to ask what proof there was that no one had tampered with the tape, and how good the access controls were on the tape library. The next go-round featured an FBI computer type who said that he, too, had reviewed the tapes, and found the prosecutor's call; however, he apparently couldn't explain why other calls shown on the microfiche were not on the tape. (I may have some details wrong; local media coverage has been less than stellar. One radio station has been doing things like calling defense questions ``desparation tactics''. And the New York Times referred to the tapes as the ``Volser tapes'', as if that were the name of the billing system. I suppose it might be, though given IBM's JCL nomenclature I find that notion a bit improbable...)

I won't even say that the jury is still out on this case, since it hasn't progressed that far yet. Stay tuned for the next episode of ``As the Disk Turns''....

--Steve Bellovin

E-mail role in LA cop probe

Sean Eric Fagan <seanf@sco.com>
Mon, 1 Apr 91 13:00:04 PST

Taken from the March 25 Computerworld

Electronic messages transmitted between computers assigned to three Los Angeles police officers suspected in the beating of a black motorist could be used as evidence to show "intent to harm," according to legal experts.
[...] [Dialogue ommitted]
Legal experts say they know of no previous case in which electronic messages have been used as evidence in a criminal case. Most agreed that such communications are likely to be treated as recorded voice transmissions.
[end excerpts]

Obvious RISKS spring to mind, such as: how secure is the identification (or, put another way, how easy is it to forge messages)? Giving electronic messages the same validity as recorded voice is a bad move, it seems to me.

Sean.

Re: E-mail role in LA cop probe

RISKS Forum <risks@csl.sri.com>
Tue, 2 Apr 91 9:13:40 PST

We have been around on this one numerous times before in RISKS. Even with elaborate techniques (e.g., multikey encryption facilities), essentially any message can be spoofed, tampered with, or destroyed altogether, given suitable system access. Therefore, essentially any evidence provided by a system COULD have been tampered with, even though it may be unlikely in a particular case.

Sierra Club and Electronic Voting

Ed Ravin <eravin@panix.UUCP>
Wed, 3 Apr 91 16:41:41 GMT

The Sierra Club, in their board elections, have sent paper ballots to all their members, who are asked to return the ballot with the appropriate votes checked in. There is no name or other identification on the ballot, except for a computer-printed number and the caption "This random number tells the computer that the voter is a member in good standing... It is not related to the membership number".

Annonymous verification of ballots? If their scheme is sound, then it shouldn't matter if the ballots are mailed in or keyed in over the phone or some other computer-assisted device. Does anyone out there know what system Sierra Club is using or is able to comment on simliar systems?

Ed Ravin, cmcl2!panix!eravin philabs!trintex!elr

Leonard Rose

<smb@ulysses.att.com>
Mon, 01 Apr 91 21:31:23 EST

> If one had root access, there was no need to hack into a system
> because one was already there.
> ... [text deleted and reordered]
> I have yet to hear even a marginally literate Unix type claim
> that login.c is a realistic "hacking device."

OK, I'll byte [sic]. I consider myself more than ``marginally literate'' on both subjects, UNIX and system security, and I'll make the blatant assertion that login.c is a very realistic ``hacking device''. Why? Because many people tend to use the same password on different machines. If I can get your password on some machine I've already penetrated, the odds are quite good that I can then log in to some other machine you use. And even if you follow proper practice, and don't reuse passwords in different security domains, the probability is near unity that someone on your machine isn't so careful.

Possession of a hacked login.c is the electronic equivalent of being caught with burglar's tools or a ``deadly weapon'' (which may be as innocuous in other contexts as a baseball bat). The prosecutor must demonstrate intent to misuse in such cases. If possesion of ``hacking tools'' were against the law (as far as I know, it's not, and given how loosely many such statutes are drawn, that's probably just as well), there would be a considerable burden of proof. Maybe such evidence could be produced in this case, maybe not. But it's far from unreasonable to claim that hacking is at issue.

> At least one computer security consultant indicated that he used login.c to log passwords as a way of protecting security, not subverting it.

Maybe so. In that case, the charge should be extreme negligence. I don't care what your motives are; no responsible system administrator should ever store cleartext user passwords online. If you really want to analyze them, do the analysis immediately, and dispose of the input text as soon as possible. A list of passwords, no matter how well protected, is an open invitation to trouble. The classic Morris-Thompson paper on password security gives several lovely examples of this.

--Steve Bellovin

Justice Department's One Big File

"Clifford Johnson" <GA.CJJ@Forsythe.Stanford.EDU>
Mon, 25 Mar 91 14:24:18 PST

The Privacy Act was supposed to prohibit file-matching across government databases. It contained a broad EXCEPTION to this rule, if matching was required in order for an agency to perform a special duty. This was supposed to permit only individual case exceptions, but it turned out to be such a big loophole that in no cases is matching prohibited, and automatic bulk file matching is now routine. What privacy advocates often fail to address in their conceptual attacks on matching is the simple fact that the critical government databases on people sit on the same mainframes, managed by people who report to the same person. Fighting file-matching is at best Quixotic -- because there's de facto One Big File. I.e.:

Harry H. Flickinger is Assistant attorney general for administration in the Justice Department. Under him are officers responsible for databases that support the FBI, the DEA, the INS, the Bureau of Prisons, civil/tax and other divisions. There is a new vacant post under him, for Deputy Assistant Attorney General, Information Resources Management. This single position is to be responsible for ALL the Justice Department's computational needs, as reported in Gov't Computer Week, March 18:

Q: What is your IRM philosophy?

Flickinger: [It's] unitary. Although it is diversified in what it does, the components tend to impact one another. Investigators go out and conduct investigations that lead to prosecution. We have lawyers that handle that. Prosecution may lead to incarceration. We have the Bureau of Prisons. This

attorney general and others have said we have to look at the department as a single entity -- to provide as much uniformity and standardization of support as we possibly cann... The theory is, we ought to have one system that lets virtually anybody in this department regardless of location talk to anybody else. We're trying to promote that uniformity right across all the administrative activities... We're going to have... theoretically one data center. WE THINK IT'S SMARTER TO PUT IT IN ONE LOCATION.

The article continues:

"The Justice Department's two data centers [each has 4 Amdahl 5870s, one has another 4 IBM 3090-400Es] ... keep humming about 99 percent of the time 'sometimes 100,' [!] according to Lee Brown... The 56 major customers include the Drug Enforcement Administration, Immigration and Naturalization Service, U.S. Marshals Service, Bureau of Prisons, and Interpol..."

Search RISKS using swish-e

Report problems with the web pages to the maintainer

Search RISKS using swish-e

THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

ACM Committee on Computers and Public Policy, Peter G. Neumann, moderator

Volume 11: Issue 38

Thursday 4 April 1991

Contents

Risks of "recycled" phone numbers

Barry Wright <ronin@ronin.sbi.com>
Thu, 4 Apr 91 13:04:02 EST

>From clari.nb.telecom:

> SAN LUIS OBISPO, CALIFORNIA, U.S.A., 1991 APR 3 (NB) --Ron Hopson got a call at work from his neighbor who informed him police broke down his front door, and were confiscating his computer equipment. The report, in the San Luis Obispo (SLO) Telegram-Tribune, quoted Hopson as saying, "They took my stuff, they rummaged through my house, and all the time I was trying to figure out what I did, what this was about. I didn't have any idea."

According to the Telegram-Tribune, Hopson and three others were accused by police of attempting to break into the bulletin board system (BBS) containing patient records of SLO dermatologists Longabaugh and Herton. District Attorney Stephen Brown told Newsbytes that even though the suspects (two of which are Cal Poly students) did not know each other, search warrants were issued after their phone numbers were traced by police as numbers attempting access to the dermatologists' system by modem "more than three times in a single day."

Brown told Newsbytes the police wouldn't have been as concerned if it had been the BBS of a non-medical related company, but faced with people trying to obtaining illegal narcotics by calling pharmacies with fraudulent information...

What the suspects had in common was the dermatologists' BBS phone number programmed into their telecommunications software as the Cygnus XI BBS. According to John Ewing, secretary of the SLO Personal Computer Users Group (SLO PC UG), the Cygnus XI BBS was a public BBS that operated in SLO, but the system operator (sysop) moved less than a year ago and discontinued the board. It appears the dermatologists inherited the number.

John Ewing, SLO PCUG editor, commented in the SLO PC UG ewsletter, "My personal opinion is that the phone number [for the Cygnus XI BBS] is still listed in personal dialing directories as Cygnus XI, and people are innocently calling to exchange information and download files. These so-called hackers know that the password they used worked in the past and attempt to connect several times. The password may even be recorded as a script file [an automatic log-on file]. If this is the case, my sympathies go out to those who have had their hardware and software confiscated."

Bob Ward, secretary of the SLO PC UG, told Newsbytes, "The number [for Cygnus XI] could have been passed around the world. And, as a new user, it would be easy to make three mistaken calls. The board has no opening screen, it just asks for a password. So, you call once with your password, once more trying the word NEW, and again to try GUEST."

Tricky application of Caller ID

Jeff Johnson <jjohnson@hpljaj.hpl.hp.com>
Fri, 29 Mar 91 13:15:54 PST

At the "Computers, Freedom, and Privacy" conference this week, one of the speakers, MIT sociologist Gary Marx, described an interesting use of Caller ID: A children's TV show host told kids to hold their phones up to the TV speaker. The TV station played touch tones to dial a certain number. Phone equipment at

the receiving end of all those calls used Caller ID and reverse-directories to create a data-base of people who watch the show, which were then used to send junk-mail to those households.

Does anyone have any documentation on this supposedly-true story?

Thanks, JJ

Land your MD-11 at 15000 feet?

Eric K. Olson <olson@endor.harvard.edu>
Thu, 4 Apr 91 02:28:11 EST

My favorite part of the PBS program "Living Against the Odds" occurs during the demonstration of the MD-11's computer's ability to correct for unsafe flying situations. I've tried to quote enough to be fair to the obviously capable testing crew. Note the single verbal suggestion made by the computer:

Narrator: Chief Test Pilot John Miller has to fight the computer as he tries to put his plane into a dangerous stall.

Pilot: When I roll out on this heading, I'll disconnect the throttles and try and make it fly an unsafe speed. You'll notice the throttles will re-engage, and then take [maintain?] me at a safe speed. I'll do it right now. OK? You Ready? I'm disconnecting the throttles, and I'm reducing the speed. And the speed is going down, and the throttles are going forward on their own now. Because they say "You're going too slowly". Now I'm going to close them and hold them closed. I have to hold them because if I let them go they'll go forward and increase the speed. If I continue to reduce the speed, notice the bank angle limiter is decreasing. The bank angle is saying "You mustn't bank now". It's down to 5 degrees. The pitch limit indicator is going amber, at 213, telling me that's [enough?].

[Close examination of the cockpit tape reveals the plane is at 15000 feet]

Pilot: I'm getting an increase in stick force.

Computer: *Beep* Landing Gear. [!!!]

Pilot: Stick force is telling me "Move the nose down". I'm having to pull quite hard to stop the nose going down. So I'm now holding the throttles back, and I'm having to pull very hard on the stick. And I'm having to pull harder and harder on the stick.

Computer: *Alarm* [Presumably the Stall Warning]

Pilot: Alright and the stick's shaking.

[The plane is shown to stall]

[The pilot lets go of the throttles]

Pilot: And the ASC [?] goes out.

[The plane recovers]

No mention was made by the pilot or the narrator of the computer request for the Landing Gear. If you believe that the outside footage was truly from the same flight, the gear was up. So the computer wanted it down? Is this a good idea when your MD-11 is about to stall?

The pilot seemed to completely ignore the computer request.

Eric K. Olson, Editor, Lexington Software Design, 72A Lowell St., Lexington, MA 02173 (617) 863-9624 OLSON@HARVARD.BITNET harvard!endor!olson

---

Automatic Vehicle Identification (was driving and privacy)

Ed Ravin <eravin@panix.UUCP>
Thu, 4 Apr 91 16:41:06 GMT

At a recent meeting of the Comittee for an Auto-Free New York, a fellow from TRANSCOM, a consortium of NY/NJ regional transportation authorities described how they hope to use an Automatic Vehicle Identifaction system (AVI) that is going to be implemented in the New/Jersey-Staten Island- Brooklyn corridor to keep track of traffic speeds and alert them of possible traffic jams forming. As I understand it, here's how it will work:

The local toll authorities are going to install an AVI system at existing toll points, namely the bridges that link up New Jersey and Brooklyn to Staten Island. These readers will identify vehicles that are participating in the AVI system and bill them for using the bridge.

TRANSCOM wants to install more AVI readers every few miles along the highways feeding the bridges. Then they want to take the vehicle ID's from the bridges and notice when they encounter the same vehicle ID's at various points along the highways. Their computer will then be able to calculate the average speed of the tagged vehicles and set off an alarm if the average speed is below some threshold, indicating that there is a traffic incident of some kind slowing things down.

It seems that this technology could also be used to generate automatic speeding tickets, perhaps even billed to the same account that's being used for the toll payments. One point to make is that TRANSCOM expects that the vast majority of vehicles participating in the AVI system will be commercial vehicles, especially trucks and busses. One could argue that privacy is less of a concern for commercial operators, especially if all their routes and itineraries are logged by other means already.

It seems that as soon as someone comes up with a new way of getting computerized information about something, someone else will come up with another application for the data that wasn't in the original plan.

Those of you in the Northeast will also be happy to hear that all the toll

authorities from Harrisburg, PA to Buffalo, NY have all agreed to use the same AVI system for their future automatic toll collections.

Ed Ravin cmcl2!panix!eravin philabs!trintex!elr

---

dealing with billing errors

Scott Schwartz <schwartz@groucho.cs.psu.edu>
Wed, 3 Apr 91 20:45:08 EST

I heard an interesting story on a local radio station (WPSU) today. It was about a family that had recently moved into a new house; when they got their phone bill for that month, the charge was more than 18 million dollars. They realized there was a mistake, but decided to pay the bill anyway. They wrote a check for that amount, dated it "April Fool's", voided it, and mailed it to the phone company. Bell of PA was reportedly "very helpful" in clearing up the erroneous charge.

Two obvious risks include the usual problems with computer generated bills, and the ever present danger that someone on the collecting end may not have a sense of humor.

Computer Ballot Tally

Richard Wexelblat <rlw@ida.org>
Thu, 4 Apr 91 15:01:12 EST

Later this year, I'll be helping to validate the computer tally of ballots in the ACM election. In brief it works like this:

Before the Validators get there, the company has opened any ballots with signatures on the outside and run the ballots through the readers. Any that fail are put aside. So when we arrive, we get four things: ballots that passed, ballots that failed, ballots that weren't opened, tally. (Another category, ballots returned for bad address, are a separate matter.)

We then select at random about 1% of the "passed" group and tally them manually. Then they are run through the computer and the computer output compared with the manual tally. If 100% match skip next step

> If discrepancy, resolve it (manual tally error).
> (No machine discrepancy has yet been discovered; don't know what to do if one occurs)

We then open all unsigned ballots. If a signature inside, manually add to tally; if none, ignore ballot.

Certify (possibly amended) tally.

Question: is this felt to be a reasonable method?

If you have a simple yes/no/maybe response, please mail directly to me.
If a subtantive problem or suggestion for improvement, copy risks for
possible inclusion in a future posting.

Dick Wexelblat (rlw@ida.org) 703 845 6601

Open forum on computer voting system standards

"Peter G. Neumann" <neumann@csl.sri.com>
Thu, 4 Apr 91 14:29:19 PST

On Wednesday 17 April 1991 in Room T640, George Washington Univ. Academic Center, 22nd and Eye (I) St. NW, Washington DC, there will be an open forum on Developing Standards for Computer Voting Systems. Roy Saltman (NIST) and Howard Jay Strauss (Princeton) will be the speakers, and Eva Waskell will moderate. All three have been quoted in or contributed to The RISKS Forum in the past, on this topic. DC Area folks should try to attend. (Someone PLEASE write a report for RISKS, and agree among yourselves who it should be.) The meeting is sponsored by the Washington D.C. chapter of CPSR (Computer Professionals for Social Responsibility). For information, phone 703-435-1283.

Re: Len Rose (TK, RISKS-11.36)

Andrew Tannenbaum <trb@ima.isc.com>
Thu, 4 Apr 91 15:33:35 -0500

> I have yet to hear even a marginally literate Unix type claim that, despite
> prosecutors' claims in press releases (where they try to create meanings and
> images that they couldn't do at court), login.c is a realistic "hacking
> device."

Let me do that for you then. Having root access on a UNIX system X gives you access to that system, and to any other systems that trust system X (through passwordless rlogin using rhost files, and so forth).

Replacing a copy of /bin/login on a UNIX system to harvest passwords gives you keys to other systems, assuming that people use the same passwords on multiple systems, as many do.

So if you can replace /bin/login, then manipulation of login.c is a legitimate hacking device, and one that I have seen used in practice. (Yes, it may be possible to replace /bin/login with a replica without knowing exactly what it does, but if you're a crook, it's comforting to know whether /bin/login has tamper-resistance safeguards in it.)

Andrew Tannenbaum Interactive Cambridge, MA +1 617 661 7474

Another computer time/date processing problem

"29706::MLC" <mlc%29706.decnet@consrt.rockwell.com>
4 Apr 91 12:59:00 PST

As several people have noticed, we don't have to wait until the years 1999 - 2001 to be affected by bad time/date processing via computers. On our DEC VAX system on January 2, 1991, I entered the following command to get some information about system processes:

```
   $ SHOW SYSTEM
```

Note the "Uptime" value (days hh:mm:ss). Our system isn't *that* good!

```
VAX/VMS V5.3-1  on node GV3   2-JAN-1991 15:40:47.36   Uptime  366 04:36:58
  Pid    Process Name    State  Pri      I/O       CPU       Page flts Ph.Mem
20200081 SWAPPER         HIB     16        0   0 00:00:40.89         0      0
[rest of output deleted...]
```

Michael Cook mlc%gva.decnet@consrt.rok.com

Search RISKS using swish-e

Report problems with the web pages to the maintainer

Search RISKS using swish-e

THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

ACM Committee on Computers and Public Policy, Peter G. Neumann, moderator

Volume 11: Issue 39

Thursday 4 April 1991

Contents

Computers, Freedom, Privacy Trip Report

Rebecca Mercuri <mercuri@grad1.cis.upenn.edu>
Mon, 1 Apr 91 22:56:31 EST

The following constitutes my trip report for the Computers, Freedom and Privacy Conference held March 26-28, Airport Marriott Hotel, Burlingame, California. Although I have made a sincere attempt to relate the events of the conference in a fair and unbiased manner, the nature of the material covered entails a certain amount of emotion and it is difficult, if not impossible, to separate one's own feelings from the subject matter. I therefore apologize for any inadvertent mistakes, omissions, or philosophical commentary. Readers are encouraged to send corrections to me at the email address below. No flames please!

Respectfully submitted, R. T. Mercuri mercuri@gradient.cis.upenn.edu

  [Edited lightly by PGN and included in RISKS with permission of the author.]

==========

The First Conference on Computers, Freedom and Privacy was organized and chaired by Jim Warren, and sponsored by the Computer Professionals for Social Responsibility (CPSR). Numerous other organizations also lent their support to the conference, which was attended by approximately 400 individuals (described by Terry Winograd as ranging from the sandals of Silicon Valley to the dark

suits of Washington) covering the fields of law, investigation, programming, engineering, computer science, hacking, industry, media, academics, government, law enforcement, and civil rights. The crowd was about 75% male, with very few minorities in evidence (only ~10% of the speakers were female, and none were minorities). Attendees formed a veritable who's who of hacking with key figures such as Captain Crunch, Phiber Optik, Steve Jackson, Craig Neidorf, and other notables there, some accompanied by an entourage of defense and prosecuting attorneys. Cliff Stoll and Ted Nelson (separately) took the opportunity to distribute copies of their books and give autographs. (Cliff was fond of playing with a brightly-colored yo-yo and writing memos to himself on his hand, Ted appeared to be creating a video record of the conference by filming each speaker with a small hand-held camera for a few seconds as each talk began.) A list of attendees was distributed, providing all information that each participant marked as "open". The vast majority of participants provided their name, company, address, phone number and email address. Some people remarked privately that had they been more aware of the manner in which such information is currently being used, they likely would have "closed" more of their own data. (The list was printed in name-alphabetical order so it was unfortunately possible to derive the names of individuals who elected not to be listed.)

Jim Warren, who described himself as a self-made multi-millionaire, entrepreneur, futures columnist, and member of the board of directors of MicroTimes and Autodesk, Inc., took a severe loss on the conference. He had estimated break-even at 500 participants, but had only achieved around 300 paid admissions as most of the media and some staff members attended for free. To his credit, he organized a fast-paced, well-run (on-time) conference which allowed many of the key figures in this field to present their thoughts and ideas. Audio and videotapes, as well as the conference proceedings (published by Springer-Verlag) will be available shortly [write to CFP Proceedings, 345 Swett Road, Woodside, CA 94062]. The conference was preceded by a day of tutorial sessions, but I was unable to attend those activities.

My major criticism regarding the conference was that the sheer volume of speakers (over 20 per day) allowed little time for questioning from the audience. Many of those who were not wearing red speaker's badges began feeling like second-class citizens whose opinions were neither wanted nor recognized. If someone managed to obtain a microphone and used it to make a statement rather than to ask a question, they were routinely hissed by a large portion of the audience. The unresolved tension became most obvious on the last day of the conference when, during the panel discussion on Electronic Speech, Press & Assembly, a loud altercation broke out in the front of the room. This panel had a representative from Prodigy Services, but the person who was supposed to give opposing commentary (apparently regarding the email privacy issue) had been unable to appear. Certain attendees were prepared to present their views, but were informed that they would not be permitted to do so. A private meeting was arranged for those who wished to discuss the Prodigy matter, but many found this to be unacceptable.

An oft-heard word describing the material revealed during the conference was "chilling". After the second day of the conference I became aware of how invasive the monitoring systems have become. As I returned to my room within the hotel, I realized that my use of the electronic pass-key system could alert the hotel staff of my entry and exit times. People could leave messages for me,

which would be reported on my television screen, all of this being recorded in some database somewhere, possibly not being erased after my departure. My entire hotel bill, including phone calls and meal charges could also be displayed on my television screen, along with my name, for anyone to access (without a password) if they were in my room. Chilling indeed. Pondering all of this, I left the room, lured to the hotel lobby by the sound of what I assumed to be a cocktail piano player. When I located the baby grand piano I realized that, through the high-tech wonders of Yamaha, no human sat at the keyboard. A sophisticated computerized unit rendered a seemingly- endless sequence of expertly arranged tunes, with no requests allowed from the audience. This ghostly image reemphasized, to me, the silent pervasion of computers into our daily lives, and the potential erosion of personal freedom and privacy.

Throughout the conference, many problems were posed, few answers were given. Factions developed --- some people felt we needed more laws, some people felt we needed fewer laws, some felt that all data (including program code) should be free and accessible to everyone, some felt that everything is personal property and should be specifically released by the owner(s) prior to general use. Certain people felt that all problems could be resolved by tightly encrypting everything at all times (the issue of password distribution and retention was ignored). What was resolved was to form an organization called the US Privacy Council which "will attempt to build a consensus on privacy needs, means, and ends, and will push to educate the industry, legislatures, and citizens about privacy issues." The first thing this organization did was form a newsgroup, called alt.privacy. I observed that at least 50 messages were posted to this newsgroup within the 3 days following the conference, most pertaining to privacy of emails. This was disappointing, to say the least. Presumably people will use the mailing list and the newsgroup to disseminate information, but whether this is merely a duplication of other existing newsgroups (such as RISKS), and whether the Privacy Council will have any impact at all, shall be left to be seen.

The conference opened with a comment by Jim Warren that this meeting could be "the first Constitutional Convention of the new frontier". He then introduced Harvard Law Professor Lawrence Tribe who used the analogy of cyberspace to describe some of the problems of a "virtual constitutional reality". He quoted Eli Noam as saying that "networks become political entities" and that there could conceivably be "data havens", private networks much like Swiss bank accounts, which are virtual governments in themselves. He asserted that a bulletin board sysop is not a publisher, in the same way that a private bookstore owner is not a publisher. The individual merely makes the products available, and has the responsibilities of a seller, not a publisher. Tribe then went on to delineate five major points. First, there is a vital difference between governmental (public) and private actions. Second, ownership is an issue that goes beyond that which may be technologically feasible. Property encourages productivity. You have a constitutional right to inhabit your own body. Free speech may be a luxury we can't afford (like yelling "fire" in a crowded theater, or viruses roaming the network). Third, the government cannot control speech as such. Recently it was ruled that answers to very simple questions (such as your name, age) are considered testimonial, as they require the use of the human mind. Fourth, the Constitution was founded on a normative understanding of humanity, and should not be subject to disproof by science and

technology. The words of the 4th Amendment apply to material things, it defends people, not places. It is the task of law to inform and project an evolutionary reading of the bill of rights to new situations. Fifth, Constitutional principles should not vary with accidents of technology. In conclusion, Tribe proposed an additional amendment to the constitution which asserted that "this Constitution's protection for freedom of speech, press, assembly...shall be construed as fully applicable without regard to the technological medium used."

The first panel discussion of the conference was titled: Trends in Computers and Networks. Peter Denning of NASA Ames introduced the panel by stating that computers are now under attack due to security being added on as an afterthought. John Quarterman of Texas Internet Consulting then discussed the manner in which user/host names could be made more readable (accessable) on the network. Peter Neumann of SRI overviewed general issues surrounding the authorship of the "Computers at Risk" book, stating that the group involved with the text was primarily interested in motivating efforts towards evaluating safe, secure, reliable systems (and that they only proposed general guidelines in the text). He warned the listeners "don't wait for the catastrophe". Neumann also mentioned the issue of disenfranchization of the poor and lower class who will be unable to access the new technology, stating that "gaps are getting much bigger". Martin Hellman of Stanford University discussed cryptography. He stated that the 56 bit DES standard was set not by technology, but instead by economics. He mentioned a study at Bell Labs that indicated that 70% of all passwords there could be cracked using a dictionary technique. He believes that technology will not solve all of our problems, and that persons who are concerned about social responsibility are not (necessarily) anti-technical. David Chaum of DigiCash spoke about informational rights and secure channels with regard to electronic money transactions. He believes that with an adequately encrypted system there is no necessity for a central, mutually trusted party. The problem is in finding a practical encryption protocol, or a distributed, mutually-trusted tamper-proof box solution. David Farber of the University of Pennsylvania expressed the view that protection schemes might not be "retrofittable" and should be part of the fundamental design of computer architecture, protocols and technology, rather than being tacked on, but he worried that people may not be willing to pay for these design features. Farber also mentioned the possibility of retroactive wiretapping, where archived data could be obtained through invasive means.

The second panel session was titled: International Perspectives and Impacts. Ronald Plesser of the Washington D.C. law firm of Piper & Marbury first mentioned that these issues impact on how international business is conducted. Many countries, particularly in Europe, have already established standards with which we must comply. Databases feeding Europe must be concerned with the processing of personal data of individuals. Certain directives have been authored that are so general in scope as to be difficult to apply ("to all files located in its territory" was one example). Tom Riley, of Riley Information Services in Canada, continued this discussion regarding data protection policies. He urged the authoring of a harmonized directive, similar to that for other exports. The United States, by lagging behind in establishing standards of its own, risks the possibility of losing the opportunity to affect these policies as they are being written. David Flaherty entertained the crowd with his "George Bush" speech, stressing that "privacy begins at home". Robert Veeder of the D.C. Office of Information Regulatory Affairs discussed the impact of the 30,000+ messages to Lotus which effectively stopped the

production of their CD-ROM database. This electronic lobbying had never been used to such great effect prior to that time. He believes the electronic forum will provide larger access to public concerns. (The impression I was left with was that certain governmental agencies are not wholly enthusiastic about this powerful method of expression, and that they are monitoring the situation.)

Next, we heard from a variety of speakers on the subject of Personal Information and Privacy. Janlori Goldman, of the ACLU, discussed the "library lending" project by the FBI. This was an attempt to track library usage habits of foreign nationals. The ACLU objects to this sort of surveillance as well as other similar broad-based methods. An audience member criticized the ACLU's own release of membership data, to which Janlori replied that she did not agree with her organization's policy to allow such releases, but was currently unable to do more than protest against it. John Baker, Senior Vice President of Equifax, described the benefits of information with regard to improved goods, services, prices, convenience and wider choices. (Equifax is an organization which supplies marketplace data with specific information about consumers.) He stressed that people need to understand their rights, responsibilities and opportunities with regard to their published data. He believes that the Lotus Marketplace product was flawed because of the delay involved when customers wanted to "opt-out" of the database. He portrayed a spectrum of controls over data usage, ranging from no restrictions (free speech), through some restrictions (based on impact, sensitivity, access, security and confidentiality), to absolute restrictions (where the available information would have little value). Equifax took a survey on consumer interest in availability of data for direct marketing purposes which revealed that 75% would find it acceptable as long as there is a facility to opt-out. An audience member raised the point that the default is opt-out rather than opt-in.

These two speakers were followed by a debate between Marc Rotenberg, Washington Office Director of the Computer Professionals for Social Responsibility, and Alan Westin, Professor of Public Law and Government at Columbia University, with the subject "should individuals have absolute control over secondary use of their personal information?" Marc argued in favor of the statement, using an eloquent oratorial style, and Alan spoke in opposition with the demeanor of a seasoned litigator. Marc made such statements as "we are all privacy advocates about something in our personal lives", "it is the most fragile freedom" and "protect privacy, change the default", stressing that the individual should have the right to control the value and use of their personal information. Alan outlined four major issues: 1. Nature of the secondary use; 2. Society should decide on fair uses, not a nihilistic veto; 3. Underpinning of constitutional democracy; 4. Adequate control protects against potential misuse. He believes that the consumer benefits from the advantages of a knowledge society. No winner/loser of the debate was declared.

Speakers continued on the subject of Personal Information and Privacy. Lance Hoffman, of the EE & CS department at George Washington University, mentioned that Japan will be instituting a system of personal phone number calling --- basically you can send and receive calls at your "own" phone number wherever you happen to be situated. This permits very close tracking of individual movements and is a potential further invasion of privacy. He noted that no one has ever received the ACM Turing Award for a socially responsible system, and

encouraged positive recognition of achievements along these lines. He also recommended that a "dirty dozen" list of worst systems be compiled and distributed.

Evan Hendricks, editor and publisher of Privacy Times, listed many records that are and are not currently protected by law from distribution. Interestingly, video rental records are protected, but medical records are not. He cited an interesting example of a circumstance where a man and woman living in the same home (but with different last names) were sent copies of each other's bills, urging them to encourage their "roommate" to pay. It turned out that the individuals were landlady and tenant. Another interesting fact that Evan revealed was that studies indicate ~30% of social security numbers in some databases are inaccurate. Lists of persons having filed Workmen's Compensation claims have, in some cases, been used to blacklist people from jobs. Hendricks urged people to ban the recording and distribution of human genome information --- some parents voluntarily provide cellular test results in case their child is later missing or kidnapped. There is no way to know how these records are likely to be used in the future.

Tom Mandel, director of the Values and Lifestyles Program (VALS) at SRI, spoke in favor of the Lotus Marketplace product. He felt that the 30K response was not representative of the general public, and believes that a small percentage of "media sophisticates" can have apply greater leverage. He noted that VALS is currently involved with a joint venture with Equifax, who is currently involved with a joint venture with Lotus.

Willis Ware, of the RAND Corporation, chaired the HEW committee that led to the 1980 privacy act (a reporter preparing materials for publication can not be searched). He felt that the government previously was considered to be a threat to privacy, not a protector, and considers the privacy issue as one of social equity. He indicated that personal information should not be considered to be private property, and should be shared in an equitable manner. To apply royalties for usage would place a tremendous impact on costs. He noted that the databases behind airline, pharmacy and point-of-sale systems may be open to access by various groups including the Internal Revenue Service and Drug Enforcement personnel.

Simon Davies, a member of the law faculty at Australia's University of New South Wales, provided a sobering criticism of this conference and the United States' policy making processes, stating that the conference was too "nice" and "conciliatory" and that the "US is an embarrassment to the privacy issue". He used the term "pragvocate" (pragmatic advocate) to describe policy-makers who are well-trained, say the right things, and denounce extremes, giving environmentalists as an example. He reminded us that the basis of the US system is not to "opt-out" --- no one would write to the LA police asking "don't beat me up". Davies alerted us to the fact that Thailand, an oppressive military government, is currently purchasing US technology to provide smart ID cards for their citizens. He noted that the Smithsonian Institute awarded them a trophy for their use of technology. He stated that the United States is encouraging similar activities in the Philippines and Indonesia.

A somewhat light-hearted after-dinner talk was delivered by Eli Noam, of Columbia University's School of Business, on the subject of "reconciling free speech and freedom of association". He suggested that phone systems be

established whereby individuals can provide their friends and associates with special access codes so that they can dial them. Others can call, but at a higher rate. (Note that this would likely have an adverse impact on legitimate business and social calls as well as possibly reducing undesirable calls.) He stated that presently "no computer can write the 4-line plot capsules that appear in TV Guide", with regard to the failure of AI systems. Noam questioned the lack of policies concerning what happens to an information data base after an individual's death. He concluded with the statement that for "all digital systems --- 0's and 1's are created equal."

The second day of the conference opened with a session on Law Enforcement Practices & Problems. Glenn Tenney, well known as the organizer of the Hacker's Conference, chaired this panel with little comment. Don Ingraham, Assistant DA of Alameda County, Calif. (who, during a tutorial earlier in the week, distributed information on the writing of search warrants), gave a fantastically humorous presentation. He spoke of the "pernicious myth of cyberspace" and declared "you ARE the country". He mentioned that systems exist with "the security built in of a sieve" and that people have their information on these systems, but not necessarily because they want it to be there. He feels that the attitude of "don't worry, we don't need standards" is a poor one, and that laws should be written to let the people know what the rules are. He would rather see an organization formed called Sociable Professionals for Responsible Computing (instead of CPSR). He finished his talk by saying "if you don't do it, who will -- if not now, when" (a Talmudic quotation that he used without citation).

Robert Snyder, of the Columbus Ohio Police Department, presented the view of the "cop on the street". He spoke of his naivete when first entering the field of computer law, and how much evidence was destroyed at first by listening to suspects who told him to type things like "format c:" in order to access the hard disk. He has encountered situations where the suspect actually does not know what is on the system --- some of these are cases where a parent is running a business and a child is using the machine for illicit hacking purposes. In these cases, even though he has a warrant to obtain all of the computer equipment, he often will not shut down a legitimate business. He brought up the issue of unregistered software sitting on a confiscated system. There are liability problems dealing with the return of such materials. Basically he stated that the law enforcement personnel require further education and training, and should operate within guidelines but with prudence.

Donald Delaney, Senior Investigator with the New York State Police, began his talk by relating how when his home was burglarized in 1985, he experienced a feeling of violation. This feeling is much the same with computer crime. Many firms experience a loss of income from such activities. In his experience, many of the people caught are engaged in more crimes than the ones they are charged with.

Dale Boll, Deputy Directory of the Fraud Division of the U.S. Secret Service, spoke of the various forms of access device fraud (credit card, ATM, passwords, phone access, frequent flyer numbers, etc.). He stated that it is illegal to posses counterfeit access devices and that if you have 15+ illegal access devices or numbers in your possession, you may be a subject of federal investigation. They have a 96% conviction rate. ATM cards can be manufactured

illegally using cardboard and regular audio tape. The credit card industry is now losing $1 Billion per year. An audience member asked if they are using programs like Gofer (grep for UNIX hackers) to search for information they want on bulletin boards and networks. He replied that although they own this program, they use it personally and not for investigation purposes. The next session, on Law Enforcement and Civil Liberties, had seven participants, none of whom were given much time to present their views. I will briefly highlight what they said here. Sheldon Zenner, the Attorney for Craig Neidorf said that the prosecutors had originally sought a 2-year sentence, and that thanks to many of the people at this conference who rallied to Craig's support, they were able to get him off. Mark Rasch who defended the internet worm case stated that the expectation of privacy is changed because of the technology employed --- technology affects behavior. Cliff Figallo, manager of the WELL (Whole Earth 'Lectronic Link, popular among many Bay Area participants as an alternative means of accessing the Internet) addressed his concerns about overuse of law enforcement. He wants his users to feel safe. Sharon Beckman, Litigation Council to the Electronic Freedom Foundation (EFF) and Attorney for Steve Jackson Games (whose computers were seized, when one of his fantasy games was perceived as being capable of training users to "hack" into computers) stated that underlying values of the constitution should be interpreted in terms of today's technology. Ken Rosenblatt, a District Attorney covering the Silicon Valley area, stated that he is charged with upholding civil liberties and feels that the laws are presently adequate. Mike Gibbons, Special Agent for the FBI, mentioned that he worked various white collar cases, including the 75 cent case (described in Cliff Stoll's book), and the Robert Morris case. He feels that there are various classes of computer crime, including impairment, data theft, and intrusion. Mitch Kapor, founder of EFF, stated that the "electronic frontier hasn't been settled yet" and that we should not stifle the "network petri dish inventing the future". He questioned the nature of reasonable search, stating that there haven't been enough cases yet to establish a meaning for this in computer law. Everyone should be protected from tyranny, not only hackers. He looks at the EFF as a means of civilizing cyberspace. The matter of free speech was discussed in the questioning session with the panel -- much speculation was directed towards the legality of discussions of bomb-making, system hacking, and the publication of other potentially lawless activities on the net or in technical papers. Other comments included the fact that law enforcement cannot seize an entire post office, their search must be limited to the mailbox of the suspect. This analogy applies to computer networks as well, although the volatility (ease of total destruction of evidence) of computer data is of concern to investigators.

As I had an extended and quite insightful conversation with Russ Brand over lunch, I returned a tad late to the next session, on Legislation and Regulation, and was only able to catch two of the speakers. Elliot Maxwell, Assistant Vice President at Pacific Telesis stated that it is "difficult to have simple and specific rules". Paul Bernstein, whose LawMUG BBS and Electronic Bar Association is well known among the legal community, stated that one should "use mediums that exist -- participate in fashioning the laws."

The most eye-opening session of the entire conference, in my opinion, was the following one on Computer-Based Surveillance of Individuals. It opened with Judith King describing the FBI Library Surveillance Program, where the reading habits of foreign nationals were investigated. She stated that many librarians

want laws to protect the confidentiality of users, and some statutes have been passed. Karen Nussbaum, Executive Director of 9 to 5 (on which the film was based), gave an accounting of the monitoring of employees in the workplace. Currently over 26 Million employees are having their work tracked electronically, and over 10 Million have their pay based on computer evaluations. The personal habits of the worker can be monitored, one can look into a user's screen and see what they are doing or even send them messages. She described the "corporate plantation" as a place of stress, humiliation and harassment. Gary Marx, Sociology Professor at MIT, gave a whirlwind assessment of the importance of privacy, some technofallacies (like the Wizard of Oz "pay no attention to the little man behind the curtain"), and steps you can use to protect privacy (the bulk of these useful lists are published in the proceedings). He related how a telephone can be made "hot on the hook" so that you can silently monitor your babysitter, your children or your spouse, when you are not at home. Most devices, such as this one, are perfectly legal within your own house. David Flaherty spoke again, this time in a more serious vein, saying "we are living in a surveillant society" and "you have to make daily choices about what you are willing to give up about yourself." The second day's after-dinner speaker was William Bayse, Assistant Director, Technical Services Division of the FBI, who discussed a newly created national system called the NCIC-2000, under the topic of "balancing computer security capabilities with privacy and integrity". He began by asserting that crime has become more mobile and that conventional crime-tracking methods are inadequate. For example, he said, many missing persons actually want to remain missing. He feels that the accuracy of records is imperative. Various information bases have been formed, including lists of stolen items, vehicles, and wanted persons. Presently 65,000 officers are using this system, with 360M transactions annually, at a cost of 3 cents a transaction. For an example of effectiveness, over $1.1 Billion in vehicles have been recovered. Proposed, but not yet implemented is the portion of the system which provides a live scan of fingerprints at the scene of an arrest (or when someone is stopped for a motor vehicle violation) [with the intended purpose of considerably reducing false identifications... PGN]. Much criticism was generated from the audience regarding the potential misuse of this system for harassment, and the retention of fingerprints for future use. Marc Rotenberg addressed Bayse questioning why documents requested under the freedom of information act from his agency have still not been supplied, and stating that currently a lawsuit is pending to obtain their policies regarding monitoring of computer bulletin boards. Bayse refused comment.

The final day of the conference opened with a session on Electronic Speech, Press and Assembly. Jack Rickard of Boardwatch Magazine mentioned that bulletin boards are highly specialized, primarily funded by individuals, and are in their embrionic stage. David Hughes, Managing General Partner of Old Colorado City Communications, added some color to the conference with his western garb (10-gallon hat, bolo tie) and use of his laptop for the notes of his speech. He described himself as a "Citizen of the Western Frontier of the Information Age" and drawled, "Read my Cursor". He described electronic speech as "fingers of the tongue with the ear for the eye --- but it is still speech". In describing US history, were it to have occurred today, Jefferson would have used a Macintosh, Adams would have used a PC, but "Tom Paine would have put Common Sense on a private BBS with a Commodore 64". "Don't tread on my cursor!" he cried. George Perry, Vice President of Prodigy, began by saying that he did not

want to engage in discussion on the dispute, but then stated that "Prodigy does not read private email". Prodigy is a privately owned and operated company which believes that the market should be allowed to decide what services need to be provided. The Constitution regulates free speech with respect to the government, Prodigy thinks of itself as a publisher. Lance Rose, a NY Attorney, enumerated the types of rights afforded to individuals and companies with regard to ownership, including trade secrets, confidentiality, trademark, copyright and patent. There is currently a great diversity of laws which service providers must adhere to, making the provider, in some instances, a law enforcement agent. During the open comment section, Hughes noted that very few legislators are currently on-line, and he thanked Prodigy for preparing the NAPLPS market (for his products).

The notable talk in the Access to Government Information session was David Burnham's (Co-Director and Writer with the Transactional Records Access Clearinghouse [TRAC] in D.C.). He stated that "badly administered agencies are more damaging than rogue operations". The objectives of TRAC are to obtain transactional data from federal enforcement agencies, such as the IRS, NRC, and Justice Department. He demonstrated how the raw statistics could be combined with additional figures regarding inflation, population, and margin of error, showing that the so-called "trends" of increasing crime, or increased non-compliance with tax law, were actually flat lines when the mitigating factors were added in.

The final panel discussion was on Ethics and Education. Richard Hollinger, Sociology Professor with the University of Florida, asserted that the "same officers who are investigating computer crimes are the ones who are protesting computers in their patrol cars because they feel it would be oppressive." He is concerned with the industry's encouragement of the use of computers in schools, before rules for their ethical use have been written. Donn Parker with SRI stated that laws are needed in order to convict hackers. Convictions have a "very good effect on our whole problem", he said. He referred back to the 60's when the ACM and IEEE drafted codes of conduct, and said that these should be popularized. He believes that one can not teach ethics, that it comes from interpersonal relationships, and (for him) the Christian religion and the Bible. One can teach, he believes, the application of ethics, beyond the golden rule. He delineated three rules: 1. The Owner's Rule - you choose to issue your property into the public domain, or not; 2. The User's Rule - you assume everything belongs to something else, unless otherwise informed; 3. The Hacker's Rule - systems are free, everything should go to the people (which he rejected as childish, not worth considering). He suggested that we consider the dilemma of Descartes -- if it is OK to start by stealing pencils, where then can we draw the line? Dorothy Denning spoke briefly regarding the network uses by children (Kids Net). She speculated that we should teach them something about hacking in order to take the mystery out of it. She compared telephone fraud by children as a more sophisticated version of the "is your refrigerator running" prank.

The Education and Ethics panel continued with the softspoken John Gilmore, a "generalist" with Cygnus Support. He warned that we are losing the larger open society. The US is currently #1 in percentage of population in jail. He spoke of drug usage as a victimless crime. John asked the audience "who has not broken a law in the past month?" Only a few raised their hands. He then asked "who here has all their disks clean -- free from something you would not want

them to find if you were investigated?" About 15% raised their hands, but after pondering it, a number of them lowered them (the person behind me muttered that he had some shareware for which he had not paid). Gilmore said "privacy is a means -- what is the end we are looking for? Tolerance." He urged real privacy of personal communications, financial transactions, things should be as "private as that thought held in our minds." He demanded that we stop building fake systems -- laws that dictate that you "can't listen to cellular phone calls" -- and instead build real protections into your systems and buy them from others. His talk received a standing ovation from the vast majority of the audience members.

The remaining panel speaker, Sally Bowman, a Child Psychologist with the Computer Learning Foundation, stated that her organization is working to raise awareness and solve a number of problem areas. The problems she outlined were: 1. Lack of awareness of the magnitude of the problem. Software industry is being hurt by piracy; 2. Many misimpressions -- confusion, lack of information; 3. Lack of teeth in software copying policies; 4. Lack of strategies in teaching ethics; 5. School budgets are too small to allow legal procurement of software. Her organization is presently educating parents as to the "tell-tale" signs which indicate whether a child is "abusing" computer systems.

The concluding session, entitled "Where Do We Go From Here" was staffed by a number of the conference speakers. They overviewed their feelings regarding the issues raised during the sessions and made general comments with respect to what they might do to raise awareness and resolve some of the problems. Throughout the conference many pamphlets, brochures and newsletters were distributed. Although it is infeasible for me to provide copies of this literature, interested parties can contact me or Jim Warren (jwarren@well.sf.ca.us) to provide source names and addresses. Some of the more interesting items (in no particular order, just how they happened to come out of my briefcase) included:

- Brochures from the Cato Institute "Toward a Moral Drug Policy", "America's Counter-revolution", "The Semiconductor Industry and Foreign Competition", "The Promise of High-Definition Television: The Hype and the Reality", and their publication catalog.
- Matrix Information and Directory Services Newsletter.
- The Manifesto of Militant Humanism.
- "Are you a Hacker?" by Robert Bickford, reprinted from MicroTimes.
- Call for formation of a World Privacy Network.
- An advertisement for SafeWord Software (password checking/protection).
- Condom distributed by Anterior Technology (they market a system whereby you can retrieve the first 80 characters of emails while out of town).
- "The Bill of Rights is Under Attack" from Committee for the Bill of Rights.
- Hollywood Hacker Info, reprinted from Computer Underground Digest.
- Calif. State Assembly Bill #1168 on Personal Information Integrity.
- Computer Learning Month - from the Computer Learning Foundation.
- The Equifax Report on Consumers in the Information Age
- A reprint of John Barlow's article "Crime and Puzzlement" from Whole Earth Review, Fall 1990.
- Various brochures from the First Amendment Congress, an organization providing educational materials on the First Amendment.
- Policy papers from the League for Programming Freedom including "Against Software Patents", "Lotus Disinformation Forewarned is Forearmed",

and the Effector (its newsletter).
- CPSR reprints of newsarticles regarding the Lotus database.
- Promotional literature for Ted Nelson's Xanadu.
- Brochure for the Community Memory BBS, and its newsletter.
- Brochure for the Art Com Electronic Network.
- Brochure for the International Society for Individual Liberty.
- Various copies of MicroTimes.
- Application forms for CPSR and the League for Programming Freedom.
- Rel-EAST, the east-west high-tech business report.
- Suggested reading on how computer crime is investigated from Don Ingraham.
- Book promotional literature including:
"Rogue Programs" edited by Lance Hoffman, Van Nostrand Reinhold
"Protecting Privacy in Surveillance Societies", David Flaherty,
University of North Carolina Press
"Spectacular Computer Crimes", Buck Bloombecker, Dow Jones-Irwin
"Using the Public Library in the Computer Age", Westin & Finger, ALA.
Directions & Implications of Advanced Computing, Vol. 1 and Proceedings
from 88 and 90, CPSR.
- Flyer announcing "The Privacy Project" an NPR series (for which I was
interviewed) to be broadcast in the Fall of 1991.
- Flyer advertising "Your Expanding Infosphere" an NPR ComputerTalk Program.
- Reason, a magazine for "free minds and free markets" whose cover story
was on cryogenics.
- Flyer on the National Apple Users Group Conference, June 7-9, 1991.
- Flyer on the Silicon Valley Networking Conference, April 23-25, 1991.
- Flyer on the third Chugach Conference, University of Alaska, Oct. 3-5,
1991. Plus Center for Information Technology News from U. Alaska.
- Flyer on the Calif. Forum of the First Amendment Congress, May 6, 1991,
Stanford University (free to the public).
- Flyer for the Electronic Democracy Conference, Sept 4-5, 1991.
- Calls for Papers from:
The National Conference on Computing and Values (Aug. 12-16, 1991)
Directions & Implications of Advanced Computing (May 2-3, 1992)

I returned home with a broader idea of the many facets of the computer freedom and privacy issue. I must now admit to being more worried than I was before I attended this conference, as to the lack of solutions being offered by my colleagues. Perhaps this meeting of the minds is a first start. More work needs to be done.

R. Mercuri mercuri@gradient.cis.upenn.edu

Search RISKS using swish-e

THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

ACM Committee on Computers and Public Policy, Peter G. Neumann, moderator

Volume 11: Issue 40

Friday 5 April 1991

Contents

Re: Computers, Freedom, Privacy Trip Report (RISKS-11.39)

Lance J. Hoffman <hoffman@eesun.gwu.edu>
Fri, 5 Apr 91 2:03:09 EST

RISKS readers of R. T. Mercuri's long trip report (RISKS, Volume 11, Issue 39, 4 April 1991) on the Computers, Freedom, and Privacy Conference who were not there now have a pretty good sense of what they missed. As our moderator said a few days ago in this forum, and as many have told me, it was one of the most thought-provoking and enjoyable conferences in a very long time.

One important point was omitted. Towards the end of the conference, a general consensus emerged that there should be a follow-on conference, and the general feeling was that it should take place on the East Coast. To make a long story short, Jim Warren and others twisted my arm with the result that I have become the general chairman of CFP-2, which will take place in Spring 1992

in Washington. This was announced during the last session. Many holdovers from the Bay Area based program committee and advisors have already agreed to serve, and we have some important East Coast people already lined up as well. We are already moving to obtain an appropriate site; the planning process has begun. We hope to keep the diversity of attendees (it indeed ranged from the sandals of Silicon Valley to the dark suits of Washington [Terry Winograd's phrase]) -- it's pretty rare to see most if not all of the computer crime prosecutors at the same conference with a large number of the prosecutees. We also hope to provide at least the same large amount of information transfer. Stay tuned!

And -- for those who were there and those who weren't -- suggestions are welcome and this is the best time to send them in; just mail them to me (address below).

Also, if you for some reason were not on the mailing list for this conference but wish to be kept informed about the next one, mail me your snailmail (and, optionally, email) address.

A few things I saw differently enough from Ms. Mercuri to comment on:

> "Jim Warren ... took a severe loss on the conference."

Final figures are not in yet, but the most recent appear to suggest this is not the case. (This is not posturing; I think it is just later information.)

> "What was resolved was to form an organization called the US Privacy Council which `will attempt to build a consensus on privacy needs, means, and ends, and will push to educate the industry, legislatures, and citizens about privacy issues.'"

This was not resolved by the attendees there, but in fact had been done before the conference; its first public meeting was held during an evening break, and had no official conference involvement (except that a breakout room was made available). It's important to note this because the conference, under Jim Warren's stellar direction, was hospitable to a number of points of view. CFP 2 will also serve this brokering function and will not itself take advocacy positions, but rather provide a platform for the contending ideas.

> "Robert Veeder of the D.C. Office of Information Regulatory Affairs discussed the impact of the 30,000+ messages to Lotus which effectively stopped the production of their CD-ROM database."

Rob Veeder will be surprised to hear that he works for the D.C. Government. In fact, that Office is part of the federal Office of Management and Budget.

> "Lance Hoffman, of the EE & CS department at George Washington University ... noted that no one has ever received the ACM Turing Award for [constructing a] socially responsible system, and encouraged positive recognition of achievements along these lines. He also recommended that a "dirty dozen" list of worst systems be compiled and distributed."

I said this *could be done*, but (ever cautious!) stopped short of *recommending* it (see the paper in the Proceedings).

> "Simon Davies, a member of the law faculty at Australia's University of New South Wales, provided a sobering criticism of this conference and the United States' policy making processes, stating that the conference was too `nice' and `conciliatory' ..."

I guess this ended when, on the last day, during the "Prodigy discussion", "a loud altercation broke out in the front of the room" [from the third paragraph of Ms. Mercuri's report]. Jim Warren was quoted (I think in the San Jose Mercury-News) as saying that the conference would be a success if (two speakers whose identities I forget) could speak without killing each other, or words to that effect. (They did.) Don Delaney from the New York State Police stated that he had never been to a conference with such a diverse group of attendees. I have *never* been to a meeting of such a diverse group where so much information (as opposed to rhetoric) was orally transmitted per unit time.

> "Mark Rasch who defended the internet worm case stated that the expectation of privacy is changed because of the technology employed --- technology affects behavior."

Mark actually *prosecuted* that case.

The Conference may indeed have started something. In addition to the L. A. Times 3/28/91 report of Laurence Tribe's speech already excerpted in RISKS, John Markoff wrote "Remember Big Brother? Now He's a Company Man" in The New York Times of Sunday, March 31. I've heard that Time magazine has a whole page on the conference this week, but I haven't seen it yet.

Professor Lance J. Hoffman, Department of Electrical Engineering and Computer Science, The George Washington University, Washington, D. C. 20052
(202) 994-4955 fax: (202) 994-0458

Re: Computers, Freedom, Privacy Trip Report

Dorothy Denning <denning@src.dec.com>
Fri, 5 Apr 91 10:46:31 PST

Kudos to Rebecca Mercuri for providing such a thorough and candid report of the first CFP conference. I'd like to elaborate on what she said about my talk in the Ethics and Education session:

> Dorothy Denning spoke briefly regarding the network uses by children (Kids Net). She speculated that we should teach them something about hacking in order to take the mystery out of it. She compared telephone fraud by children as a more sophisticated version of the "is your refrigerator running" prank.

My comment about Kids Net was made in the context of proposals I've heard to regulate modems and perhaps require an age limitation on their use (analogous

to getting a drivers license). I pointed out that many children have or will have access to networks at school, so I did not think it made a lot of sense to deny them that access at home. Regarding teaching "hacking," I was passing along a suggestion that a student made to me based on a positive report he had received from someone attending a school where it was practiced. In this context, hacking was referring to breaking into systems. Overall I'm wary of training young people to hack, but I can see some merit to telling students about it & why it's a crime. Regarding telephone fraud, it is not only more sophisticated, but also more costly, sometimes costing in the tens or hundreds of thousands of dollars. The reason I spoke about telephone fraud was to point out that it was not simply a question of a new technology, namely computers, that parents had no experience with, or of teaching computer ethics. The crimes under investigation by operation Sundevil, for example, are mainly toll fraud and credit card fraud.

The main point I tried to make in my talk was that we are letting our young people down by not taking responsibility for bringing them into the computing and network community as responsible users. Instead, the young people learn their ethics on their own or on BBS's run by teenagers. The consequences are that some basically good teenagers end up getting into serious trouble, which is very disruptive to their lives. One good way to teach responsible computing is to let students be responsible for computing in their schools. This recommendation is from Brian Harvey, who did it in the high school where he taught. Above all, we need to practice responsible computing ourselves, for example, by not using information gathered about individuals for one purpose for some other purpose.

Dorothy Denning

European Nervous System (ENS)

Pete Jinks <pjj@cs.man.ac.uk>
5 Apr 91 14:41:19 GMT

The 6th April issue of New Scientist carries a story on p.9:

"The ENS will create links between administrative computer networks [in the EC] including tax, social security and environmental monitoring. ... intense activity on police networks which ... will be essential when frontier control are relaxed in 1992". The EC "is seeking powers to make it compulsory for member states to to link their computer systems"

This is represented as being a vital part of a program to pump money into the european IT industry. I don't remember reading or hearing about this before. I hope that this is an April fool, but it has a ghastly ring of plausibility.

Draconian Accountability (re: Korean typographers)

<dmlaur@gauguin.Princeton.EDU>
Fri, 5 Apr 91 09:39:05 EST

this reaction forwarded for Prof. Michael Mahoney (mike@pucc.princeton.edu),

regarding Martin Minow's article on strict Korean typographic rules:

Check the Code of Hammurabi and, if I remember correctly, you will find that the builder of a structure that collapsed and killed the head of the household paid with his own life; if the collapse killed the owner's son, the builder's son paid the price of his life, etc. Similar Draconian rules governed the construction of buildings in other ancient cultures, leading to overbuilt, rock-steady structures. Now, suppose the programmers of, say, Airbus avionics software were subject to the same penalties. One adult life per adult life, etc. Suppose the programmer of an automated incubator had to place her own child's life as warranty. Would we see better software?

There is middle ground. We as a society could simply refuse to honor the disclaimers of liability that accompany software. We could start suing for damages, requiring into the bargain that the names of all participating programmers be attached to the product, if not for the purposes of suing them, then so that other companies could know who had contributed to the demise of ruined enterprise.

The trouble is, that despite all the complaints (correct and, if anything, understated) about defense software, DARPA is now riding high after the allegedly spectacular performance of weapons systems in Iraq. SEI at CMU has more money than it can spend. The products and the processes used to produce them are no better than on 16 January.

Mike

Small risk with Telephone cards

<hank@westford.ccur.com>
Fri, 05 Apr 91 01:05:05 EST

I just noticed this yesterday and although it is hardly a life threatening risk it still seems to be a bug. In Japan prepaid telephone cards have become very popular. Yesterday I made a call with a phone card that had only 1 unit of credit remaining. After dialing my call but before the othe party answered the phone debited my card to zero and returned it to me. If the other party hadn't answered I would have lost my dime. One can imagine: Late night in a storm only a phone card to make a life and death emergency call and ... :^)

Hank Cohen

Re: Tricky application of Caller ID (Re: Kiddie Call-in, RISKS-11.38)

Randal L. Schwartz <merlyn@iwarp.intel.com>
Fri, 5 Apr 91 09:00:47 PST

This sounds suspiciously like the 976-SANTA(?) in Seattle two years ago. Apparently, they ran a 1/2 hour "entertainment" show around christmas time, urging kiddies to stand by with their phones at the end of the show. The tones for the 976 phone number (along with the phone number on screen in case they

didn't have a touch-tone phone) came out over the speaker.

Caused quite a flack, if I recall.

Randal L. Schwartz, Stonehenge Consulting Services (503)777-0095
merlyn@iwarp.intel.com ...!any-MX-mailer-like-uunet!iwarp.intel.com!merlyn

---

Re: Tricky application of Caller ID

William Clare Stewart <wcs@erebus.att.com>
Fri, 5 Apr 91 11:35:44 EST

Aside from the use of caller-id mentioned here, it seems like an obvious
potential rip-off: Touch-Tone 1-900-EXPENSIVE

"Hey, kiddies - hold your phone up to the TV for a Big Surprise!"

Bill Stewart 908-949-0705 erebus.att.com!wcs AT&T Bell Labs 4M-312 Holmdel NJ

Re: E-mail role in LA cop probe (Fagan, RISKS-11.37)

The Polymath <hollombe@ttidca.tti.com>
4 Apr 91 20:57:43 GMT

}... Giving electronic messages the same validity as recorded voice is a bad
move, it seems to me.

Actually, it's a Good Thing. Recorded voice has no validity in a court of law
and hasn't for decades. It can only be used when backed up and confirmed by
eye (ear?) witness testimony. That's why someone has to actually _listen_ to a
wire tap, rather than automatically record and review at a more convenient
time.

Jerry Hollombe, Citicorp, 3100 Ocean Park Blvd., Santa Monica, CA 90405
{rutgers|pyramid|philabs|psivax}!ttidca!hollombe (213) 450-9111, x2483

Re: Len Rose (RISKS-11.37)

Mike Godwin <mnemonic@eff.org>
Fri, 5 Apr 91 08:19:45 EST

Steve Bellovin writes about the Len Rose case:

"The prosecutor must demonstrate intent to misuse in such cases. If possesion
of ``hacking tools'' were against the law (as far as I know, it's not, and
given how loosely many such statutes are drawn, that's probably just as well),
there would be a considerable burden of proof. Maybe such evidence could be
produced in this case, maybe not. But it's far from unreasonable to claim that
hacking is at issue."

What makes it unreasonable to claim that Rose is a hacker is the fact that he had authorized access to every system he wanted to use. There was no question of unauthorized intrusion in Len's case.

It bears a lot of repeating that Len pled guilty to unauthorized possession of Unix source code, not to computer fraud or unauthorized access.

Len's case identifies a RISK, by the way: if law enforcement is investigating you for another reason, and they don't find evidence of that crime, they'll look all over your system in the hope of finding unauthorized code (or anything else) in order to indict you.

"In that case, the charge should be extreme negligence. I don't care what your motives are; no responsible system administrator should ever store cleartext user passwords online."

Let me gently suggest that the criminal law is not the proper tool for making sure that system administrators are responsible or nonnegligent. While nonlawyers have doubtless heard the term "criminal negligence," the fact is that negligence is normally dealt with in civil law, where the proper remedy is money, not jail time.

--Mike

Mike Godwin, Electronic Frontier Foundation mnemonic@eff.org (617) 864-0665

Search RISKS using swish-e

THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

ACM Committee on Computers and Public Policy, Peter G. Neumann, moderator

Volume 11: Issue 41

Monday 8 April 1991

Contents

Bogus License Upends Life

<2206ca@gmuvax.gmu.edu>
5 Apr 91 18:29:00 EDT

The Arlington Journal [April 5-7 Weekend Edition]. Article by Geoffrey Brown.

Teresa Stover's life turned upside down after a woman walked into the Arlington County Department of Motor Vehicles office Dec. 14 and, using a fake identification card, got a duplicate driver's license with Stover's name on it. The woman promptly got charge accounts in Stover's name, according to police. Stover now has to convince creditors she isn't the woman who went on a $30,000 shopping spree.

Stover, 25, who now lives in Philadelphia, said she has spent weeks trying to clear her name. She charges the DMV gave the woman a license to steal. "As far as I'm concerned, DMV hung me. They helped her out tremendously." "It's far too easy to get a driver's license," Stover said. Stover is not the first to claim that DMV issues licences without properly checking identification.

Her story follows reports from DMV employees across Northern Virginia that they have given licenses to people with little proof of identification

because managers have told them to bend the rules rather than risk getting complaints from noisy citizens.

People from as far away as New York and New Jersey have trekked to Northern Virginia DMV offices to get licenses because it is easier to get a license here than in other states, according to court documents and reports from state and federal officials. [...] [The woman] apparently got Stover's Social Security number and other information from a bank - but how that happened Stover didn't know. [She] got a copy of Stover's driving record, and got her birthdate and home address from a DMV employee, Stover was told. [The woman] has brown eyes and black hair, while Stover is blond and blue-eyed, and that is recorded in a DMV computer. [...]

> The article goes on to discuss in general the problem of fraudulent driver's licenses:

A 2 and a half year federal investigation of corruption and fraud at the Baileys Crossroads DMV branch has revealed that perhaps thousands of illegal aliens have gotten driver's licences from corrupt DMV employees, and that DMV has done little in 2 and a half years to track the bad licenses.

A law enforcement official said the amounts employees took were small - as little as $10 for a license. [...]

> This is of some concern to me because the DMV branch mentioned in the article just happens to be the branch that I go to.
>
> There's more than one risk in this story, of course. Here are some observations:
>
> - The woman apparently had no problem getting personal information on other people from such institutions as banks and the DMV. (The article went on to say that she had 11 other Virginia licences - for different people, including one for a man!)
>
> - The woman obviously had no trouble obtaining credit from other institutions with nothing but her fraudulent driver's license. The power of a driver's license cannot be underestimated.
>
> - It's interesting to note the managers weighing risks against each other - and, of course, choosing the risk that is the least inconvenient for them (but riskier for society).
>
> - Lastly, I'm not sure what would perturb me more - if the DMV employee had refused to give the woman the license because of the discrepancy between her physical appearance and the data stored in the computer ("But the computer says...") or what really happened, with the discrepancy obviously being disregarded.
>
> -- Tony Lombardi

RISKS of unreadable mammograms

ESPEN ANDERSEN <EANDERSEN@HBS.HBS.HARVARD.EDU>
Mon, 8 Apr 1991 10:40 EST

The columnist Bella English had a story today (4/8/91) in The Boston Globe about a woman who was denied health insurance of her breasts, and therefore went uninsured.

Excerpts:

> "Apparently, the problem was that she'd had two mammograms within six months. It didn't matter that the second one was ordered because the first one was unreadable. She tried another agent, who told her that the information would be in a national data bank, and that she would face the same problem with other insurers."

She had been to other doctors, who had said that there were nothing wrong with her.

The article goes on to list other examples of a bloated health care system, "driven by special interest groups of doctors, hospitals and insurance companies."

The main RISK here, of course, lies in the inability of a human being to override the "systematic" decision (not necessarily computer programmed):

```
IF mammograms >= 2 AND time_between_mammograms < .5 year
THEN deny_insurance
ELSE grant_insurance
```

Or maybe the error lies on the input side: that inconclusive mammograms should not be included. Or in the choice of the number of mammograms as a decision parameter.

Note, however, that the "national data bank" does not necessarily constitute a risk in itself; the main problem is not (as the article seems to imply) that everybody uses the same data base; it is rather the way information from this source is used by the individual insurance companies that is a problem. Could it also be the case that this "national data bank" only gives out certain types of data - so that the insurance companies have to base their decisions on "available" data (number of mammograms) instead of the data they should use (diagnosed cancer), which might not be available?

New Zealand Strides towards Big Brother Society

<clear@cavebbs.gen.nz>
6 Apr 91 22:56:28 NZT (Sat)

Last year rumours were strenuously denied that the New Zealand Inland Revenue Department (controlling taxation) and the Social Welfare Department (controlling benefit entitlement and payouts) would link databases to provide powerful searching and data matching facilities for staff. The government of the time, Labour, also proposed to introduce a national identity card scheme.

Both schemes were thought to have been abandoned when Labour lost the October 1990 election. Not so. I leave it to readers of RISKS Digest to draw your own conclusions from the following:

New Zealand Computerworld, 1 April 1991.
Randall Jackson of IDG's Wellington office confirmed this is NOT a hoax.

PM'S TEAM GETS SET TO MOVE ON ID CARDS
by Clive Mathew-Wilson

The Government plans to introduce a National Identity Number scheme for all New Zealanders by the end of next year, Computerworld sources say.

The numbering system is likely to involve the use of a "smart" ID card.

A team working on the project with the Prime Minister's office has yet to announce its findings to Parliament, but it is understood it is the format of the ID scheme, not the scheme itself, that is being debated.

Usually reliable sources within Parliament suggest the ID scheme - originally proposed by the International Monetary Fund - was already part of Treasury's economic reform plans before the election, and that it is being implemented virtually without change by the new Government.

The first stage of implementation - data sharing between the Social Welfare department and the IRD - is expected to take place shortly.

It is understood that in place of any new common identity numbering scheme, the issuing and control of IRD numbers will be tightened, and an IRD number used in all relevant transactions throughout various government departments.

More than 1.7 million IRD numbers are currently allocated to wage and salary earners, and recent changes to tax laws require every bank account to be tagged with an IRD number by 1992.

This would, in effect, give every New Zealander a unique, computerised serial number.

It is believed the only real problems facing the ID card scheme are those of computer power.

Doubts have been raised over the ability of existing systems to cope with the information-handling and storage needs of a National ID Card.

The most likely scenario at present, entails a gradual phasing-in of both the card and the information-matching based around it, starting with data-matching between the huge Social Welfare and IRD computer systems, which operate out of the same GCS [Government Computing Service] installation at Trentham.

One key target of the ID card is understood to be the public health system. The computerised "smart" card, with its instant reference to a person's income details, is to be used to target healthcare as the public health system is wound down.

If Computerworld's source is correct, a number of politicians and civil servants appear to have been economical with the truth.

Prime Minister Jim Bolger, while he was in opposition, undertook not to introduce a common identification number system, despite a confirmation by the IRD at the time that the IRD number was, in fact, such a system already.

Similarly, shortly before the elections last year Inland Revenue Commissioner Dave Henry denied the IRD had plans to link its computer systems with those of Customs, Births, Deaths and Marriages, Social Welfare, Housing Corporation and ACC. Shortly after the election, plans

to link the Social Welfare and IRD computers were announced.
The Australian Government, which failed dismally in its plans to launch a national ID card, is understood to be watching the New Zealand experiment with interest, pending a possible re-introduction of the scheme in Australia in a somewhat different form.
Civil liberties spokesperson Barry Wilson attacks what he terms a "conspiracy of silence" over the issue.
"When has there been any informed public debate over whether New Zealanders need or want ID cards? The public, by and large, has been completely ignored," he says.
"New Zealanders voted against the ID card scheme when they dumped Labour."
Computerworld sought ministerial and IRD response on the issues, but neither had answered our calls by press time.

Rapid dissemination of half-truths, lies, and disinformation

"Jonathan E. Oberg" <PH461A04@VAX1.UMKC.EDU>
Fri, 5 Apr 91 20:22 CST

The following posting recently appeared in several newsgroups and forums:

>Subject: MODEM TAX
>A new regulation that the FCC is quietly working on will directly
>affect you as the user of a computer and modem. The FCC proposes
>that users of modems should pay extra charges for use of the public
>telephone network which carry their data. In addition, computer
>network services such as Compu Serv, Tymnet, & Telenet would also
>be charged as much as $6.00 per hour per user for use of the public
>telephone network. ...

Almost immediately after its posting, dozens of responses were posted claiming this was a hoax/fable/etc that was posted on a regular basis to the net. Having never seen the posting, nor having seen any reports on other media regarding this, I can not speak to whether it is accurate or not.

However, I am concerned with the way the network:
a) allows for the rapid propagation of inaccurate, misleading and bogus information

and more especially:
b) the desensitization that the net can inflict.

By the latter I intend the following. Let us suppose that this message was indeed posted on a regular basis and is known to be false. As soon as it is posted again, it is immediately flamed down as bogus. Now further suppose that what the message claims *comes to pass!* How would this information be disseminated?? Any postings to the net would be shot down, and/or ignored. The sheer volume of information passing through daily makes scanning information and discarding junk messages not only prudent by necessary. How many users' mail programs out there are already customized to scan and ignore messages containing "modem tax" in the subject line?? Certainly the *users* have become

programmed to do just that.

Knowing this, and presuming that the typical users ar both literate, informed, and sources of some authority on their local systems, one can easily propose the situation where a group floods the net with bogus information regarding a risk (say, a security hole found in ftp protocol) that doesn't exist, and "re-flooding" the net with a similar posting on a semi-regular basis. When the net becomes desensitized to that information, that group than exploits the (formally bogus) information [in our example a security hole in ftp protocol]. Even were it discovered that someone was exploiting this security hole, how would information of this discovery be communicated?? Would not the knowledgeable, net-literate at each site be likely to convince those responsible that this was just another hoax??

This is less a computer/risk as a societal/risk carried on computers, so apologies to uninterested risk readers.

Jonathan ph461a04@vax1.umkc.edu

Re: Another computer time/date processing problem

Andy Goldstein - VMS Development <goldstein@enet.src.dec.com>
Fri, 5 Apr 91 14:40:17 -0800

You're right in questioning the 366 day uptime value in your VMS SHOW SYSTEM display (although we know of VMS systems that have stayed up that long!) The cause of the problem is that SHOW SYSTEM does not compensate for changes made to the system time since the system was booted. The system time is saved as an absolute value when the system is booted; uptime is computed simply by subtracting the boot time from the current time. Thus, the likely cause of your 366 day uptime is having the system time set ahead one year after the system was booted.

The fact that this happened to you right after the new year suggests you may have been bit by the foibles of VMS time keeping. (Then again, it may also be that the system had been booted with the time set back a year and then corrected right after the boot.) Depending on the circumstances, you are likely to be prompted for the time the first time you boot after the new year. That's also a likely time for you to type in last year. (It take me well into February before I stop writing last year on my checks.)

The attached article, already sent to many customers, explains the foibles of VMS timekeeping.

==========

You have run into one of several problems associated with how the time and date are maintained in VAX/VMS. We must first present some background.

VAX VMS makes use of several clocks, some in hardware and some in software, to keep track of the date and time. Because none of the available clocks solves all the problems of time keeping, they must be used in concert and be

maintained in synch by the operating system. Under some circumstances, they may get out of synch, causing obscure and sometimes incomprehensible problems with the system date and time.

The "master" clock is maintained as a software construct by VAX VMS. It is a cell in the exec that contains the current date and time in the VMS quadword time format. This value represents the time elapsed since 17-Nov-1858 in tenths of microseconds. With this precision, the 64 bit signed value has a range of approximately 29,000 years; VMS development has not developed a plan for what to do when it overflows.

Most VAX cpus provide two hardware clocks from which the VMS master clock is derived. The interval timer is used to provide an interrupt every 10 milliseconds. At each interrupt, the quadword master clock is incremented by the value 100,000, and time-dependent scheduling activities are initiated.

A "time of year" clock is build into the console subsystem of most VAX cpus. This clock is a 32 bit counter that is incremented every 10 milliseconds, whether the cpu is running or not, and, if battery backup is available, whether power is on or not. Every time VMS is booted, the software master clock is set from the time of year (aptly named TOY) clock. This is where the trouble starts. The 32 bit, 100HZ counter has a capacity of 497 days, and therefore cannot be used by itself to represent time over an indefinite period. This 5 cent optimization has caused VMS engineering more grief than any other feature of the VAX architecture.

VMS uses the TOY clock to maintain the date and time relative to the current year, and stores the current year on the system disk in the system image file SYS.EXE. This value is updated whenever the system time is recalibrated (when the system is booted or when any SET TIME command is entered). What is saved in the system image is the quadword master clock value and the TOY clock value that corresponds to it in the current year. To recalibrate the time, the TOY clock is read and a delta is computed from the saved TOY clock value. This delta is converted into quadword time units and is added to the saved quadword time to yield the new current master clock value. If the TOY clock is found to have more than a year of time accumulated on it, one year's worth of time is subtracted out and the new value is set in the TOY clock. Finally, the new TOY clock and master clock values are saved in the system image.

VMS adds a bias of 2**28 (31 days) to the time since January 1 to compute the value maintained in the TOY clock. Thus, should the TOY clock be reset or overflow, the value read will likely be less than the bias and will be rejected as an invalid clock value. Also, if the value read from the TOY clock is a day or more earlier than the saved value, it is rejected as invalid. Because of the bias, the TOY clock overflows 100 or 101 days after the first of the new year (depending on whether the previous year was a leap year or not). Thus, provided the system is rebooted or a SET TIME command is performed some time between January 1 and April 11 of each year, the TOY clock and system time will be correctly maintained indefinitely.

Problems arise when more than one copy of VMS is run on the same machine (for example, one's normal system and stand-alone BACKUP), and when new copies of the VMS exec are booted for the first time. For example, if two different copies of VMS are used at different times on the same machine, only one system

will be presented with the opportunity to reset the TOY clock when it is first booted after January 1. The other system, when subsequently booted, will find that the TOY clock has a much smaller value than its saved value (from the last boot), and will reject the time as invalid, causing it to prompt for a new date and time.

When a new VMS system is distributed, it has assembled into it a quadword time and saved TOY clock value that represent January 1 of the current year. For example, VMS V5.3 was completed in October of 1989; therefore its internal time as distributed is based in 1989. Should a new copy of a system image be booted in a subsequent year, the TOY clock will be evaluated against the base date assembled into the system, and it will come up with the date set to approximately the current day in the year 1989. This will happen, for example, with the stand-alone BACKUP kit distributed with VMS magtape kits. The problem with stand-alone BACKUP is particularly bothersome because its system time is never updated when it is booted (because the disk it is being booted from is either write-locked or SYS.EXE is no longer present because the first floppy or TU58 has been removed).

Andy Goldstein, VMS Development

Search RISKS using swish-e

THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

ACM Committee on Computers and Public Policy, Peter G. Neumann, moderator

Volume 11: Issue 42

Monday 8 April 1991

Contents

Now the police can find you anywhere in town!

<ADEN@vf.jsc.nasa.gov>
Sun, 7 Apr 1991 21:41:40 CDT

On David Horowitz' consumer advocate show _FIGHT_BACK_ this Saturday, they "previewed" a product that's in the prototype stage called (something to the effect of) TELETRACE. This product is an antitheft device for your car. You will pay something on the order of $600 initially, then a modest monthly fee, and your car, with the TELETRACE device, can be traced anywhere in the zone of control of your police department. Polling sites are set up around the

perimeter of your city police's area of control, and these sites will receive transmissions from your car. By monitoring strength and angle of the signal (their claim, not mine), they can "pinpoint" your car.

The idea, of course, is that if your car in stolen, the police can find it. But there's an added "feature" ... you don't have to call the police to tell them it's stolen ... the car can be armed so that as soon as it's broken into, the police start to monitor it. Nifty, huh.

I suppose the readers of RISKS can spot the problems here ... from Big Brother complexes to inadvertant arrest when you steal your own car :-). Personally, I found it all terribly amusing, but I wouldn't buy it.

S. Spenser Aden -- Lockheed Engineering and Sciences Co. -- (713) 483-2028
NASA -- Johnson Space Center, Houston -- Flight Data and Evaluation Office

---

Re: Automatic Vehicle Identification (Ravin, driving and privacy)

Brinton Cooper <abc@BRL.MIL>
Sun, 7 Apr 91 20:54:00 EDT

Risky computer practices seem to be accelerating faster than sane people can react to them. However, this one seems to be on the wrong track. Cars don't get speeding tickets; people get speeding tickets. In Maryland, a speeding ticket is actually a summons to District Court sitting as Traffic Court. Such a citation would most likely be issued, if at all, to the owner of the vehicle. This being a non-civil case, however, the State bears the burden of proving that the owner was actually driving the vehicle. The owner need not testify in her/his own behalf! While this is likely to be a nuisance for the first few victims, no sane court is likely to uphold the charge.

It seems that our Risks discussions speak to two communities: we speak to one another as computer professionals and we speak to the public at large. In the former case, we ponder the correct and proper use of computers. In the latter, we'll increasingly have to invoke the tools of jurisprudence to overcome improper use.

_Brint

UPS to collect electronic signatures?

"Dwight D. McKay" <mckay@ecn.purdue.edu>
Fri, 5 Apr 1991 14:32:35 -0500 (EST)

Having just received a delivery, I am reminded of a small article in last week's Wall Street Journal. It described a new computer system United Parcel Service will be introducing which has some serious risks associated with it.

UPS plans to field a large number of the new pen-based computers as replacements for the ubiquitous UPS clipboard. When you receive a package you'll sign for it on the pen-based computer. Each evening the delivery person will drop off his "pad" which will upload the days signatures to UPS's computer

network. With in a matter of a few weeks they could have a sizable percentage of population's signatures in digital form.

Does anyone know more about this system? What sort of controls will they have in place for securing the collected signatures?

--Dwight D. McKay, Purdue University, Engineering Computer Network
(317) 494-3561 ...rutgers!pur-ee!mckay

Software fault in aircraft navigation systems

<smb@ulysses.att.com>
Mon, 08 Apr 91 20:14:43 EDT

The FAA has informed airlines that aircraft equipped with certain models of the ``Honeywell Flight Management System 1 million word database'' may fall prey to software problems. Apparently, one of the navigation systems -- the non-directional beacon landing approach system -- is buggy and can display the wrong course. Planes affected include the 747-400, the 757, the 767, and the MD-11.

Navigation system software is updated monthly; future release will omit that code until the FAA approves a bug fix.

--Steve Bellovin

Smiths Industries 737-400 LCD display

Robert Dorsett <rdd@cactus.org>
Sun, 7 Apr 91 17:29:59 CDT

RISKS readers may recall some concerns over the Smiths Industries LCD-based engine instrumentation, which was introduced on the Boeing 737-400 in 1988 (advertisements appeared in Aviation Week through 1989). This is essentially a very low-resolution engine instrumentation scheme, utilizing a series of LCD's, in a circular layout, as trend indicators, with a digital readout. It is now offered as a retrofit package for the 737-300, and is available as an option on the 737-300, -400, and -500. It replaces the electromechanical "clock" displays, which have been in use since 1969. The Smiths Industries display interface is fundamentally different from those used on the 747-200 and -300 (electromechanical dials or tapes), the 757/767 (CRT-based "moon" displays), and the 747-400 (CRT "tapes").

Following the crash of a 737-400 at Kegworth, two years ago, the British Air Accidents Investigation Branch initiated a fairly exhaustive survey of the human factors of the cockpit (which seemed warranted, since the pilots had apparently shut down the wrong engine, following an engine emergency).

Here's an interesting (i.e., supports my position :-)) article from a recent FLIGHT INTERNATIONAL, March 6, 1991. Note that many of the issues raised have been discussed on the net, and have appeared in numerous reports in real life, yet no action ever seems to be taken...

UK AAIB SLAMS 737-400 DISPLAYS, by David Learmount.

"Tests have revealed that the layout and type of engine instruments on board the British Midland Boeing 737-400 which crashed at Kegworth in 1989 were the worst possible combination by a considerable margin, says Ken Smart, chief investigator of the UK Department of Transport's Air Accidents Investigation Branch (AAIB).

"The liquid-crystal displays and their layout were cited as factors in the 737 crew shutting down teh wrong engine. The findings follow UK laboratory tests, Smart otld a UK Parliamentary Advisory Council for Transport Safety meeting in London on 26 February.

"AAIB accident investigator Ed Trimble, concerned that there are no national or international standards for testing instrument effectiveness before operation, saked why tests had not been carried out before--his questions prompted Boeing to admit that it has still not modified either the layout or display type in its 737-400's. Some airlines have reverted to electromechanical instruments in new 737's.

"Smart points out that the British and US armies have a program called 'Manprint' to test the user-friendliness and operational efficiency of equipment design choices. He says: 'It is long overdue that the position of the crew in the system should be considered. It is inevitable that its role, if things keep going the way they are, will be reduced purely to that of monitor, a role in which man is not effective.'

"International speakers at the conference claimed that 'glass cockpit' design induces errors as a result of being insufficiently tested before going into service--eventually resulting in a serious accident.

"Airlinr manufacturers, accident investigators, human-factors specialists and airline pilots believe unanimously that today's automated cockpits, which present the pilot with huge quantities of information on 'untested' displays, are not designed to keep the pilot 'in the control loop.' Future avionics and cockpit designs must bring the pilot back into the loop, says Boeing's chief flightdeck engineer, Del Fadden, making clear that [text omitted in original--another RISK of electronic publishing systems :-)] intends to do this.

"The US National Transportation Safety Board's (NTSB) chief accident investigator Robert MacIntosh told the 'Pilot error in perspective' conference that although '...glass cockpit aircraft have been remarkably accident-free ... the NTSB is trying to anticipate what kind of accidents there might be [in them].'

"Smart revealed that the results of a major line-pilot opinion survey 'Human factors on the advanced flightdeck'--to be presented by the Confidential Human Factors Incident Report Programme, showed that pilots are seriously concerned at the degradation of flying skills automation causes." (sic)

Robert Dorsett UUCP: ...cs.utexas.edu!peyote.cactus.org!rdd

UPC Hiccup and human error

Wayne Gibson <wgibson@capstan.convex.com>
Sat, 6 Apr 91 12:44:26 -0600

I was at the grocery store and spotted 12-pack coke in cans for $2.50. Being a programmer I could not pass this up and got 4 12-packs. At the checkout counter (UPC scanner) the girl took the first 12-pack and ran it over the scanner 4 times. With everything else included the total was $75.68. Since I had a couple of prescription medicines I thought this was high but not rediculus. So after paying she hands me the receipt and the first four lines look like this:

BBS	DIET COKE 12	25.00
BBS	DIET COKE 12	2.50
BBS	DIET COKE 12	2.50
BBS	DIET COKE 12	2.50

Now remember she used the exact same carton all four times!! I point out that this doesn't look right. She agrees but since I've already paid she's powerless to do anything about it; I need to go to the service desk. OK, fine. It's right there ten steps away. I have this awful headache and just want to get home and take my prescriptions, so I'm not paying close attention. Well, the "assistant manager" working at the service desk goes, "Oh, that's terrible. Here let me get you a refund. Let's see... 25.00 minus 2.50. I owe you $23.50 plus tax." With my headache I didn't even notice until I got home.

She can't add and subtract. But she also showed no concern that the UPC system might do this again. When I brought this up she just said that she hadn't seen it before a was sure it was just a "glitch".

-- Wayne

[I have been generally not too enthusiastic about including the scads of incremental-experiential sagas that are currently pending consideration in the RISKS queueueueueueueue, but this one slips through... PGN]

Re: E-mail role in LA cop probe (PGN, RISKS-11.37)

<henry@zoo.toronto.edu>
Sat, 6 Apr 91 22:02:21 EST

> ... essentially any message can be spoofed, tampered with, or destroyed
> altogether, given suitable system access...

The same is true, of course, of recorded voice. Again, the analogy seems good, and the decision to accord the same status a sensible one.

Henry Spencer at U of Toronto Zoology utzoo!henry

Re: Computer Ballot Tally (Richard Wexelblat, RISKS-11.38)

"B.J. 08-Apr-1991 1625" <herbison@ultra.enet.dec.com>
Mon, 8 Apr 91 14:28:08 PDT

> Question: is this felt to be a reasonable method?

I don't feel the method is reasonable. It *might* have been reasonable before you published it, but now that you have provided the information needed to cook the vote and avoid detection--just modify the electronic vote counter so it is accurate until the ballot count is larger than 2% of the expected returns and does anything it wants after that point.

B.J.

A `security device' that isn't.

<ark@research.att.com>
Mon, 8 Apr 91 20:20:38 EDT

I received a catalog in the mail recently that among other things advertised a device to `stop people from making expensive 900 calls from your phone.' It consisted of a little box with a lock that clamps onto the back of the phone. As far as I can tell from the picture in the catalog, it has a modular jack in it, into which you plug the cord coming from the wall. It also has about a 2-inch cable coming out of it with a modular plug at the end, which you plug into the telepone.

I wonder how many people will order these things, not realizing that they can be defeated in about two seconds? For that matter, I wonder how hard it is to pick the lock?

--Andrew Koenig ark@europa.att.com

Re: Computer Ballot Tally (Richard Wexelblat, RISKS-11.38)

<erikn@tekcae.cax.tek.com>
08 Apr 91 17:12:04 PDT (Mon)

> is this felt to be a reasonable method?

Controls on a vote counting system, like controls on any system, can be reasonable only in relation to the types of threats that are bring controlled against.

Broadly, for vote counting, there are two threats:
- someone fixes the election (fraud)
- something goes inadvertently wrong (error)

In each case, the reported results won't match the true results.

Terminology:

results: the number of votes each candidate and measure received
outcome: who won, which measures passed and which failed.
reported: what the counting system claims happened
true: what each voter intended to do

The probability that the reported results will perfectly match the true results will never be 100%. The probability that the reported outcome will match the true outcome must be very high, even if the race is arbitrarily close.

Back to the question. If the ballots have already been mailed, it's too late to do much about fraud. For next time, a few issues you might want to think about for both fraud and error are:

- how is ballot stock controlled? Are ballots numbered? Are secrecy envelopes numbered? How are both secrecy and security maintained?
- how is the mailing list maintained? Are you sure that everyone one the mailing list had a ballot mailed to their address of record? Who has access to the official mailing list? How many days before the election must a member join to be eligible to vote? Is this the day you take your pull from the mailing list?
- is the ballot designed in such a way that all voters will be reasonably able to follow the instructions and vote their choice, with equipment they will have at the address the ballot is mailed to? Don't laugh, I'm not sure that this is true for all U.S. elections. It sounds like you're using some sort of markable form. If it's a form where you have to punch little squares out, I'm not sure the manufacturer recommends those for mail voting. If it's a form where you mark a square, what kind of pencil or pen are you assuming your voter has?

It's best to think out the whole process IN DETAIL before you even send out the ballots. Perhaps you have, but I can't tell from your posting. I have a few questions:

> Before the Validators get there, the company has opened any ballots with

How are the validators chosen and trained? Who is "the company"? What are they doing with your ballots? Why are they doing anything with them while you aren't there? Remember, security is trust with a paper trail.

> Any that fail are put aside.

For what reasons would a ballot be failed? Someone intended to vote with that ballot, it is your responsibility to count it, if it can be done so unambiguously, even if a particular piece of hardware can't deal with it.

BTW, you need to count the ballots that failed, too. In a mail election, it is difficult to account for every ballot, but you need to get reasonably close. Call a random sample of the people you sent ballots to, but didn't get one from, to see if they actually got their ballot. Just an idea.

A few more comments:

> We then select at random about 1% of the "passed" group and tally them

This is too low, and shouldn't be a constant. There are formulas for calculating how many ballots you need to recount, to reach a certain confidence that no undetected fraud or error of certain types has been reached. I can dig some of them out, if you're interested, but all of them share the property that, as a race approaches a dead heat, the percentage of ballots you need to recount approaches 100%.

> (No machine discrepancy has yet been discovered; don't know what to do if one
> occurs)

Either you haven't counted many ballots, the errors aren't being caught, or you aren't hearing about the errors that are caught. The ballot counting systems I've seen out there just aren't that reliable. A big number of "failed" ballots is a good sign that your system is flakey.

For machine count systems, a failed ballot usually means that the ballot is marginal in some way. Maybe it's dirty, or a mark is outside a line, or the ballot was cut slightly narrow. Maybe there was a power glitch while the ballot was read. In this last case, the failure has nothing to do with the ballot, so I'm sure this is what you'd call a "machine discrepancy." For failures that do have something to do with the ballot, they all exhibit a transition zone, so that a ballot that is a little dirty will read OK 40% of the time, and fail 60% of the time. A little dirtier, and it reads bad 80% of the time. So machine discrepancies are inevitable, and fairly common. However, machine discrepancies aren't the voter's problem, your duty is to determine voter intent if it is possible to do so.

I can see problems with your recount method, because it doesn't verify anything except that the reader is working OK while you happen to be doing the recount. You might argue that you are validating the software that does the counting, but only for the volume of cards in the recount, only if you are sure the program hasn't changed since the count, and only if you aren't worried about fraud. You don't know if the counters were zero when the count started. You don't know whether ballots were intentionally or inadvertently counted twice, or not at all,

The preferred method is to subdivide the ballots into groups, called precincts, then count each precinct separately, and sum the subtotals. Each group needs an anonymous, yet deterministic method of group assignment, such as a number on the ballot. You might want to think about zipcodes. As I recall, your recount work is minimized if all groups are approximately the same size, and the number of groups is about the square root of the number of ballots. It depends on how expensive each operation is, some people believe that there is never a reason to have more than about 1000 precincts.

If an election is worth something, someone may try to steal it. It it isn't worth anything, someone may not take it seriously enough to count it correctly.

> We then open all unsigned ballots. If a signature inside, manually add

Why can the voter sign one of two places? Why wasn't this designed out?

We could get into vote counting software issues, but that's another huge area.

Your responsibility is to not only correctly count the election, but to be able to demonstrate that you counted the election correctly. This requires careful documentation at each step of the process, and opens up another huge area that I won't get into.

Conducting a trustably accurate election is difficult. Ask yourself how much accuracy you need, then design a system to give you that accuracy for a reasonable amount of money. For elections that matter at all, the accuracy needs to be pretty high. For small elections, say only a few thousand ballots, it is often cheaper to get an accurate count by hand.

Erik Nilsson, CPSR Vote-Counting Project Leader
erikn@tekcae.cax.tek.com (503)690-8350 690-9292[fax]

Re: Tricky application of Caller ID (Johnson, RISKS-11.38)

Randall Davis <davis@ai.mit.edu>
Fri, 5 Apr 91 14:50:40 est

> Does anyone have any documentation on this supposedly-true story?

Consider the scenario for a moment and imagine, say, 10,000 kids in the audience actually do what they're told. You've got 10,000 phones dialing the same number simultaneously. How many of those calls do you think will actually get through?

Sounds like a typical urban legend and a very ineffective way to get a sizable mailing list. They'd be much better off with the coupon in the paper trick.

I strongly suspect that what Gary said was of the form ``What if...,'' and it's now being repeated as ``He said that...'' I tried calling him here at MIT to find out more, but his answering machine says he's in Belgium for the year.

[Lots of other folks commented on this one also, including Jerry Hollombe. PGN]

Search RISKS using swish-e

THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

ACM Committee on Computers and Public Policy, Peter G. Neumann, moderator

Volume 11: Issue 43

Wednesday 10 April 1991

Contents

U.S. Senate S. 266

<WHMurray@DOCKMASTER.NCSC.MIL>
Wed, 10 Apr 91 17:23 EDT

Senate 266 introduced by Mr. Biden (for himself and Mr. DeConcini)
contains the following section:

SEC. 2201. COOPERATION OF TELECOMMUNICATIONS PROVIDERS WITH LAW ENFORCEMENT

It is the sense of Congress that providers of electronic communications services and manufacturers of electronic communications service equipment shall ensure that communications systems permit the government to obtain the plain text contents of voice, data, and other communications when appropriately authorized by law.

U.S. Senate 266, Section 2201 (cryptographics)

<WHMurray@DOCKMASTER.NCSC.MIL>
Wed, 10 Apr 91 18:20 EDT

The referenced language requires that manufacturers build trap-doors into all cryptographic equipment and that providers of cconfidential channels reserve to themselves, their agents, and assigns the ability to read all traffic.

Are there readers of this list that believe that it is possible for manufacturers of crypto gear to include such a mechanism and also to reserve its use to those "appropriately authorized by law" to employ it?

Are there readers of this list who believe that providers of electronic communications services can reserve to themselves the ability to read all the traffic and still keep the traffic "confidential" in any meaningful sense?

Is there anybody out there who would buy crypto gear or confidential services from vendors who were subject to such a law?

David Kahn asserts that the sovereign always attempts to reserve the use of cryptography to himself. Nonetheless, if this language were to be enacted into law, it would represent a major departure. An earlier Senate went to great pains to assure itself that there were no trapdoors in the DES. Mr. Biden and Mr. DeConcini want to mandate them. The historical justification of such reservation has been "national security;" just when that justification begins to wane, Mr. Biden wants to use "law enforcement." Both justifications rest upon appeals to fear.

In the United States the people, not the Congress, are sovereign; it should not be illegal for the people to have access tto communications that the government cannot read. We should be free from unreasonable search and seizure; we should be free from self-incrimination. The government already has powerful tools of investigation at its disposal; it has demonstrated precious little restraint in their use.

Any assertion that all use of any such trap-doors would be only "when appropriately authorized by law" is absurd on its face. It is not humanly possible to construct a mechanism that could meet that requirement; any such mechanism would be subject to abuse.

I suggest that you begin to stock up on crypto gear while you can still get it. Watch the progress of this law carefully. Begin to identify vendors across the pond.

William Hugh Murray, Executive Consultant, Information System Security 21 Locust Avenue, Suite 2D, New Canaan, Connecticut 06840 203 966 4769

The price of quality

"David G. Novick" <novick@cse.ogi.edu>
Wed, 10 Apr 91 14:53:01 -0700

I noticed an interesting column by Joshua J. Kaufman on computers for lawyers in the March/April edition of The Washington Lawyer, the official journal of the District of Columbia Bar. The column began:

> On Second Thought
>
> "What do you expect from a $69 program?" were the last words said to me by the technical department at Isogon Corporation. The comment was made after its product NewSpace, a data compression utility (which I have reviewed favorably in the past), managed to destroy 1,400 files and 42 megabytes of my data. I spent over an hour on the phone with technicians trying to find a way to correct the problem--all to no avail.

What happened to Kaufman is that he had been using NewSpace successfully to compress files on his hard disk. One night he started up the program, left work, and came back in the morning to discover that his computer had "frozen." When he rebooted, the "file allocation table" was damaged in a way that could not be recovered. Thus while his files were almost all fine, he could not retrieve them, despite the fact that he could list the files in his directory.

The RISKS I see here are (1) relying on reviewers of software who use a product casually but who do not systematically test, and (2) producing software that can, without prior notice, leave your system in an unrecoverable state. For $69, perhaps Kaufman was entitled to a product that, even though possibly buggy, would be designed to fail safely.

David G. Novick, Department of Computer Science and Engineering, Oregon Graduate Institute of Science and Technology, Beaverton, OR 97006-1999

Some data on Len Rose

Jerry Leichter <leichter@lrw.com>
Mon, 8 Apr 91 22:29:15 EDT

With all the verbiage about whether Len Rose was a "hacker" and why he did what he in fact did, everyone has had to work on ASSUMPTIONS. Well, it turns out there's now some data: A press release from the US Attorney in Chicago, posted to the Computer Underground Digest by Gene Spafford. I've extracted one interesting portion concerning the famous "modified login.c" program:

> In pleading guilty to the Chicago charges, Rose acknowledged that when

> he distributed his trojan horse program to others he inserted several warnings so that the potential users would be alerted to the fact that they were in posession of proprietary AT&T information. In the text of the program Rose advised that the source code originally came from AT&T "so it's definitely not something you wish to get caught with." and "Warning: This is AT&T proprietary source code. DO NOT get caught with it." The text of the trojan horse program also stated:
>
> > Hacked by Terminus to enable stealing passwords.
> > This is obviously not a tool to be used for initial
> > system penetration, but instead will allow you to
> > collect passwords and accounts once it's been
> > installed. (I)deal for situations where you have a
> > one-shot opportunity for super user privileges..
> > This source code is not public domain..(so don't get
> > caught with it).
>
> Rose admitted that "Terminus" was a name used by him in communications with other computer users.

I can't imagine a clearer statement of an active interest in breaking into systems, along with a reasonable explanation of how and when such code could be effective. (BTW, back in the early 70's, some friends of mine and I discovered that a newly-installed APL system still had no password, or a standard password, set on its operator account. Because we had quick access to some code that would let us to "trap" the resulting privileges, we were able to continue to play God on that system for years - although the operator password was changed within a day or two. "One-shot opportunities" DO occur.)

The only thing that will convince me, after reading this, that Rose was NOT an active system breaker is a believable claim that either (a) this text was not quoted correctly from the modified login.c source; or (b) Rose didn't write the text, but was essentially forced by the admitted duress of his situation to acknowledge it as his own.

-- Jerry

"LIVING AGAINST THE ODDS" abuses statistics (what else is new)

Jeremy Grodberg <jgro@lia.com>
Mon, 8 Apr 91 13:30:50 PDT

The PBS Special "Living Against the Odds" showed some signs of statistics abuse which were especially annoying for a special which is supposed to enlighten the masses about this kind of thing. It is bad enought that this king of abuse is the foundation of much of our current public policy debates, but to see it emphasized like this: isn't there anything we can do?

2 examples:

The statistic they used to judge the risk of an activity was deaths per 100,000 participants. In other words, they said that 20 out of 100,000 people who climb rocks die while climbing rocks, and 20 out of 100,000

people who drive cars die while driving cars, so the two activities are equally dangerous. This conclusion does not follow, for it does not take into account the very likely possibility that people who climb rocks spend a significantly different amount of time climbing rocks than people who drive cars spend driving cars, over the course of a lifetime. If the average rock climber spends 1,000 hours of his life climbing rocks, and the average driver spends 10,000 hours driving, then the mortality statistics suggest that rock climbing is 10 times as dangerous.

One of the "experts" was shown saying (I quote from memory) "80% of people surveyed think they are safer than average drivers. Obviously this can't be true." Unfortunately for the expert, it can be true, and it wouldn't surprise me if it *were* true. For a very simple example, take the case where 80% of the people have exactly 1 accident every 2 years, and 20% of the people have exactly 2 accidents every 2 years. The "average" driver therefore has 0.6 accidents per year, and 80% of the drivers are better than average, since they only have 0.5 accidents per year.

How can we survive as a democracy in a technological age when even the experts can't understand the complexities of the data they are evaluating?

Jeremy Grodberg

Re: Rapid dissemination of half-truths, lies, disinformation (11.41)

Robert E. Van Cleef <vancleef@garg.nas.nasa.gov>
Tue, 9 Apr 91 09:48:42 -0700

Accepting the statements of "those who should know" without question is an old problem. If my memory serves, one of the reasons given for the success of the Communist Revolution in China was a belief on the part of the Chinese population that written statements were "Truth"; leading them to believe the propoganda posters without question.

I have seen the same factor at play with individuals who believe everything they read in the paper, or hear on a TV news programs, or learn from their friend, neighbor, or pastor. The FCC has been repeatedly hit by unfounded petition drives of various sorts. Most of these problems have been well documented as Urban Legends.

The computer related risk, like always, is in the speed and ease of propagation. It is too easy to mail a copy of this "important" message to hundreds of people, where it can sit in someone's mailbox until they decide to pass it on.

There are two things that we can do as individuals:

1) Establish and use clearing houses for sensitive information.

   Having the CERT validate and announce security problems will help prevent the problem of people ignoring a security bug in ftp because of too many previous false messages.

2) Identify your sources:

> If all you have is hearsay, note it as such! If you have a reference, list it. One of the most valuable features of the RISKS digest is the fact that most of the posters identify the sources of their information.

As long as people believe what they want to believe, be it the National Enquirerer or alt.rumors, this will be a problem.

Bob Van Cleef, NASA Ames Research Center (415) 604-4366 vancleef@nas.nasa.gov

---

Re: Bogus License Upends Life

Steve Elias <eli@cisco.com>
Tue, 09 Apr 91 10:43:47 MDT

I'd like to point out that the woman who had her life upended by someone stealing her identity probably would have been able to avoid this problem if she had been a member of TRW Credentials service. Many of you usenet-folk love to slam this TRW service, but in a case like this woman's, it may have saved her all that trouble.

/eli

Re: Computer Ballot Tally

<erikn@tekcae.cax.tek.com>
09 Apr 91 10:42:24 PDT (Tue)

Oops, I forgot an important point. A big advantage of precincts is that you pick precincts to recount at random, then verify the recount numbers against the original counts for that precinct. If you start seeing discrepancies, then you need to recount everything. Then, the recount actually tells you something about the original count.

I also didn't say anything about pre- and post-election testing of the system, yet another BIG AREA.

- Erik

erikn@tekcae.cax.tek.com (503)690-8350 690-9292[fax]

Security does not come through obscurity (B.J. Herbison, RISKS-11.42)

<wex@PWS.BULL.COM>
Tue, 9 Apr 91 17:29:12 edt

Herbison takes Richard Wexelblat to task for asking if a ballot-verification method is secure by stating:

> [The method] *might* have been reasonable before you published it, but now
> that you have provided the information needed to cook the vote and avoid
> detection--just modify the electronic vote counter so it is accurate until
> the ballot count is larger than 2% of the expected returns and does
> anything it wants after that point.

This argument is fallacious on two counts. One, it assumes that if Richard hadn't publicised the verification method, no one with ill intent would have known it. Any system security manager can tell you that those with ill intent are often the best-informed on system vulnerabilities. Security through obscurity just doesn't work.

Two, it implicitly assumes that someone could be in a position to "modify the electronic vote counter" and yet not know the verification method. Highly unlikely, I'd say.

[For the record, Richard Wexelblat is my father. That doesn't make Herbison's argument any less unreasonable.]

--Alan Wexelblat, Bull Worldwide Information Systems, phone: (508)294-7485

Re: Tricky application of Caller ID (Davis, RISKS-11.42)

Bill Woodcock <woody@ucscb.UCSC.EDU>
Mon, 8 Apr 91 20:39:56 -0700

> Consider the scenario for a moment and imagine, say, 10,000 kids in the
> audience actually do what they're told. You've got 10,000 phones dialing the
> same number simultaneously. How many of those calls do you think will
> actually get through?

In answer to your question, all 10,000 of them will get through. Sprint has a service called "Mass Event 900/800" for doing exactly this. It can handle, coincidentally, 10,000 calls simultaneously, and is offered to all their larger 800 and 900 customers. I've heard, but not been able to substantiate, that AT&T has a similar service.

-Bill Woodcock, BMUG NetAdmin

Search RISKS using swish-e

THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

ACM Committee on Computers and Public Policy, Peter G. Neumann, moderator

Volume 11: Issue 44

Thursday 11 April 1991

Contents

---

re: U.S. Senate 266, Section 2201 (cryptographics)

Jerry Leichter <leichter@lrw.com>
Thu, 11 Apr 91 09:32:49 EDT

In a recent RISKS, Bill Murray comments on this "sense of the Senate" that would require providers of information transfer equipment and services to ensure that the government, as authorized by law, could obtain clear-text copies of any messages sent. Murray comments that that this would require the providers to leave "trap doors" in their systems, and that as a result it would be impossible to ensure that others did not gain access to the trap doors.

In fact, this claim is false. A system with the properties desired was proposed several years ago as a replacement for DES, and is used (where DES was never approved to begin with) for classified information. In this system, the government supplies the cryptographic "boxes" as sealed units; details of their operation is not made public. Keys are also provided only by the government. The algorithm has the property that only a tiny fraction of the possible keys actually work; using an "incorrect" key either produces nonsense, or produces an encryption that is easily breakable. Note that, while the algorithm used may be kept secret, it is quite possible that even if it were known, the following two problems would still be very difficult: Reversing an encryption with an unknown, good key; finding the algorithm for generating good keys. DES appears to have properties somewhat like this: Text encrypted with a "good" key

- any but one of a small set of weak keys - is hard to decrypt (no one appears to have broken DES in years of trying, except by brute force); and the method used for constructing the particular S and P tables in DES and showing that they are "safe" remains secret to this day, despite all details of DES itself being public.

With a system of this sort, the government (read some central authority) has in its hands a registry of all keys used, and can read whatever it wants. This is no different from, say, French law, which has always required that all users of cryptographic equipment register design details AND KEYS USED with the government.

A database of this sort, if properly implemented, would be fairly small. It could be centrally maintained and NOT available on networks. (In fact, ideally it might even be kept on paper, not in a computer!) No system of protection is foolproof, but a constrained system like this could be made quite secure. Whether we SHOULD accept such a system is a political and moral question, quite apart from its feasibility. I will point out, however, that the strongest argument FOR such a system is that it doesn't take away any rights that anyone has ever had in the past - it simply refuses to create a new right to (essentially) absolutely secure storage of information. (I'll also point out a strong argument AGAINST: The genie is long out of the bottle on this one. There are too many computers out there, with too much power, and too many reasonably good, well-known cryptographic algorithms to prevent anyone who really wants to keep data secure from doing so. Sure, the algorithms available to most people will probably fall quickly to a concerted attack by the NSA - but how many such attacks can the government reasonably expect to mount? This is difficult, labor-intensive work by highly skilled people who are a scarce resource.)

BTW, the same issue is certain to come up in a different form - in fact, I'm surprised it hasn't yet. I work for BIGCORP, which provides me with a workstation on which I store all my "work product". To keep the data secure, I encrypt it, using a key only I know. Can BIGCORP demand that I tell them the key? They, of course, argue, that the data is THEIRS, not mine. If I'm hit by a truck tomorrow, they need to be able to get at their data without me. (Further, though they probably won't say so in public, it's intolerable to them that I hold so much power over them: If I demand a raise "or the data stays encrypted", they are in big trouble. Sure, they can sue me, but they are unlikely ever to be able to recover what the lost data could cost them.)

-- Jerry

Re: U.S. Senate 266, Section 2201 (cryptographics)

<dsr@mir.mitre.org>
Thu, 11 Apr 91 10:06:00 -0400

It seems to me that it is not in the national interest for manufacturers of cryptographic gear to retain anything resembling a back door for themselves or "appropriate use of law enforcement." The existence of such a back door renders the equipment useless for secure transmission as those organizations and agencies which rely on secure transmission would have to rely on not just a

private key remaining secret but also a constant, i.e. the back door.

It is not even the case that the entire US government would be sanguine about even other sections of the government being able to wiretap secure conversations.

And as W. H. Murray points out, there are definitely problems with violating the constitutional guarantees against unreasonable search and seizure.

So any gear manufactured for Sec 2201 would, by default, be useless for any serious user of such gear. Maybe someone should tell the senate?

Douglas S. Rand, MITRE, Burlington Road, Bedford, MA <dsrand@mitre.org>

Re: U.S. Senate 266, Section 2201 (Cryptographics)(Bill Murray)

Ed Wright <edw@sequent.com>
Thu, 11 Apr 91 10:28:45 PDT

> ensure that communications systems permit the government to obtain the plain
> text contents of voice, data, and other communications when appropriately
> authorized by law.

It is precisely because of provision for such government snooping that people in Germany may not have extension phones. The analogy of the Secret Police listening in the phone is a bit crude but not entirely farfetched. Should this bill pass, I wonder how long it will take for the whiplash, or if society will still be able to produce whiplash.

Re: U.S. Senate 266, Section 2201 (cryptographics)

Gary Greene <garyg@convergent.com>
Thu, 11 Apr 91 11:54:35 PDT

>The referenced language requires that manufacturers build trap-doors
>into all cryptographic equipment and that providers of cconfidential
>channels reserve to themselves, their agents, and assigns the ability to
>read all traffic.

...Stuff intimating that leaks of back-doors are likely deleted...
It is quite likely, so no argument.

>Is there anybody out there who would buy crypto gear or confidential services
>from vendors who were subject to such a law?

Given any choice in the matter, I likely would not. I am not a drug dealer, but still have some things (strictly legal) that are my business and nobody else's. I may seem hypocritical to you in light of my comments below, but I see no conflict.

>David Kahn asserts that the sovereign always attempts to reserve the use of

>cryptography to himself. Nonetheless, if this language were to be enacted into
>law, it would represent a major departure. An earlier Senate went to great
>pains to assure itself that there were no trapdoors in the DES. Mr. Biden and
>Mr. DeConcini want to mandate them. The historical justification of such
>reservation has been "national security;" just when that justification begins
>to wane, Mr. Biden wants to use "law enforcement." Both justifications rest
>upon appeals to fear.

>In the United States the people, not the Congress, are sovereign; it should not
>be illegal for the people to have access tto communications that the government
>cannot read. We should be free from unreasonable search and seizure; we should
>be free from self-incrimination. The government already has powerful tools of
>investigation at its disposal; it has demonstrated precious little restraint in
>their use. < ...restatement deleted>

The problem I see in the above is what does the government do when there is grounds for "reasonable" search or seizure. And yes we should be free from self-incrimination, but as I understand the term (and I'm a pointy-headed liberal who worked for McGovern in '72 ...wonder how many of us are left who admit to it?) this protection from self-incrimination extends to our being forced to give testimony against ourselves. Fifth Amendment does not give blanket coverage to all our documents or uterances to third parties.
A search warrent or a wire tap must have means of entry to be enforceable, or are you saying that all electronic data communications should be off limits because they already can tap our phones and search our homes with an appropriate warrent? I can think of a few people in organized crime who would promptly move ALL their data and communications to this media if this were true. The guarantees in the Bill of Rights never said nor have the courts ever upheald, to my knowledge at least, any assertion that the government had no right of search or seizure, nor have the courts ever upheld that the people as a whole or individualy had a blanket right to communications which the the government could not access during proper and reasonable process.

While any process is subject to abuse by self-rightious people under color of office, and we can certainly point to many abuses in the past to our civil liberties (and not just in recent times ...look at the Palmer raids under Woodrow Wilson, and still earlier abuses throughout our history) I personally find your assertion that the government "has demonstrated precious little restraint" specious without supporting evidence. What I would like to see in your arguments is something more to the practical point of how we balance these various rights against the daily value and practice of law enforcement. Government should never be trusted blindly to protect our interests; that is the central theory behind seperation of powers. The problem with government in a libertarian democracy is how do we protect ourselves while extending to government the powers necessary for it to protect us from wolves. As JFK observed riding the tiger is often uncomfortable.

Gary Greene, Unisys/Convergent Technology, San Jose, California

---

SB 266 -- MORE

"Willis H. Ware" <willis@rand.org>

Thu, 11 Apr 91 15:46:45 PDT

Everything Bill Murray has raised about SB 266 is appropriate. But do note that the draft legislation says "It is the sense of Congress ...." It's a strange section in a way; Congress is simply stating its position on the matter, not doing something about it. SB 266 per se would take no action as Bill has outlined, but it sets the stage for action later by someone else.

The more subtle and real RISK in SB 266 is that it opens the door for putting such provisions into effect at other times. Then the Washington pols can claim: "It didn't happen on my shift."

Some time, some place, somebody -- legislator or agency bureaucrat -- will propose an action under SB 266 [if this Section passes] that will be socially acceptable and maybe even innocuous at the time. Then another one will come along, and maybe some ideas would not make it. But the cumulative consequence of all such indivdually small and individually socially acceptable actions will be disasterous to the established traditions and mores of the country and its basic structure.

Willis H. Ware

S. 266

<WHMurray@DOCKMASTER.NCSC.MIL>
Thu, 11 Apr 91 15:57 EDT

On re-reading S. 266, I find that I may have overstated my case a little. If this section were a stand-alone resolution of the Congress, then it is fairly clear that it would not be binding upon anyone. That is, the fact it is the sense of the Congress that someone ought to do something, does not mean that they must do so. As a part of this bill the provision has great potential for mischief, but it is still not clear that it would have the force of law.

William Hugh Murray, Executive Consultant, Information System Security
21 Locust Avenue, Suite 2D, New Canaan, Connecticut 06840
203 966 4769, WHMurray at DOCKMASTER.NCSC.MIL

Search RISKS using swish-e

THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

ACM Committee on Computers and Public Policy, Peter G. Neumann, moderator

Volume 11: Issue 45

Monday 15 April 1991

Contents

Simulation: Minus heart disease, life expectancy only 3 years greater!

<[anonymous]>
Mon, 15 Apr 91 12:06:46 xxT

New Heart Disease Study Issued
BOSTON (AP) [14 Apr 91]
Completely eliminating heart disease, the nation's leading killer, would increase the average 35-year-old American's life span by just three years, a new study concludes. Although the gain in longevity may seem surprisingly small, the finding reflects the difficulty of pushing back the boundaries of old age, the researchers said. Even if people escape the No. 1 killer, a host of other ailments are likely to take its place as people reach their 80s and beyond. "If you wipe out heart disease, people don't live forever," said Dr. Lee Goldman, a co-author of the study. "It is the leading killer, but there are other things people die from," such as cancer, pneumonia and strokes.
Similar analyses of cancer have concluded that life expectancy would

increase about two years if that disease were conquered. Heart disease kills about 500,000 Americans annually. The average life span in the United States has risen from 47 in 1900 to 75 today.

The latest study was based on a computer program developed by Goldman of Brigham and Women's Hospital in Boston and Dr. Milton C. Weinstein of Harvard School of Public Health. The study's principal author was Dr. Joel Tsevat of Boston's Beth Israel Hospital. It was published in the April issue of the journal Circulation.

In an accompanying editorial, Dr. Robert M. Kaplan of the University of California at San Diego called the study "well executed, well reported and very provocative."

The study asks such questions as: What if all Americans got their cholesterol levels below 200? What if everyone stopped smoking? The computer simulation concludes that achieving such major public health goals add only a year or so to the average life span. However, the authors point out that even though average increases are small, the gains for individuals can be dramatic, especially if healthier habits prevent occasional deaths from heart attacks at age 40 or 50.

Among the findings:

For the average man who turned 35 last year, getting blood pressure under control will add one year of life. Getting cholesterol under 200 increases longevity by eight months, eliminating smoking adds 10 months and getting weight down to the ideal level adds seven months.

For a woman, blood pressure control adds 5 months of life, cholesterol lowering 10 months, smoking cessation eight months and weight loss five months.

Individuals who already have one of these risk factors benefit more from eliminating them. For instance, a 35-year-old man who reduces his cholesterol from 250 to 200 gains one year of life. If he reduces his weight by 30 percent to the ideal level, he gains another year.

[What are the computer-related risks, you ask? Here are people using computer models to yield results that could have drastic impact on health care and research funding...]

[But the results may be quite sound... On the other hand, the elimination of heart disease would undoubtably have many concomitant effects, which overall probably could dramatically increase longevity. PGN]

Accident statistics continued

Paul Smee <P.Smee@bristol.ac.uk>
Mon, 15 Apr 91 11:15:11 BST

Don't normally follow-up things twice in a row, but apropos the recent thread about interpreting accident statistics (80% of drivers believe themselves to be better than average) I found a relevant article in the Guardian on Saturday, 13 April. I'll try a (probably weak) tie-in with computer risks at the end. Following is quoted without permission.

Most road accidents are caused by flouting the law rather than human error, such as a misjudgement, a psychologist said yesterday.

> Prof Tony Manstead, of Manchester Uni, said most accidents were
> caused by a small number of drivers who deliberately exceeded the
> speed limit and enjoyed racing other cars away from traffic lights
> and driving too closely to cars in front.
>
> One study of the Government's road research lab involved 500 drivers,
> the other 1500. The known accident records of the the drivers was
> compared with the way they described their driving.
>
> Those involved in two or more accidents shared certain characteristics,
> he said. They were likely to be young males who believed themselves
> to possess above-average driving skills.
>
> There was no correlation between people who admitted making driving
> errors, such as misjudging distances when overtaking, and accidents.
>
> But there was a strong link between accidents and people who admitted
> frequent traffic violations such as speeding or overtaking on the
> inside.
>
> Prof Manstead said: "At the risk of oversimplifying the picture, it
> appears that those who are involved in accidents are not those who
> tend involuntarily to make errors of judgement when driving but
> rather those who wittingly drive in a manner which flouts social
> and legal conventions.
>
> "... the strategy for promoting greater driver safety should be to
> identify the beliefs and values that underlie the commission of
> violations and then target those beliefs and values for change."

This fits in with a sample of one, known to me. My friend James, whose driving is such that I refuse to ride with him, even if that means we need to take two cars rather than one. He regularly ignores the 'social and legal conventions'. His rationale is that the conventions were designed to allow average drivers to drive safely. Since (of course, and according to him) his reactions are both faster, and more accurate, than average, the rules cannot possibly be meant to apply to him. Terrifies me.

Apropos technorisks, my intuition has long told me that similar principles apply to product design. I've known programmers, for example, who felt that they could dodge, where possible, company standards for testing and design reviews, on grounds that they were too competent to make silly mistakes. I suspect that the observations of Professor Manstead's study could equally be applied to most human activities.

Paul Smee, Computing Service, University of Bristol, Bristol BS8 1UD, UK
P.Smee@bristol.ac.uk - ..!uunet!ukc!bsmail!p.smee - Tel +44 272 303132

Another bogus security system

Gord Deinstadt <gd@geovision.UUCP>

Fri, 12 Apr 1991 19:52:14 -0400

A local muckazine (Ottawa Frank) reports that a student at Carleton University used the touch-tone registration system to deregister another student from all her courses. Apart from the political interest (the alleged practical joker is the son of the Governor General), this is another story of ill-conceived computer security.

When you enroll at Carleton you are issued a student id number, and a student card with the number displayed. Since the card is used to get into pubs and get discounts at off-campus bookstores, your id number is effectively public knowledge.

The touch-tone system responds to your id number and a "password". The "password" is your day and month of birth. No, you can't change it. Harrrumph.

Urban Legends crying wolf...

Peter da Silva <peter@taronga.hackercorp.com>
Sat, 13 Apr 1991 15:38:39 GMT

> The following posting recently appeared in several newsgroups and forums:

> >Subject: MODEM TAX
> As soon as it is posted again, it is immediately flamed down as bogus. Now
> further suppose that what the message claims *comes to pass!* How would
> this information be disseminated??

People don't apply equal weights to any source. For example, if this article comes from Joe_User@fred.fidonet.org it will likely be ignored. If it comes from Henry Spencer or Mike Godwin it'll be closely examined.

> Even were it discovered that someone was exploiting this security hole, how
> would information of this discovery be communicated??

Through postings in moderated groups of known reliability, and references in other groups.

(peter@taronga.uucp.ferranti.com)

Smart traffic: "drive-by-wire"

Rodney Hoffman <Hoffman.El_Segundo@Xerox.com>
Sun, 14 Apr 1991 20:22:22 PDT

The 14 April issue of the 'Los Angeles Times Magazine' features two articles on Mobility 2000, an Intellignet Vehicle / Highway System or "drive-by-wire" (my term, not theirs): THE BIG FIX by J.E. Ferrell and STREET SMART by Ronald B. Taylor. The last major 'Los Angeles Times' article on this was in July '89 (see RISKS 9.10 et seq.).

California Dept. of Transportation (CalTrans) researchers project "no revolutionary technological advances, just evolutionary applications" which "will allow platoons of cars, separated by only a few feet, to zoom along at 90 mph while their drivers read the newpaper." Similar moves are under study or development elsewhere in the U.S., Japan, and Europe.

Planners see financial, political, and cultural obstacles, but they are adamant that smart traffic systems are "the only way to keep things moving."

They also say automated travel will be much safer, since more than 90% of all vehicular accidents today are caused by human error. According to one UCBerkeley researcher, future accidents will resemble airliner crashes: "You'll be trading 100 accidents in which a total of 105 people get killed for two accidents in which 30 people get killed."

Here are some of the pieces discussed in the stories:

* Pathfinder, an in-car navigational computer and information system.
* Advanced Traffic Management System to monitor and control traffic flow via computers, sensors, and communications.
* Advanced Traveler Information System to link drivers with the management system.
* Advanced Vehicle Control System -- high-tech vehicles and roadways.
* Freeway Real-Time Expert System Demonstration (FRED), a UCIrvine project to "capture the expertise, judgment and knowledge of the best traffic controllers and put it into a computer program."
* Parataxi, a computerized system to link up commuting drivers with passengers on the spur of the moment.
* Transportation Resources Information Processing System (TRIPS) allows travelers to tap into bus schedules and the parataxi service
* Roadway Electric Powered Vehicle, powered by batteries continually charged by cables built into the roadway.
* Automated Traffic Surveillance and Control, installed for the 1984 Los Angeles Olympics, monitors corridor traffic lane-by-lane, and controls stoplights and freeway on-ramp meters.

A recommended article: "Probability Blindness: Why We Misread Risk"

Bob Frankston <Bob_Frankston%Slate_Corporation@mcimail.com>
Mon, 15 Apr 91 01:58 GMT

I'll start out with the citation for the article on Probability Blindness (Neither Rational nor Capricious): Bostonia Magazine, March/April 1991 issue. Author: Massimo Piattelli-Palmarini at the MIT Center for Cognitive Science. I recommend the article to readers of this forum. It does a good job of exploring how people assess risks and probabilities with a number of examples.

I found it much better than Nova's "Living Against the Odds". While there are many real risks in the world, I felt the Nova show emphasized risks rather than unlikelyhoods. Perhaps that was their intent. My problem is that I feel that people are acutely tuned to risks and not the unlikelyhood of many occurrences. The Bostonia article was a more balanced piece. I'm more accepting of the

emphasis on risks in this forum not only because of the name, but because I see its purpose as making people aware of possible implications of the technology we are responsible for. Even here, I'd like to see more discussion of engineering tradeoffs.

Back to the citation problem. I'm used to electronic distribution (such as Risks Forum). If I want people to read something, I either mail it out or announce a means of accessing it online. Recommending an article in the print media is not the same. The effort to actually obtain a copy is relatively large and unaided -- it involves either phoning or writing for a back issue or a reprint. If people actually did follow through the volume might be larger than the publication is ready to handle.

If you do want to contact Bostonia Magazine, their subscription number is 617-353-2055 (yes, that is the Boston University phone exchange). Too bad they (nor the author) didn't publish an email address.

Kevin Poulsen Arrested

Peter G. Neumann <neumann@csl.sri.com>
Mon, 15 Apr 91 11:25:07 PDT

Today's papers (e.g., NY Times, LA Times) note that Kevin L. Poulsen (Dark Dante) had been arrested after 15 months, under a variety of computer-fraud charges, while entering the canned vegetable section of a supermarket in Los Angeles. Poulsen and co-defendants Robert Gilligan and Mark Lottor were charged with using stolen Pacific Bell access codes to invade a U.S. Army computer network, eavesdrop on telephone security personnel and obtain information used in an FBI investigation of former Philippine President Ferdinand Marcos, said Richard W. Held, special agent in charge of the FBI's San Francisco office. Gilligan has pleaded guilty to one count of illegally obtaining telephone access codes and agreed to cooperate with authorities. Lottor pleaded not guilty and declined a similar plea bargain, officials said.

Computerized Vote Tallying report

Terry Gauchat <trgauchat@tiger.waterloo.edu>
Thu, 11 Apr 91 23:12:39 EDT

[Terry sent me a rather long term paper on the subject of computerized vote tallying, which I have edited for net use. Those of you with a burning interest in the subject may find it useful. The original is available from him, and my slightly edited version can be obtained from the CRVAX.SRI.COM archive, as CD RISKS: and GET GAUCHAT.VOTING . Apparently his net address is about to change, however, so I hope he will advise us when it does. PGN]

(PLEASE REMEMBER THE COLON IS ESSENTIAL. I KEEP GETTING COMPLAINTS THAT FTP DOES NOT WORK, MOST OF WHICH ARE DUE TO IGNORED COLONS. OTHERS ARE DUE TO LOCAL FTP VARIANTS... AND IF YOU DON'T LIKE "CD RISKS:", you may happily type "cd sys$user2:[risks]" instead, courtesy of VMS. PGN)

Search RISKS using swish-e

Report problems with the web pages to the maintainer

Search RISKS using swish-e

THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

ACM Committee on Computers and Public Policy, Peter G. Neumann, moderator

Volume 11: Issue 46

Monday 15 April 1991

Contents

Credit card number theft at major Toronto BBS

<rwh@ontmoh.UUCP>
Fri Apr 12 22:18:38 1991

I received the following below when I logged on to ROSE Media BBS, Toronto's (and probably Canada's) largest public access bulletin board system. I'll relay further developments if there's any interest on the part of RISKS.

Russ Herman

==========

Date: 04-11-91 (19:40) Number: 48911 of 49624
To: RUSSELL HERMAN Refer#: NONE

From: SYSOP Read: NO
Subj: Your Mastercard Status: RECEIVER ONLY
Conf: MAIN BOARD (0) Read Type: GENERAL

Russell,

Last night, a Sysop in the Toronto area uploaded a file to us which was a listing of the portion of the Users file that was downloaded from Rose Media during the security breach that occurred on or about February 9th last. This list did contain credit card numbers of 420 Visas, 150 Mastercards and 4 American Express cards. Unfortunately, your card was one of those that got out. The breach was an accident that apparently was caused by failure in one of the third party programs we use to run Rose Media.

We sincerely regret that this has happened, and have rearranged our files in such a way, that it will never happen again. There is another message posted to you which will give you more details on how the breach occurred, what we did at that time, what we are doing now and in the future to protect you and Rose Media.

We wish to assure you, that in no way are you obligated to pay for any fraudulent charges on your card. Please check you card statements very carefully to make sure that everything is valid. It would also be advisable to call your credit card Company and have them issue you with a new card. We will be supplying a list of all card numbers acquired during the breach to the security divisions of the various card granting Companies affected. The names and numbers of all security officers in these Companies was given to us today in a meeting with the Metropolitan Toronto Police Fraud Squad, who will be actively pursuing the case. Charges will be laid against all those apprehended.

Thank you for your patience and understanding in this matter. We have done, and will continue to do everything we can to apprehend and bring to justice all those that have used the information obtained during the breach, no matter how this information was used. If you do find a fraudulent charge, please advise your credit card Company, as well as David Hodgson of the Metropolitan Toronto Police Fraud Squad at 324-6136. If you have any information whatsoever that you think might help to catch and prosecute the offenders, please let us know by a private message to the Sysop. We will be working very closely on this matter with the police.

Best regards ..... Vic.

Junk FTP hits internet

Larry Hunter <hunter@nlm.nih.gov>
Tue, 9 Apr 91 13:05:31 EDT

I suppose it was bound to happen. First junk mail, then junk fax, now junk ftp. Someone has apparently been using anonymous ftp to write two files to internet hosts. These files contain advertising for a consumer credit insurance service (which sounds suspect in itself) and offers bounties for putting up advertising fliers and sending in unspecified information about local banks. The only identification offered in the files is a name (P.L.

Miller) and a post office box in Auburn, Alabama.

The two files were written to our local machine at 2:16 am on April 8, and were called CREDIT_CARD_INDEMNIFICATION and MONEY_FOR_BANKS. Randomly picking a distant internet host, I found two very similar (not identical) files on cs.yale.edu, created at 12:51pm on March 31. Looking around elsewhere, it appears that the files were only writen to hosts that allow the world to create files in the "login" directory for anonymous ftp; there were no files on hosts where there was a writable subdirectory but the top level was write protected, implying that the junk ftp was delivered via some automated process.

The risk here is a variation on the "tragedy of commons," i.e. a free resource provides incentive to overuse it, which degrades its value to the community. Being able to upload files anonymously is valuable, but the ability to do so will be curtailed if we are innundated with junk. Unfortunately, there is no way to screen out the junk without also losing the ability to get valuable but unsolicited uploads.

Larry

Lawrence Hunter, PhD., National Library of Medicine, Bldg. 38A, MS-54
Bethesda. MD 20894 (301) 496-9300 hunter%nlm.nih.gov@nihcu (bitnet/earn)

Status of S. 266

<WHMurray@DOCKMASTER.NCSC.MIL>
Sun, 14 Apr 91 14:43 EDT

S. 266 has been referred to the Senate Judiciary Committee chaired by its author, Mr Biden of Maryland, and to the Senate Environment and Public Works Committee. No action has been taken on the bill. No hearings are scheduled.

Re: S 266

<34AEJ7D@CMUVM.BITNET>
Mon, 15 Apr 91 10:49:43 EDT

The potential for abuse here is mind-boggling. The common custom and practice in America has, for 200 years, been that the government has NO automatic right of access to private papers, documents, transmissions, data, etc., sithout clear due process. By creating a clear-text copy of a cryptographic transmission, or the immediate means to do so, this idea would short-circuit that due process into an Orwellian parody of prove-we-should-not-have-your-data.

And who is going to pay for the additional archiving that could be required under such legislation?

I know of at least one prominent American who has openly expressed a global distrust for the government's attitude toward personal privacy. Further, he has gone to such lengths to preserve his own personal

privacy as to encrypt a large portion of his personal correspondence, using a number of different ciphers depending upon the intended recipient. This same gentleman has expressed the opinion that documents entrusted to the mails are not secure and should be encrypted.

You know him. His name is Thomas Jefferson.

This S 266 business is a very old wolf, dressed up in a few new clothes. The government has been trying to spy on its citizens since it was *created by those citizens.*

W. K. Gorman

Congress and Encryption (Murray, RISKS-11.43)

Roy M. Silvernail <roy@cybrspc.UUCP>
Sun, 14 Apr 91 02:47:21 CDT

In V11, Issue 43, Bill Murray passes on an extract from Senate Bill 266:

> It is the sense of Congress that providers of electronic communications
> services and manufacturers of electronic communications service equipment
> shall ensure that communications systems permit the government to obtain
> the plain text contents of voice, data, and other communications when
> appropriately authorized by law.

While Mr. Murray comments on the impact to cryptographic equipment manufacturers, I wonder about the RISKS to common-carriers and, for that matter, entities such as Usenet and local BBS's.

A "provider of electronic communications services" such as CompuServe would, under this provision, have to forbid the movement of encrypted text over its facilities. Let's say I choose to encrypt my E-mail before sending it, and further hypothesize that the FBI had some interest in what I say in E-mail. Would CompuServe now be required to monitor my E-mail? Would they forbid the encrypted transmissions, or simply demand the key and program to decrypt them?

Considering Usenet is even cloudier. With the distributed nature of the Net, literally thousands of admins would be held responsible for accessing cleartext translations of encrypted transmissions passing through their systems. This places all of us in the ethically untenable (and physically impossible) position of having to monitor all the traffic passing through our systems.

What of common carriers under this act? They have been traditionally held not to be accountable for the actions of their users. Will the telephone companies now be forced to monitor all its lines, cutting off the first sign of a scrambled transmission?

I see this as another step in the same style of repression that gave us Operation Sun Devil. It's apparant that our leaders fear the Information Age and the power that it places in the hands of the people.

Making the ability to privately communicate an exclusive privelege of
the ruling class is nothing short of terrifying.

Roy M. Silvernail roy%cybrspc@cs.umn.edu cybrspc!roy@cs.umn.edu

---

S. 266

<WHMurray@DOCKMASTER.NCSC.MIL>
Sun, 14 Apr 91 11:45 EDT

>In fact, this claim (re: trap doors) is false. A system with the properties
desired was proposed several years ago as a replacement for DES.....

Well, I think that is a little strong. I will not be so strong in my
characterization of Mr. Leichter's posting. I will only say that: 1) while
the mechanism to which Mr. Leichter refers may have the properties which the
sponsors of the bill desire, it certainly does not remedy my objections to S.
266, 2) that I take the authors at their word and that word requires a trap
door, 3) perhaps Mr. Leichter has a greater trust in authority than I do, and
4) perhaps he missed the point of my objection.

First, I am well familiar with the mechanism to which he refers. Rather than
refute my claim, he proves it. Unfortunately for me, he chose the one proposal
that I am least happy having to discuss in a public forum.

Please do not get so bogged down in the elegance of the mechanism that he
endorses that you fail to recognize it for what it is. It is a trap door. "In
this system, the government supplies the cryptographic "boxes" as sealed units;
details of their operation is not made public. Keys are also provided only by
the government." That is a TRAP DOOR in any system into which it is
incorporated. Even if it is never used or exploited it reduces confidence in
the system.

Now, make no mistake about it, dear reader; the proposal which Mr. Leichter so
well represents did not originate with the U. S. Postal Service or Her
Majesty's PTT. It did not originate with those whose job it is to deliver the
mail while preserving its confidentiality. It originated with the world's
largest intelligence gathering agency, whose name ne'er escapes my lips. It
originated with those whose job it is to read other people's mail.

Dear reader, this proposal originated with the fox; it did not originate with
the farmer and it certainly did not originate with the chickens. The fox is a
fox to his toes; he is all fox. He is not sometimes a fox and sometimes a
farmer. Those of you who are familiar with the world's largest intelligence
gathering agency, whose name ne'er escapes my lips, know that reading other
people's mail dominates the essence of the institution. The ability to read
other people's mail dominates every thing they do, every decision they make,
every proposal they offer. They will read other people's mail, and when they
do not, they will still preserve their ability to do so.

Who can have confidence in any encryption mechanism that comes from and whose
keys are supplied by the world's largest intelligence gathering agency? I

quote Courtney (if I could not quote Courtney, I would be more often silent), who said at the time this proposal was first floated, "While I trust the minions of the world's largest intelligence gathering agency, (whose name ne'er escapes my lips) to abstain from treason, I do not trust them to abstain from fraud." The last thing I might expect of them is that they would abstain from reading other people's mail.

Indeed, this proposal is a "trap door." It is a hoax. It is precisely the kind of mechanism that I fear in response to the law. It is a mechanism that puts too much power in the hands of the government.

I do not have any direct evidence that the proposal to which Mr. Leichter refers and S. 266 have any common origins; no reasonable person would expect that I could have. Nonetheless, I will go to my grave suspicious that they do.

Orwell understood that bureaucracy need not have malicious motives in order to be malevolent; it only has to do what bureaucrats do. I respect the fox; I have many friends who are foxes. Nonetheless, I expect them to behave like foxes and I behave accordingly.

William Hugh Murray, Executive Consultant, Information System Security
21 Locust Avenue, Suite 2D, New Canaan, Connecticut 06840 203 966 4769

Re: U.S. Senate 266, Section 2201 (cryptographics) (Greene)

Robert I. Eachus <eachus@d74sun.mitre.org>
Mon, 15 Apr 91 19:51:23 EDT

> Gary Greene <garyg@convergent.com> says:
>
> The problem I see in the above is what does the government do when there is grounds for "reasonable" search or seizure. [...] The guarantees in the Bill of Rights never said nor have the courts ever upheald, to my knowledge at least, any assertion that the government had no right of search or seizure, nor have the courts ever upheld that the people as a whole or individualy had a blanket right to communications which the the government could not access during proper and reasonable process. [...]

I could not disagree more. The words "`reasonable' search or seizure" should tell you that there are many types of search or seizure which are totally immune to a bench warrent. For example, Constitution is quite explicit in the way it says that communications between TWO individuals cannot be evidence of treason. Also most conspiracy laws require "three or more persons" for their to be a conspiracy. Under many circumstances, a discussion with a lawyer cannot be revealed, even voluntarily, by the lawyer. And finally, the many laws (and the common law provision) that a man cannot be compelled to testify against his wife, and vice versa. (P.S. In what follows, you might want to keep in mind that I am not a lawyer, although there are several in my family. I have spent a lot of time studying constitution law, both as a hobby, and as a part of family history.)

Now let's sit down to an actual case: You and I agree on a key, and we send several messages back and forth using, say, DES. A police officer comes into your office with a search warrent allowing him to seize all messages to and from Robert Eachus, and all keys pertaining thereto.

Then the fun begins. You don't have a written copy of the key, so it can't be seized, so after heavy badgering, you agree to testify under a grant of immunity. The cops now say, okay what is the key? You say, tough luck Jack! You can force me to testify as to the contents of the messages (providing a basis has been established, etc.) but there is no power in the law to force me to translate the messages for you...

Okay, so you want to be that way, do you...and they start setting a basis for asking you about the conversation in which I told you the key... However we agreed to a procedure which established the key from two words, one from each of us. (Assume for the moment we did it "right," and half the seed is worse than useless.) Now, can you be forced to testify about your chosen word? I don't see how. It is either self incrimination, the most serious violation of privacy possible, entrapment, or since YOU have immunity concerning any criminal actions of yours discussed in the encrypted messages, they cannot be shown to involve a crime. (The distinction between messages which describe a crime {useless} and those which are part of a crime is very important.) So I am safe from the thought police unless you are stupid and vice-versa.

A similar, but as you realize, different in nature situation, is if I have a warrent which allows me to seize a safe (and its contents) in your house. In theory, the combination is safe from seizure, in practice the police will use brute force to open the safe if you don't provide the combination. In theory, a judge could order you to open the safe. In practice, I don't think any such evidence could be used. (So a safe which destroyed its contents upon "unauthorized" opening could protect you, legally, but I don't think I'd want a bomb around which could accidentally blow my head off.

I have thought and thought about a "safe" law allowing some such seizures and, in this country, there is no such thing. The rule is, should be, and has to remain, that unless someone who saw me type that message is willing to testify, IN OPEN COURT, that that is in fact the message I sent, such correspondence is no evidence of anything and should neither be admissable or subject to seizures.

Stolen software is another situation, including stolen data... Seizure is possible and theoretically useful , but I would hate to be arguing chain of evidence in front of the Supreme Court to show that:

1) The software was "in the possesion of the defendant." -- Relatively easy, but chain of evidence may be very hard to prove, if procedures are sloppy.

2) The defendant knew he had it, and knowingly received to stolen merchandise. -- If you haven't got the guy who gave it or sold it the defendant to testify, lots of luck. Circumstantial evidence? Boasting to friends? Sold it to others? Aaah. Such things as the defendant putting his name in it, or handwriting on a floppy disk, might do the job. (According to what we just saw, some people are THAT dumb. In my opinion stealing software is always dumb, but there are degrees of dumbness.)

I have been thinking about a constitutional amendment to fix forever some of these problems. When I've gotten the wording worked out I'll post it, but basically it tries to establish "beyond the reach of the law" three things:

* Personal papers, disks, RAM, etc., which are notes to oneself. The distinction between in your head and on paper is getting less and less clear...

* "Private correspondence" whether electronic, on paper, or in person, without the permission of one of the parties to the correspondence. The wording, and the intent could be that telephone conversations, unless encrypted are public, but I am not sure that that is a valid distinction. Certainly, I would like to see lots of evidence that legal wiretaps, entered in evidence, had resulted in convictions. They certainly have resulted in lots of legal mischief. A much better rule here might be that a use of a legal wiretap could not contaminate evidence it led to, but it could only be presented in court as part of a chain of evidence.

The idea here is that even if I were to write you a letter explaining, in gory detail, how I dismembered your mother-in-law. There is no legal path to that evidence without your co-operation or mine. (Posting it on a bulletin board, electronic or otherwise, is of course such co-operation, even if unintentional. Again, proper definition of private is the trick. The circumstances under which E-mail must be considered to be private will need to be established by legislation and case law, but certainly the enciphered messages above are beyond search and seizure. Notice that this type legal presumption already exists for some types of communications.

* Finally, there is a class of tools and records which should be incapable of seizure even when search is permitted. Can a man get a fair trial if deprived of his hearing aid? If he is only allowed to use it in the courtroom? What use are eyes, if notes useful in my defense are encoded magnetically? Translation: Even if you are allowed to search my "memory aids," to deprive me of their use denies me a fair trial. Period. A court would not dream of making records available to the prosecution which are unavailable to the defense. (Well maybe some judges dream about it, but they know they had better not.)

What I want to do here is to say that a paper listing of a database is not the same thing at all, and that part of my entitlement to council could be a net connection (and my personal computer). If the prison doesn't provide an Internet connection, it's bail or walk away free. This may seem extreme, but it is on the verge of becomming a necessity. To deprive a junky of illegal drugs is not considered "cruel and unusual punishment" but to deprive a diabetic of insulin certainly would be. At what point does depriving a net junky of net access fall into the second class? And hadn't we better wait until after the trial to impose such a punishment if legal? Especially since, I can imagine many situations in which relatively access to the net would be the difference between conviction and freedom.

Hypothetical example: I was home "alone" when the murder was committed, participating in an electronic meeting. I may have to act quickly to get several people who attended the meeting to keep their session records to show that there was no gap of say twenty minutes in which I could have committed the

crime. The jury is going to have to decide if I had a confederate, and whether or not I was posting from home, but with that transcript, preferably more than one copy, I am in much better shape. Just having access to MY records may be all that is needed to allow me to say, oh yeah, I was bowling that night with friends. As interaction times get shorter, and with things like Shadow, and talk, and... we may soon have a major electronic alibi case, other than on televison.

Risks of Silly Legislation

Joseph Pallas <pallas@alydar.eng.sun.com>
Fri, 12 Apr 91 10:03:40 PDT

Without knowing the context, it's difficult to judge just how senseless this "sense" is. The significance of "sense" in this case, I suspect, is to guide the judiciary in decisions about the intent of Congress. The executive has broad power to make binding regulations that can only be voided if they contradict the clear intent of the legislature (or are unconstitutional).

Whether there is really any sense here depends on a number of things, including the definition of an "information transfer service." The most widely used electronic information transfer service today is the telephone system. The suggestion that AT&T, for example, might be responsible for ensuring that no unauthorized encrypted messages cross its network is absurd. There is no way that an information transfer service can even tell whether a message is encrypted, not to mention that the Electronic Communications Privacy Act would explicitly disallow observation of message traffic for that purpose (by my reading, I am not a lawyer, this is not legal advice, consult a lawyer blah blah blah).

A more basic question that's been raised in the discussion is whether the risk of allowing secure communication outweighs the right to keep secrets. If it does, then we can surely expect as a consequence any number of changes in our lifestyle, most of which will be reminiscent of Orwell's 1984. Secure communications go far beyond electronic information systems, extending to every possible communications medium. If we remain free to speak and publish whatever we will, then secure communication will be possible. Attempts to prohibit it are in conflict with the very foundation of a free society.

joe

Re: Sense of Congress

Edward N. Kittlitz <kittlitz@granite.ma30.bull.com>
Fri, 12 Apr 91 09:48:57 EDT

Willis Ware writes about the sense of Congress: "Congress is simply stating its position on the matter, not doing something about it." Isn't it the case that many judicial questions revolve around the "intent" of the legislators? Isn't this a handy way to reduce the language of a law, while expanding its applicability in unpredictable ways?

E. N. Kittlitz kittlitz@world.std.com / kittlitz@granite.ma30.bull.com

Security Contest

"Dr. Harold Joseph Highland, FICS" <Highland@DOCKMASTER.NCSC.MIL>
Fri, 12 Apr 91 13:23 EDT

CALL FOR PAPERS for ACM/SIGSAC Student Paper Contest in Computer Security

Dr. Harold Joseph Highland, FICS
Distinguished Professor Emeritus of State University of New York
Managing Director of Compulit Microcomputer Security Laboratory
Editor-in-Chief Emeritus of Computers & Security

Telex: +1-650-406-5012 MCI Mail: 406-5012 Voice: +1-516-488-6868
Electronic mail: Highland@dockmaster.ncsc.mil

CALL FOR PAPERS

Student Paper Competition: Computer Security, Audit and Control
Sponsored by ACM/SIGSAC

The purpose of this paper competition is to increase the awareness of security, audit, control and ethics as they apply to the computing field. SIGSAC will award $1,000.00 to the student or junior faculty member whose paper is selected by the review committee as the outstanding contribution of the year.

The contest is open to all full-time undergraduates, graduate students and junior members of the faculty of a recognized or accredited institution of higher learning. Only those who have not previously had a paper published in a referred journal in which he or she was the lead or sole author will be eligible for the award.

Papers must be received by the SIGSAC Competition Committee Chairman
on or before October 7, 1991

SIGSAC reserves the right to publish any submitted paper, whether selected for a prize or not, in SIGSAC Security, Audit and Control Review. Author will be notified about acceptance of his or her paper for publication within 90 days after the announcement of the contest winner.

SUGGESTED TOPICS

Access/authentication control
Administrative policies, standards and procedures
Audit concerns for data communications
Auditing in computer security
Banking industry security
Communications security
Computer crime
Computer law
Computer security audit techniques

Computer viruses and other threats
Contingency planning
Crypto systems and encryption
Data integrity and security
Database security
Distributed systems security
Dynamic signature verification
Education for computer security
E-mail systems security
Electronic funds transfer
Ethics and security
Expert systems in security
Formal specifications and verification
Information system security
Key management
Local area network security
Logging and accountability in security
Medical databases and security
Microcomputer security
Modeling security requirements
Multi-level security
Network design for security
Network security issues
Office automation security
Open communications and security
Operating systems security
Operational assurance in security
Passwords: management and controls
Penetration testing as an audit tool
Physical security
Privacy and security
Protecting programs and data
Risk analysis and assessment
Risk management
Smartcards and security
Telephone intrusion threat
Tokens as a security tool
Trusted systems
Use of microcomputers in an audit environment
User authentication

INSTRUCTIONS TO AUTHORS

[1] The manuscript must be typed double-spaced on one side of the page with one-inch top, bottom and side margins. All illustrations must be in camera-ready form. An abstract [maximum of 100 words] should be included on the first page. Style and format of the paper should follow the form used in Communications of the ACM.

[2] Manuscript is limited to a maximum of 25 double-spaced typewritten pages.

[3] The author's name, address and any references to a university must not appear in the paper. Acknowledgements, if any, must appear on a separate page.

[4] Five (5) copies of the paper [quality photocopies will be accepted] should be submitted together with a covering letter and the additional information requested as contained in this announcement.

[5] A floppy disk [3 1/2" or 5 1/4" standard or high density format], preferably in DOS ASCII format, should also be included.

[6] All copies should be sent prior to October 7, 1991 to:

Dr. Harold Joseph Highland, FICS
SIGSAC Competition Committee
562 Croydon Road
Elmont, NY 11003-2814 USA

Telephone: [+1] 516-488-6868 Telex: [+1] 650-406-5012
MCI mail: 406-5012 E-mail: Highland -at dockmaster.ncsc.mil

==== Author Information Entry Form ====

[Please reproduce in typewritten form and submit with paper]

Title of paper .....
Author's full name .....
Full name of school .....

Author's home address .....
Author's school address [if applicable] .....
Telephone number .....
E-mail address .....

Name of faculty advisor .....
<For junior members of faculty only>
Full address .....
Telephone number .....
E-mail address .....

Degrees held or year at college .....
Previous publications [if any]; list title(s), publication in which article appeared and date .....

COMPETITION COMMITTEE

* Mr. Virgil L. Gibson, Grumman Data Systems, McLean, VA USA
* Dr. Daniel Guinier, IREPA Computer Security Department,
French National Research Council, Strasbourg, France
* Mr. Gerald Isaacson, Information Security Services, Northborough, MA USA
* Mr. Stanley A. Kurzban, International Business Machines, Thornwood, NY USA
* Dean Dennis Longley, Faculty of Information Technology, Queensland University
of Technology, Brisbane, Queensland Australia
* Mr. Hanan Rubin, Metropolitan Life Insurance Company, New York, NY USA
* Squadron Leader Martin Smith, Royal Air Force, Peterborough, England
* Professor Louise Yngstrom, The Royal Institute of Technology, The University
of Stockholm, Stockholm Sweden

Search RISKS using swish-e

THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

ACM Committee on Computers and Public Policy, Peter G. Neumann, moderator

Volume 11: Issue 47

Tuesday 16 April 1991

Contents

"Electronic mail message may be bylaws violation"

"Peter G. Neumann" <neumann@csl.sri.com>
Tue, 16 Apr 91 12:01:22 PDT

The Stanford Daily on 15 April 1991 had a front page article by Howard Libit, staff writer, on Nawwar Kasrawi, a Stanford senate associate and election candidate who on 14 April sent EMail to over 2000 students urging them to support the People's Platform Council of Presidents `Stand and Deliver` slate, senate candidates, and special fee requests. Academic Information Resources, which operates the campus computer system, froze his account soon afterwards, because the messages were clogging the system. There is debate over whether he violated election bylaws governing the use of EMail in elections, whether the disk space used exceeded AIR policies, and whether the fair-market value of the mailing would exceed the campaign spending limits. It seems to me as an

uninformed observer that the existing guidelines did not adequately anticipate all of the potential (mis)uses, creative and otherwise. The article listed various unrelated problems, and did not indicate whether this election would be conducted on-line as was the case in a recent election, noted here in RISKS... PGN

Re: Nuclear Detonation Model Wanted (Michael Squires via Keith Bostic)

Gene Spafford <spaf@cs.purdue.edu>
Tue, 16 Apr 91 14:21:59 EST

From: bostic@okeeffe.Berkeley.EDU (Keith Bostic)

From: mikes@iuvax.cs.indiana.edu (Michael Squires)
Newsgroups: alt.sources.wanted
Subject: Re: Nuclear Detonation Model Wanted.

The Office of Civil Defense published a book called "Nuclear Weapons Effects". It was used in CD training classes. It contains equations and nomographs that will let you determine how quickly an air, land, or water burst will demolish various structures. GE published a little booklet in the '60's (the may still do it) that contained a nuclear weapons effects slide rule, plus similar tables.

In terms of computer software the most famous isprobably the SIR NEM model (Strategic International Relations Nuclear Exchange Model) created by the Agency for Interscience Methodology in Chicago in the 70's which was run by ACDA and by the Joint Strategic Targeting Planning Staff. Another model still apparently in use is the Arsenal Exchange Model which was less disaggregated. (This is current as of 1980, the last time I spent much time in this area..) The sources for SIR NEM were available from ACDA at one time, with all the comments removed (except for the JSTPS line numbers!).

An interesting aside: when I recompiled a version of AEM that I know was used during the SALT I talks I was interested to find 13 FORTRAN errors missed by the more primitive compilers of the early 70's (CDC 3600 FTN). These were all uninitialized variables. Now, about that 100% reliability you promised....

Mike Squires (mikes@iuvax.cs.indiana.edu) 812 855 3974 (w) 812 333 6564 (h)
mikes@iuvax.cs.indiana.edu 546 N Park Ridge Rd., Bloomington, IN 47408

---

automated car parking?

Alayne McGregor <alayne@geas.gandalf.ca>
Tue, 16 Apr 91 09:39:02 EDT

The local CBC morning show in Ottawa had an interview with a Volkswagen of Canada representative this morning about a car that supposedly parallel-parks itself.

The representative said the car is a test prototype built by Volkswagen of

America. It can sense whether a parking space is large enough, and place itself in the spot with only inches to spare on either side. The driver does not need to be in the car.

She said the proximity sensors used for this can also be used while driving to ensure the car does not get to close to other cars.

I wonder who would be liable if the car software bashed the next car while parking, or if it ran over a cat, dog, or child on its approach. One would think the location and range of the sensors would be very important.

Alayne McGregor alayne@gandalf.ca

Databases v. Privacy in Europe and the US

<sullivan@poincare.geom.umn.edu>
Tue, 16 Apr 91 15:03:13 CDT

Two pointers to recent NYT articles:

Front Page, Thursday, April 11: "Europe's Plans on Privacy Upset Business" describes new rules the EC is considering regarding corporate databases. All databases would have to be registered with a government authority. Customer lists or other data could not be sold without the customers' permission. Databases would not be able to be transferred to outside countries with less stringent laws. American companies with European subsidiaries are worried they would have problems keeping track of personnel. Critics claim a strict interpretation would prevent, say, European Airlines from taking reservations from overseas, since this would involve info like credit card numbers.

Business Section, Sunday, April 14: "The Man With All The Numbers" talks about James Bryant, who sells the complete contents of all US phone directories (white pages) on 2 CD-ROMs, for about $2k. His company, Phone Disk, used to compile the list of about 100M names from direct marketers, but a recent Supreme Court ruling has established that White Pages listings are not copyrighted. Bryant hopes eventually printed white pages (which use 4 million trees' worth of paper) will be unnecessary.

--John Sullivan@geom.umn.edu

Re: European police networks

Sanford Sherizen <0003965782@mcimail.com>
Tue, 16 Apr 91 17:27 GMT

Pete Jinks <pjj@cs.man.ac.uk> asked about the European Nervous System (ENS),

>"The ENS will create links between administrative computer networks [in the >EC] including tax, social security and environmental monitoring. ... intense >activity on police networks which ... will be essential when frontier control >are relaxed in 1992". The EC "is seeking powers to make it compulsory for >member states to link their computer systems"

>This is represented as being a vital part of a program to pump money into the
>european IT industry. I don't remember reading or hearing about this before.
>I hope that this is an April fool, but it has a ghastly ring of plausibility.

EC '92 Single Market Unification will have a major impact on information security and privacy. Here is some information on the topic that Pete raises. This is taken from my book, INFORMATION SECURITY IN FINANCIAL INSTITUTIONS (London, Dublin: Lafferty Publications, 1990).

"The Schengen Accord on open borders was signed by EC nations as an attempt to balance the potentially contradictory goals of open borders and crime control, particularly drug distribution. Prior to the Schengen and similar agreements, drug trafficking restrictions were based primarily at the state level, often concentrating on police activities at border control offices. The Schengen Accord builds on previous EC action against drugs, including the establishment of an information system or data network, to share information about suspected criminals and other police intellgence. The Trevi Group, which focuses on the fight against terrorism, drug trafficking, and organized crime, also proposed a legal regime on European information technology for identifying and controlling criminals, particularly international terrorists and drug dealers.

Belgium, which at the time of the signing, did not have a law protecting access to electronic data kept on file about its citizens, promised to pass new legislation before the Agreement came into full effect. Other European nations outside of the EC will be brought into negotiations quite soon in order to expand the Agreement's provisions to larger areas of the Continent."

Non-European nations, including the U.S., and international police organizations such as Interpol, are sharing an increased amount of information that will interface with and supplement the EC network. The EC and Council of Europe Data Privacy laws will play some role in defining appropriate collection and use of police information but the fight against drugs, money laundering, and terrorism will strongly influence how much the police network will collect and how information will be used.

Sandy

Sanford Sherizen, President, Data Security Systems, Inc., 5 Keane Terrace
Natick, MA 01760 USA MCI MAIL: SSHERIZEN (396-5782) PHONE: (508) 655-9888

Fear of Information Age/Systems

"351M::ESTELL" <estell%351m.decnet@scfb.nwc.navy.mil>
16 Apr 91 07:50:00 PDT

Two books by Alvin Toffler describe the general causes of the apparent fear that "those in control" have of information age systems (e.g., e-mail, encryption programs ...):

FUTURE SHOCK, which describes how some of us are overwhelmed with the pace of progress; and

THE THIRD WAVE, which describes how control of the masses first
rested on control of land (in the agricultural age, the first wave),
the control of the money supply (in the industrial age, the second wave),
and will soon rest on control of information (in the informatin age,
the third wave).

"Those in control" include most traditional authority figures, not just
government; and "fear" [as I have used it] implies "lack of comfort"
BUT NOT NECESSARILY any subsequent malicious actions.

Both books are available in paperback; maybe at used book stores.

Bob

[Classics. We have seen these mentioned in RISKS before,
but include them again for our newer readers. PGN]

Re: Simulation: Minus heart disease, life expectancy only 3 years greater!

Brinton Cooper <abc@BRL.MIL>
Mon, 15 Apr 91 22:23:41 EDT

Another risk of this computer-assisted study is that the conclusions miss the
point. It's not adding 3 years to human life that's significant about
eliminating heart disease. It's about the elimination of perhaps decades of
various degrees of disability; it's about perhaps not having to spend 5-10
years in a nursing home while your life's savings are not so slowly eroded.

One of the serious risks of computer-assisted studies is that the data can be
munged so quickly that the investigators don't take the time to reflect upon
the problem. In the old days, when hordes of grad students had to collect and
reduce data more or less manually, such studies took much longer. The PI had
plenty of time to reflect upon just what question was being addressed.

Re: Simulation: Minus heart disease... [RISKS 11.45]

Jeff Johnson <jjohnson@hpljaj.hpl.hp.com>
Tue, 16 Apr 91 16:37:33 PDT

Though the relation of the AP article (RISKS 11.45) to computer risks
does seem rather tenuous, I think a clarifying response might be useful:

Measuring and reporting average life-expectancies (by computer-based methods or
otherwise), or changes in them resulting from changes in society, has high
potential to mislead. People tend to think of average life expectancy as
indicating how old an individual in a given society can expect to get. In fact
the "expectancy" referred to is a statistical expectancy that probably doesn't
jibe with most peoples' notion of "life expectancy". The impact upon this
number of eliminating a particular cause of death depends as much on the age of
the people killed as on the number of them killed.

For example, the average life expectancy in Nepal is approximately 45 years.
That seems very low by our standards. However, when you go there (as I have),

you will find many old people; much more than you might expect from the above figure. The reason for the discrepancy is that one third of all Nepalese die before they are five years old. Those who survive past five have a life expectancy probably not much lower than that seen in many poor U.S. communities. The high infant/child mortality rate pulls the average expected lifespan down very low. Nepalese adults want and need offspring to support them in their old age (this is the only form of social security they have), so they generate lots of them, expecting many to die.

Simply targetting diseases that kill large numbers of people won't necessarily affect average life expectancy much, especially if the deaths being eliminated are primarily deaths of older people. The way to have a large impact on statistical life expectancy is to target major causes of death in children. The AP article quoted in RISKS (11.45) focuses on the "nation's leading killer": heart disease. I assume that the risk of death from heart disease in our society increases with age, making it mainly a disease of adults (maybe even mainly of seniors). If raising statistical life expectancy is our goal, we'd get more bang for our buck focussing on sources of infant and child mortality, expecially where they are now highest.

Of course, raising statistical life expectancy may not be our goal. Instead, we may be trying to increase the longevity of those who survive to adulthood. This is the meaning of "life expectancy" that people have in mind when they tell one another how long people in their respective families tend to live: only deaths by "old age" count here; "early" deaths by accident and disease are ignored.

JJ, HP Labs, Palo Alto

Re: Euro Update

Rob Kling <kling@ICS.UCI.EDU>
Mon, 15 Apr 91 19:11:10 -0700

Some colleagues in Western Europe and Australia have asked us how to obtain copies of the anthology Computerization and Controversy: Value Conflicts and Social Choices (Charles Dunlop & Rob Kling, eds). This note provides information about ways to obtain the book outside of North America.

Computerization and Controversy introduces some of the major social controversies surrounding the computerization of society through over 50 articles. It highlights various key value conflicts and emphasizes a wide variety of social choices posed by computerization. It helps readers to recognize social processes that drive and shape computerization, and to understand the paradoxes and ironies of computerization. It is divided into seven major section; each section begins with an analytical introduction which identfies key controversies, frames the selections, and discusses other litertaure as well.

To obtain Computerization & Controversy outside of North America, please contact your local Academic Press/Harcourt Brace Jovanovich office, including:

Harcourt Brace Jovanovich, Ltd (Western Europe and UK),
24-28 Oval Rd., London NW1 7DX U.K.
Telephone: 44-71-267-4466 Fax: 44-71-482-2293 Telex: 25775 ACPRESS G
Cable: ACADINC LONDON NW1

Harcourt Brace Jovanovich Group Pty, Ltd (Australia/New Zealand)
Locked bag 16, Marrickville, NSW 2204 Australia
Telephone: (01) 517-8999 Fax: (02) 517-2249

Individuals in North America may purchase copies directly from Academic Press by calling 1-800-321-5068, faxing to 800-235-0256 or by writing to:

Academic Press Ordering, Academic Press Warehouse, Order Dept.
465 S. Lincoln, Troy, Missouri 63379

Computerization and Controversy is a 758 page paperback and sells for $34.95 in US$ in the US and Canada. Prices in other parts of the world may differ slightly.

Faculty who offer related courses (Values and Technology; Applied Ethics; Computers & Society; Information Systems and Behavior, etc.) may order examination copies from Academic Press. Write on university letterhead, and include the following information about your course: class name and number, department, # of students, books used --in the past, adoption deadline.

Send your requests for examination copies in the US or Canada to:

Amy Yodannis, College and Commercial Sales Supervisor
Academic Press, 1250 Sixth Avenue, San Diego, CA 92101
tel: 619-699-6547 fax: 619-699-6715

If you wish a review copy outside of North America, please contact your local Harcourt Brace Jovanovich office. If you have trouble obtaining a review copy for a legitimate course of journal, please contact Rob Kling at UC-Irvine (kling@ics.uci.edu).

Search RISKS using swish-e

Report problems with the web pages to the maintainer

Search RISKS using swish-e

THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

ACM Committee on Computers and Public Policy, Peter G. Neumann, moderator

Volume 11: Issue 48

Thursday 18 April 1991

Contents

US Gov't is not careful with its supplies

Garrett Wollman <wollman@emily.UVM.EDU>
Wed, 17 Apr 91 7:58:13 GMT-6:40

[Related to me by my father, who works for the Federal Courts. -GW]

On Monday, April 15, a truck containing thousands of dollars worth of US Government forms, stationery, and supplies (250 line-items, as it happened) was delivered to the US District Court in Burlington, Vt. At about the same time, five small items ordered by the court were delivered to the US Mint in San Francisco. Neither office got what it needed--"did you say *six* paper cutters?"

How did this happen? It turned out, on further investigation, that there is a very large flaw in the computerized ordering system the General Services Administration uses for Government offices to enter their supply orders. When logging in, the user is required to enter a location code and a password.

However, it seems that the program *never bothered to check* whether the password (which was, of course, valid) corresponded to the location code that was entered. Thus, anyone who has access to this system could literally cause millions of dollars of equipment to be shipped--and billed--to another agency which doesn't need or want it, without anyone being the wiser until the trucks pull in.

The cause of our error? A single letter in the location code was changed from 'c' to 'd'.

Garrett A. Wollman - wollman@emily.uvm.edu

Trap doors and such

Jerry Leichter <leichter@lrw.com>
Wed, 17 Apr 91 12:23:34 EDT

Bill Murray dislikes my claim that S. 266 would not require "trap doors", and goes on to long philosophical discussions of whether one should trust the government.

Let's try and keep the issues separate.

a) The phrase "trap door", as used in computer science, has a fairly specific referent: It is a technique for getting around a security provision in a system, inserted into that system by its designers, of which the user of the system is generally unaware.

   A cryptographic system based on a central authority that issues keys does NOT have a trap door. It is plain to every user of the system that the issuing authority has access to the key.

   Beyond the difference in knowledge, there is another quite significant distinction: A trap door is a general mechanism. Knowledge of the trap door may leak out, or an outside party may discover the trap door on its own. Once that knowledge is out, ALL users of the system have been compromised. This makes a trap door an extremely dangerous thing to have in a cryptosystem.

   On the other hand, compromise of a given user's key by the central authority only compromises that given user's security. Yes, the central authority adds one additional place for compromise to occur. However, there is no analog in this setup to a third party finding the trap door: The only thing he can do is find the key, i.e., make a traditional attack on the cryptosystem.

b) There is a difference between the government HAVING THE CAPABILITY to decrypt your private mail, and its actually

choosing to do so. The government today has the capability to tap your phone, intercept your mail, plant bugs in your office, and so on. Your ONLY protection from such actions (and it's certainly a protection that has at many times proved insufficient) are the legal limitations on what the government may do.

c) As a result of (b), I'll repeat: Truly strong widely-available cryptosystems would provide a capability that no one in history has ever really had: The ability to shield communications and records in a way that the government cannot get around, whether or not it is bound by law.

Whether, on balance, we wish to provide a capability as in (c) is worth debating. There are strong arguments on both sides. But a rational debate on these issues isn't possible unless we begin by being clear about what the choices actually are.

-- Jerry

Re: S. 266

<smb@ulysses.att.com>
Wed, 17 Apr 91 14:17:17 EDT

I think we should separate any discussion of S. 266 from discussion of the secure telephone units (STU-III) that NSA is willing to let its friends buy. Paranoia aside, there are sound technical reasons, or at least justifications, for some of the decisions made by NSA (there -- I've uttered the Name) in the design of the new cryptogear. And there are reasons to doubt that NSA has quite as much control of the key space as has been portrayed; if there's a trapdoor, it's more subtle. I'll try to explain what little I know without straying into material more suited to sci.crypt.

I should preface my comments with a few disclaimers. First, I don't really know that much about what I'm talking about; I've never had (and don't want) any sort of security clearance. Second, very little about this system has been disclosed to the public. For the most part, those who do know something aren't talking, even if they are reading this. (And some probably are reading RISKS, often quite legitimately. The parent organization of NCSC is not classified information....) For the most part, my information about the secure phones comes from Diffie's paper ``The First Ten Years of Public Key Cryptography'', Proc. IEEE 76,5, May, 1988; other information comes from Aviation Week, June 2, 1986 and Feb 27, 1989.

There is little doubt that public-key technology is used for key distribution. Among other useful properties, this means that the actual session keys are generated randomly by the STU-IIIs themselves, for each conversation, and no permanent record of them exists. NSA's key distribution center is manifestly not involved in supplying such keys. Rather, its role appears to be limited to issuing and renewing the public-key certificates used for authentication, as opposed to secrecy. They certainly could issue themselves bogus certificates to allow them to impersonate any user, but that's a different issue entirely.

(The KDC might be involved in authorizing pairs of individuals to talk; I'm not sure. I'd welcome any (public) information on that topic. A revoked certificate list is definitely maintained by the KDC; some references indicate that this list is consulted on every call, though that seems unwieldy.)

Next, it strikes me as highly improbable that the actual encryption algorithm used contains trap doors. That's just too big a risk to take. Those phones, in some versions, are rated for top-secret traffic; NSA cannot assume that its opponents (whomever they may be) are incompetent cryptanalysts. Nor would they take the risk that one defection could blow the entire secure phone network. If there is a back door, I'd speculate (note: *speculate*) that it's more along the lines of the ``key-or'' techniques discussed by Gifford in ``Cryptographic Sealing for Information Secrecy and Authentication'' (CACM 25,4, April 1982), or perhaps Shamir's multipart keys (``How to Share a Secret'', CACM 22,11, November 1979).

Furthermore, there are often valid technical reasons for a restricted key space. DES itself has a handful of weak and semi-weak keys. Historically, the M-209 cipher machine used by the U.S. Army during World War II had a number of restrictions on key selection. (``Cipher Systems'', Beker and Piper.) These restrictions are often inherent in the design of an otherwise-excellent cryptosystem. Again, I'll use DES as an example. The first step in employing DES is to expand the 56-bit key into a ``key schedule'' of 16 48-bit subkeys. The key schedule only has 56 bits of information; an obvious way to try to strengthen DES is to let the user specify all 768 bits. Remarkably enough, that doesn't work nearly as well as might be expected -- among other things, Biham and Shamir (Crypto '90, I think) showed that that variant of DES was only slightly stronger than the standard version. And you'd likely lose other valuable properties, such as independence of the key bits. In DES, if you flip one key bit, you'll (statistically) invert half of the output bits for a given plaintext. I doubt that that's true if you change individual subkey bits.

Incidentally, it also seems apparent now that NSA actually strengthened DES against outside attacks. While they may have buried a trap door in the S-boxes, they also produced one that's very resistant to the Biham-Shamir attack. Regardless of whether or not they can now crack DES (and there's some reason to think that they can, even if they couldn't 15 years ago), they did do a credible job of helping folks protect their secrets from other opponents.

If the equipment is really as good as I say it is, why do I think NSA runs the KDC? Simply because the equipment really is that good, and they want to make sure that only their friends have that quality of encryption gear. NSA, as an organization, has at several different goals: protecting U.S. confidential information, reading foreign traffic, and -- maybe -- reading as much domestic traffic as they can. While deploying weak cryptosystems furthers the latter two goals, it directly conflicts with the first. They won't give up that mission lightly.

To summarize, while there's ample reason to be suspicious of NSA's motives, either in general or with respect to S.266 or the secure phones, I don't think the evidence presented supports the conclusions drawn. (Of course, there's always Nixon's Law: just because you're paranoid doesn't mean they aren't out to get you....)

--Steve Bellovin

Re: S. 266

<WHMurray@DOCKMASTER.NCSC.MIL>
Wed, 17 Apr 91 14:44 EDT

>I think we should separate any discussion of S. 266 from discussion of the
>secure telephone units (STU-III) that NSA is willing to let its friends buy.

Steve, okay. I am not sure that they are not related, but I will agree to the separation for sake of orderly argument.

However, if you are thinking of Jerry Leichter's posting to RISKS and my response, we did not have STU-III in mind. We were talking about a different proposal; one that was proposed as a replacement for the DES in commercial data applications. While it had many of the same properties, and may have shared some origins, it was different.

William Hugh Murray, Information System Security, Consultant to Deloitte & Touche Wilton, Connecticut 203-966-4769

Re: S. 266

<WHMurray@DOCKMASTER.NCSC.MIL>
Wed, 17 Apr 91 14:58 EDT

Steve, my original reply stands. We were not talking about STU-III and your new reply, if anything is more restricted to that than the original. I think that there may be some small errors in your response, and I think that you insert some discussion that is not relevant to Jerry's point or my rebuttal. However, I am not moved to a response.

William Hugh Murray

[WHMurray: Status of S. 266]

Brinton Cooper <abc@BRL.MIL>
Mon, 15 Apr 91 22:44:09 EDT

NO! NO! Mr Biden of DELAWARE, Please!!! [not Maryland]

On Toffler

Rob Kling <kling@ics.uci.edu>
Thu, 18 Apr 91 09:24:16 -0700

I just saw an enthusiastic posting about Alvin Toffler's books "Future Shock" and "The Third Wave" on RISKS. Toffler's a provocative and popular journalist. But I recommend that readers of RISKS read him VERY critically. Toffler's Third

Wave is a technologically utopian treatise whose assumptions undermine the kinds of social realism which are essential commentaries on RISKS. In Toffler's Third Wave, there would be no need for a RISKS!

I see some value to utopian and anti-utopian analyses. But technological utopianism is so seductive to technologists, and dangerous (IMHO), that we should be aware of how its rhetoric "works."

I've written about the character of technological utopianism, anti-utopianism, and social realism as genres of analysis which give selective insight into issues of computerization, but which also have important systematic limitations, in:

> "Reading 'All About' Computerization: Five Common Genres of Social Analysis" in Directions in Advanced Computer Systems, 1990 Doug Schuler (Ed.). Norwood, NJ:Ablex Pub. Co. (in press) and

my new book,

> "Computerization and Controversy: Value Conflicts and Social Choices" (co-edited with Chuck Dunlop). (Academic Press, 1991).

I'm attaching a commentary Toffler's "The Third Wave" from "Computerization and Controversy." The following paragraphs are from the introduction to a section I, which examines Technological Utopianism and Technological Anti-Utopianism.

> ==========

Alvin Toffler's best seller, The Third Wave, helped stimulate popular enthusiasm for computerization. Toffler characterized major social transformations in terms of large shifts in the organization of society, driven by technological change. The "Second Wave" was the shift from agricultural societies to industrial societies. Toffler contrasts industrial ways of organizing societies to new social trends that he links to computer and microelectronic technologies. He is masterful employing succinct breathless prose to suggest major social changes. He also invented terminology to help characterize some of these social changes -- terms like "second wave", "third wave", "electronic cottage", "infosphere", "technosphere", "prosumer", "intelligent environment", etc. Many of Toffler's new terms did not become commonly accepted. Even so, they help frame a seductive description of social change. These lines from his chapter, "The Intelligent Environment" illustrate his approach. (Toffler devoted ONLY ONE PARAGRAPH in his chapter to possible problems of computerization.)

> Today, as we construct a new info-sphere for a Third Wave civilization, we are imparting to the "dead" environment around us, not life, but intelligence. A key to this revolutionary advances, of course, the computer (Toffler, 1980:168) . . . .
>
> As miniaturization advanced with lightning rapidity, as computer capacity soared and prices per function plunged,

> small cheap powerful minicomputers began to sprout everywhere. Every branch factory, laboratory, sales office, or engineering department claimed its own . . . . The brainpower of the computer . . . was "distributed." This dispersion of computer intelligence is now moving ahead at high speed (Toffler, 1980:169).
>
> The dispersal of computers in the home, not to mention their interconnection in ramified networks, represents another advance in the construction of an intelligent environment. Yet even this is not all. The spread of machine intelligence reaches another level altogether with the arrival of microprocessors and microcomputers, those tiny chips of congealed intelligence that are about to become a part, it seems, of nearly all the things we make and use . . . . (Toffler, 1980:170)
>
> What is inescapably clear, however, whatever we choose to believe, is that we are altering our infosphere fundamentally . . . we are adding a whole new strata of communication to the social system. The emerging Third Wave infosphere makes that of the Second Wave era -- dominated by its mass media, the post office, and the telephone -- seem hopelessly primitive by contrast. . . . (Toffler, 1980:172)
> In all previous societies, the infosphere provided the means for communication between human beings. The Third Wave multiplies these means. But it also provides powerful facilities, for the first time in history, for machine-to-machine communication, and, even more astonishing, for conversation between humans and the intelligent environment around them. When we stand back and look at the larger picture, it becomes clear that the revolution in the infosphere is at least as dramatic as that of the technosphere -- in the energy system and the technological base of society. The work of constructing a new civilization is racing forward on many levels at once. (Toffler, 1980:177--178).
> [(pages from paperback edition of 1980].

Toffler's breathless enthusiasm can be contagious -- but it also stymies critical thought. He illustrates changes in the infosphere with The Source -- a large commercial computer-communication and messaging system which has thousands of individual and corporate subscribers. (Today, he could multiply that example with the emergence of competing commercial systems, such as CompuServe, Genie, and Prodigy, as well as tens of thousands of inexpensive computerized bulletin boards that people have set up in hundreds of cities and towns.) However, there have been a myriad of other changes in the information environment in the United States which are not quite as exciting to people who would like to see a more thoughtful culture.

For example, television has become a a major source of information about world events for many children and adults. (Many children and adults report that they watch television for well over 5 hours a day.) Television news, the most popular "factual" kind of television programming, slices stories into

salami-thin 30 to 90-second segments. Moreover, there is some evidence that functional illiteracy is rising in the United States (Kozol, 1985). The problems of literacy in the United States are probably not a byproduct of television's popularity. But it is hard to take Toffler's optimistic account seriously when a large fraction of the population has trouble understanding key parts of the instruction manuals for automobiles and for commonplace home appliances, like televisions, VCRs, and microwave ovens.

Toffler opens up important questions about the way that information technologies alter the ways that people perceive information, the kinds of information they can get easily, and how they handle the information they get. Yet his account -- like many popular accounts -- caricatures the answers by using only illustrations that support his generally buoyant theses. And he skillfully sidesteps tough questions while creating excitement (e.g., "The work of constructing a new civilization is racing forward on many levels at once.").

==========

Utopian images permeate the literatures about computerization in society. Unfortunately, we have found that many utopian writers distort social situations to fit their preferences ..... We are not critical of utopian ideals concerned with a good life for all. The United States was founded on premises that were utopian premises in the 1700s. The Declaration of Independence asserts that "all men are created equal" and that they would be guaranteed the right to "life, liberty, and the pursuit of happiness".

Although utopian visions often serve important roles in stimulating hope and giving people a positive sense of direction, they can mislead when their architects exaggerate the likelihood of easy and desirable social changes. We are particularly interested in what can be learned, and how we can be misled, by a particular brand of utopian thought -- technological utopianism. This line of analysis places the use of some specific technology -- computers, nuclear energy, or low-energy low-impact technologies -- as the central enabling element of a utopian vision. Sometimes people will casually refer to exotic technologies -- like pocket computers that understand spoken language -- as "utopian gadgets." Technological utopianism does not refer to a set of technologies. It refers to analyses in which the use of specific technologies plays a key role in shaping a utopian social vision. In contrast, technological anti-utopianism examines how certain broad families of technology facilitate a social order that is relentlessly harsh, destructive, and miserable.

[From Introduction to Section I of Computerization and Controversy: Value Conflicts and Social Choices Charles Dunlop and Rob Kling (Editors). Academic Press, Boston, 1991.]

Rob Kling, Information & Computer Science, University of California - Irvine

---

Simulation: Minus heart disease, etc...

Gregory G. Woodbury <ggw@wolves.uucp>
Thu, 18 Apr 1991 02:15:45 GMT

>From: [anonymous]
>
>New Heart Disease Study Issued
> BOSTON (AP) [14 Apr 91]
> Completely eliminating heart disease, the nation's leading killer, would
>increase the average 35-year-old American's life span by just three years, a
>new study concludes.
:
> [What are the computer-related risks, you ask? Here are people using
> computer models to yield results that could have drastic impact on health
> care and research funding...]
>
> [But the results may be quite sound... On the other hand, the elimination
> of heart disease would undoubtably have many concomitant effects, which
> overall probably could dramatically increase longevity. PGN]

As System Programmer for one of the leading competitors to the program cited in the Circulation article I would like to comment on the AP article and the problems that the general press has with statistics.

The readers of RISKS (I am sure) are aware of the difference between the median and the mean. The popular press is much less prone to keep the fine distinction in mind when writing.

We have a set of programs that allow us to deal with similar public health interventions and the resulting population shifts (I think that our population stuff is unique). Both their program and our program create actuarial "life tables" which trace a group of individuals over time and calculate various statistics on the basis of mathematical models.

Briefly, our results tend to agree with theirs in most categories. The main thing to note, though, is that the shift of three years or so is in median expectation of life! Not the mean life expectancy at the starting age. What this means is that the projections are ONLY useable for populations and mean nothing applied to individuals.

It is interesting to note that this "insignificant" gain in median life expectancy produces a dramatic change in the population pyramid in the future. For example, in a paper to be published in one of the gerontological journals, we are showing results that are more than twice as large for males and females over age 65 in the year 2060 than the census bureau "high" figures.

All the details (of course) are at the office right now (and I'm at home).

The RISKs are even more striking when one knows what use these models are being put to for future policy making. Our models are used by NIA(NIH) and WHO(UN) in providing information about future population structures here and abroad. The models get more and more complex and draw on larger and larger data sets, and (I suspect) that we run on the verge of some kind of chaotic condition where the results are wildly sensitive to input conditions. We DO do some checking for non-chaotic behaviour in the models, but there could be some places in the function space that are chaotic that we have not seen.

Other models that I help program and compute on my work network are used in other fields of medical economics (like HCFA (medicare) and SS) to project and analyze the results of the Medicare Prospective Payment System and the Diagnosis Related Groups (DRGs) for budget projections and changes in the systems.

Certainly, my office is NOT the only think tank that advises HCFA and NIA and WHO, but ALL of the advising grantees and contractors use computer modelling with varying degrees of sophistication. From simple LOTUS-1-2-3 and Excell spreadsheets on DOS micros, to large scale economic models running on supercomputers, computing power underlies all of modern economic medical planning.

Gregory G. Woodbury @ The Wolves Den UNIX, Durham NC ggw%wolves@mcnc.mcnc.org
UUCP: ...dukcds!wolves!ggw ...mcnc!wolves!ggw

CERT Advisory - Social Engineering

CERT Advisory <cert-advisory-request@cert.sei.cmu.edu>
Thu, 18 Apr 91 16:57:35 EDT

CA-91:04 CERT Advisory
April 18, 1991
Social Engineering

DESCRIPTION:

The Computer Emergency Response Team/Coordination Center (CERT/CC) has received several incident reports concerning users receiving requests to take an action that results in the capturing of their password. The request could come in the form of an e-mail message, a broadcast, or a telephone call. The latest ploy instructs the user to run a "test" program, previously installed by the intruder, which will prompt the user for his or her password. When the user executes the program, the user's name and password are e-mailed to a remote site. We are including an example message at the end of this advisory.

These messages can appear to be from a site administrator or root. In reality, they may have been sent by an individual at a remote site, who is trying to gain access or additional access to the local machine via the user's account.

While this advisory may seem very trivial to some experienced users, the fact remains that MANY users have fallen for these tricks (refer to CERT Advisory CA-91:03).

IMPACT:

An intruder can gain access to a system through the unauthorized use of the (possibly privileged) accounts whose passwords have been compromised. This problem could affect all systems, not just UNIX systems or systems on the Internet.

SOLUTION:

The CERT/CC recommends the following actions:

1) Any users receiving such a request should verify its authenticity with their system administrator before acting on the instructions within the message. If a user has received this type of request and actually entered a password, he/she should immediately change his/her password to a new one and alert the system administrator.

2) System administrators should check with their user communities to ensure that no user has followed the instructions in such a message. Further, the system should be carefully examined for damage or changes that the intruder may have caused. We also ask that you contact the CERT/CC.

3) The CERT/CC urges system administrators to educate their users so that they will not fall prey to such tricks.

SAMPLE MESSAGE as received by the CERT (including spelling errors, etc.)

> OmniCore is experimenting in online - high resolution graphics
> display on the UNIX BSD 4.3 system and it's derivitaves [sic]. But, we
> need you're help in testing our new product - TurboTetris.
> So, if you are not to busy, please try out the ttetris game in your
> machine's /tmp directory. just type:
>
> /tmp/ttetris
>
> Because of the graphics handling and screen-reinitialazation [sic], you
> will be prompted to log on again. Please do so, and use your real password.
> Thanks you for your support. You'll be hearing from us soon!
>
> OmniCore

END OF SAMPLE MESSAGE

If you believe that your system has been compromised, contact CERT/CC via telephone or e-mail.

Computer Emergency Response Team/Coordination Center (CERT/CC), Software Engineering Institute, Carnegie Mellon University, Pittsburgh, PA 15213-3890

412-268-7090 24-hour hotline: CERT/CC personnel answer 7:30a.m.-6:00p.m. EST, on call for emergencies during other hours. E-mail: cert@cert.sei.cmu.edu

Past advisories and other computer security related information are available for anonymous ftp from the cert.sei.cmu.edu (128.237.253.5) system.

> [Don't forget Tom Lehrer's "Don't write naughty words
> on walls that you can't spell. "sic"s added by PGN]

Search RISKS using swish-e

Report problems with the web pages to the maintainer

Search RISKS using swish-e

THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

ACM Committee on Computers and Public Policy, Peter G. Neumann, moderator

Volume 11: Issue 49

Friday 19 April 1991

Contents

University library security, or lack thereof...

Marc Andreessen <andreess@mrlaxs.mrl.uiuc.edu>
Thu, 18 Apr 91 20:33:19 -0500

At the risk of taking space away from the very interesting current threads in

RISKS, I'd like to relate a very interesting administrative procedure practiced at the University of Illinois.

The U of I library, like most other university libraries, is completely computerized; terminals in each of the three-dozen departmental libraries, as well as other terminals in residence halls and a dedicated telnet port on one of the university's Unix systems, allow anyone to browse through the 12-million-book collection AND check out any available book.

Now, this is mighty convenient for us busy students and researchers. Unfortunately, this is also security-free. From a terminal or telnet connection, one can check out a book merely by giving one's university ID number (which, at Illinois, is always one's SSN). Then, one can go to the appropriate central or departmental library (where library staff regularly retrieve books from the stacks to match computer charge requests) and say something like ``I charged out a book called _The Adventures of Foobar the Dancing Bear_ a couple of hours ago,'' upon which the librarian will cheerfully hand you the book in question WITHOUT CHECKING YOUR ID, since the charge has already been processed by the central computer.

Obviously one is free to use whomever's ID (aka SSN) one pleases. (Incidentally, when I checked out a book this afternoon from our Engineering Library, the librarian had the book in hand when he suddenly looked at me suspiciously and asked, ``What's your ID number?'' I rattled it off. He checked it against the computer printout and, satisfied, gave me the book.) Of course, the minimum fine for a nonreturned book is $50, which - like an overdue fine - is automatically billed to one's Student Accounts Receivable.

Marc

Marc Andreessen_____University of Illinois Materials Research Laboratory
Internet: andreessen@uimrl7.mrl.uiuc.edu_____Bitnet: andreessen@uiucmrl

---

U.S. Senate 266, Section 2201 (cryptographics) (RISKS-11.43)

A. Padgett Peterson <padgett%tccslr.dnet@uvs1.orl.mmc.com>
Fri, 19 Apr 91 11:05:53 -0400

Bill Murray writes:

>The referenced language requires that manufacturers build trap-doors
>into all cryptographic equipment...

While the language appears to provide access to law enforcement agencies, the effect will be to simply drive all US manufacturers out of the crypto business. The reason people and companies buy secure communications equipment if for secure communications. The reason they buy a particular manufacturer's device is because it satisfys the requirement (quantum) and is at the lowest available overall cost (linear) or provides some other advantage (may be either). If the quantum requirement is not met by one device/method, another will be chosen (in this case, none is a choice).

DES became a standard because it was considered to be adequate and devices

using it were cost-effective and fast. Should such a bill pass, the market will simply turn to other solutions. PCs make alternatives easy and a true code could be considerably more difficult to break than the DES.

Padgett

Trap doors and such (Leichter, RISKS-11.48)

Robert Hartman <rhartman@thestepchild.sgi.com>
Fri, 19 Apr 91 20:05:02 GMT

Actually, I don't think there's anything to debate. If it is technically possible to create cryptographic systems that a government cannot break, people will create them and people will use them. Governments most of all.

A government can only slow the process by which they become more widely used.

Senate 266; Personal Privacy

Rob Boudrie <rboudrie@encore.com>
Fri, 19 Apr 91 14:29:49 EDT

Although US citizens have a right against self incrimination, it is unlikely that this right extends to withholding cryptographic keys encoding potentially embarassing or incriminating information. The courts would likely hold that you can be forced (under threat of being jailed for contempt of court) to disclose the keys to your files, much the same way you can be compelled to produce possibly embarrassing or incriminating paper files without violating the right of protection against self incrimination.

So what is the concerned individual or business to do?

Establish a well documented, and publicized, policy of encoding numerous "dummmy files" (perhaps using man pages as source text) using your standard encryption algorithm, with random keys which are not recorded. This will produce a *DOCUMENTED SITUATION* in which you are not able to product decryption keys for the majority of your files, even if you wanted to.

[Of course you'd better check with your attorney first - any action designed to make it more difficult to penetrate your veil of privacy may be illegal.]

Rob Boudrie rboudrie@encore.com

S. 266 Query

"David A. Honig" <honig@ics.uci.edu>
Thu, 18 Apr 91 18:24:54 -0700

Suppose that the strongest sense of the bill were law: no one could sell

crypto equipment that the government couldn't crack. Ok, the government regulates trade, so they can do this.

But could they prevent public-domain sharing of code that accomplishes the same? It would seem that sharing information freely is protected by the constitution. Shareware couldn't be construed as "obscene", even in the most backwards parts of the Carolinas...

Would the "national interest" cries be listened to, even though the Soviets (or Panamanians or Iraqis or dope capitalists or whoever) surely are aware of superior, if expensive, encryption methods (eg, 100 bit DES or 1000 bit RSA)??

S. 266

David Chase <David.Chase@eng.sun.com>
Fri, 19 Apr 91 12:24:02 PDT

I'm a little curious if there will be any point to this bill at all in a few years. It burdens the service and equipment providers with the reponsibility of permitting the government access to the plain text, but that seems to leave a gaping hole between the modem and my fingers and mouth. Is my Amiga/Macintosh/Next/PC/Sun "electronic communications equipment"?

A few notes that might be relevant here -- the basic patent on RSA encryption must be running out in a few years, because they published their method in April 1977. Seventeen years from then is April, 1994 (plus one for the US patent grace period is 1995). The most recent issue of _Computer Architecture News_ (March, 1991) contains an article describing a 200Kbit/second, 512 bit key, RSA encryption and decryption implementation (the implementation used three "Programmable Active Memory" boards). One can only assume that the hardware required to implement this will get cheaper in the future.

Public key encryption also has the delightful property that the sender need not know how to decrypt the message sent; you can hand all your keys and equipment to the Authorities, and the most that they can do is spoof your messages. Sounds to me like the horse is out of the barn and long gone.

David Chase, Sun

Re: Accident statistics continued (Smee, RISKS-11.45)

Mike Jones <mjones@fenway.aix.kingston.ibm.com>
Fri, 19 Apr 91 14:12:02 -0400

There is a risk here which is facilitated but not caused by computers. This study appears to be prone to the "Seduction of the Innocent" fallacy. This book, written by one Dr. Frederic Wertham in the 1950's, propounded comic books as the root of all evil based on the high correlation between juvenile delinquency and comic books - i.e., about 95% of J.D.'s read comic books. The omitted information was that about 95% of *all* young people read comic books at the time. I wonder, in this survey, whether the items quoted above

mean that drivers who described themselves as above average are more likely to have accidents, or that drivers who have many accidents are more likely to describe themselves as above average - the relationship is *not* commutative!

Mike Jones, AIX Development, Kingston, NY ibmps2!aix!mjones

Re: Re: Simulation: Minus heart disease (Cooper, RISKS-11.47)

David Lamb <dalamb@avi.umiacs.umd.edu>
17 Apr 91 13:44:21 GMT

An interesting point; increasing speed can increase the risk of not thinking about what you're doing. I've heard at least one netflamer say he'd like to have an option on his mail that automatically delayed sending it for a few hours, then asked him if he'd really still like to send it. There's an old science fiction short story by Cyril Kornbluth (possibly co-authored; my collection is 500 miles away) called something like "Education among the Camiroi", where one of the educators' goals was to *reduce* students' reading speeds, so they'd get better comprehension of the material.

David Alex Lamb internet: dalamb@umiacs.umd.edu

YABCWS (Yet Another Boy Crying Wolf Story)

Joe Morris <jcmorris@mwunix.mitre.org>
Fri, 19 Apr 91 16:11:46 EDT

With all of the complaints RISKers have about systems which can acquire data about users' financial situation without telling the customer, we need to remember that the notifications sent by a properly-designed system must be both timely and correct. This morning's mail included an example of a notice which fails the test.

I've had an American Express card for several years; the only basic change which has been made to the account in this time has been an address change eight years ago, and an *involuntary* change in the bank which services the Express Cash feature. This bank change occurred last June (ten months ago) because the original bank no longer participated in the program. Without offering other options AX reassigned the account to its internal bank (American Express Centurian Bank).

The notice I received this morning was a prepackaged self-mailer; the note inside had a check against the box which said "[This is a] confirmation of the change you requested in your enrollment in the Express Cash program." It did not say what that change was; it didn't even have a place for that data.

Since I hadn't asked for any changes I called AX at the number on the notice (bonus points to AX for printing the WATS number). After talking to six people and listening to the usual elevator music, I was told that:

(1) the notice was generated because someone at Centurian had changed the routing symbol used in processing bank transactions,

(2) I should ignore the notice, and

(3) I was being very unreasonable in complaining about being sent a spurious notice that an unrequested change had been made in my account.

Clearly someone's program is generating this mailer if *any* of the base account information block changes, even if the change originated completely within the vendor, and the change was in internal control information.

AX deserves credit for trying to notify its customers of changes made to their accounts, but the outright hostility I encountered in trying to chase down the reason for the notice worries me.

The law, in both the US and elsewhere, seems to be moving in a direction which places significant liability on credit vendors for damages (real or imagined) caused by bad data. (Not far enough IMHO.) Over the years RISKers and other professionals have expressed concern about the posting of incorrect, misleading, out-of-date, or just plain fraudulent information in customer credit files. I suggest that at the same time that we push the issue of making sure that the customer knows what has been put into the data base that we need to strongly pressure vendors not to play the central character in the old fable of the boy who cried "WOLF".

Joe Morris

Consumer Privacy article: Consumer's Reports, May 1991

<JONB@FAIR1.BITNET>
Fri, 19 Apr 91 10:04 EST

In the latest issue of Consumer's Reports (May '91, pp 356-60), there is an excellent article on the consumer credit databases on what appears to be 90% of adults in this country. These databases are regularly shared or sold to targeting advertisers, or referenced during loan/credit card/insurance applications. There are statistics on errors, examples of damaging mistakes, and addresses for contacting to minimize the availability of your files.

For instance, to get a copy of your file that insurance companies and doctors seem to be able to reference upon request, write to the Medical Information Bureau, P.O. Box 105, Essex Station, Boston, Mass 02112. The information provided may not be anything interesting or damaging (or legible, for that matter) but can stop you from getting insurance for seemingly unapplicable reasons.

To get a copy of your "credit rating information" you must write to all three of the major credit bureaus. The report you receive will contain mistakes and none of the reports from the three of them will match. Furthermore, they will all be impossible to understand. Write to:

Eqifax

P. O. Box 4081
Atlanta, GA, 30302
(404) 885 8000

Trans Union
East: P.O. Box 360
Phillie, PA 19105
(215) 569 4582
Midwest:Consumer Relations
222 S First St, Suite 201
Louisville, KY 40202
(502) 584 0121
West: P.O. Box 3110
Fullerton, CA 92634
(714) 738 3800

TRW Credit Data
National Consumer Relations Center
12606 Greenville Ave
P.O. Box 749029
Dallas, TX 75374-9029
(214) 235 1200 x251

To reduce the number of legitimate direct mail marketing you receive, by making your database unavailable (to the scrupulous), write to:
Direct Marketing Assn
11 W 42 St
P.O. Box 3861
New York, NY 10163-3861

As an aside, the book seems to indicate that these places don't make it easy, since they have no problems when your database is incorrect. If you stick you nose out, they might start giving you a hard time. Good way to ensure that everyone remains a sheep, I think.

A book is recommended called "Privacy in America" by David F Linowes, by University of Illinois Press.

Jon

Re: automated car parking? (RISKS 11.47)

Stephen R. Smoot <smoot@postgres.Berkeley.EDU>
Tue, 16 Apr 91 18:50:07 -0700

In RISKS 11.47, alayne@geas.gandalf.ca (Alayne McGregor) writes:
> The representative said the car is a test prototype built by Volkswagen of
> America. It can sense whether a parking space is large enough, and place itself
> in the spot with only inches to spare on either side. The driver does not need
> to be in the car.

Adding a not-so-new, but increased, RISK of being the poor person whose old-fashioned car becames sandwiched between two new Volkswagen's which can

park "with only inches to spare."

And even worse, their fate as the cars become more and more common, causing city planners to decrease the size of parking spaces. Which makes the situation even more likely...

Re: automated car parking?

Louis Koziarz <lnk10562@uxa.cso.uiuc.edu>
Wed, 17 Apr 91 00:22:47 -0500

>The representative said the car is a test prototype built by Volkswagen of
>America. It can sense whether a parking space is large enough, and place itself
>in the spot with only inches to spare on either side. The driver does not need
^^^^^^^^^^^^^^^

Gee, that's nice. So you can park in relative peace and come back to find the guy with the beater in front of you has repeatedly bashed in your front bumper trying to get out. Thanks, but no thanks...

Louis Koziarz University of Illinois Urbana/Champaign koziarz@uiuc.edu

---

Re: automated car parking?

Brian Smithson <brian@motcsd.csd.mot.com>
18 Apr 91 02:47:30 GMT

I saw a similar demonstration of a prototype from another manufacturer (can't remember which) on Motorweek '91 (PBS).

>I wonder who would be liable if the car software bashed the next car while
>parking, or if it ran over a cat, dog, or child on its approach. One would
>think the location and range of the sensors would be very important.

This one has, as I suspect the VW does too, four wheel steering. Four wheel steering allows the car to be parked with very little space between it and the adjacent cars. What I wondered was how the poor sap behind or in front of such a car would get out? Suppose someone puts their brand new '96 VW in front of my '72 Galaxie and leaves me 2 inches of clearance. I wouldn't be worried about the *software* causing some dents! :-)

Brian Smithson, Motorola Inc., Commercial Systems Division, 10700 N.DeAnza Blvd
Cupertino, CA 95014 USA, (408)366-4104 {apple | pyramid}!motcsd!brian

---

Re: automated car parking?

Scott Hinckley <scott@hsvaic.boeing.com>
18 Apr 91 14:36:13 GMT

I have always wondered about another risk this poses:

assume these are marketed
assume there are no new parking zones made
assume you in your non-self-park car get blocked in by two self-parked
Now, how in the heck are you going to get out if there are just a few inches in front and back of you?

This would perhaps necessitate the creation of self-park-only zones.

<<<<<<<<<<Scott Hinckley<<<<<<<<<<<><><><><><>>VW&Apple][Forever!!!<><><><><>
Internet:scott@hsvaic.boeing.com|UUCP:...!uunet!uw-beaver!bcsaic!hsvaic!scott

---

Re: drive-by-wire

Brad Templeton <brad@looking.on.ca>
Thu, 18 Apr 91 17:12:37 EDT

I have serious doubts that we will see such a system for some time -- not until we are truly forced into it.

People simply refuse to tolerate death by computer error. It seems they would gladly take ten times the amount of death by human error first, or death by their own error.

Any computerized traffic system would have some bugs, and thus some deaths. But even if traffic deaths are reduced from 10,000 to 100, and likewise for injuries, the problem is that a computerized traffic system creates somebody else to blame, other than yourself and the other drivers.

Lawsuits will seek out the vendors. Every accident in the automatic system will mean a costly lawsuit -- possibly millions of dollars -- for the vendor of the cars and systems, as well as the operators of the roads and the traffic authorities.

Our current system depends on the fact that most people never get properly compensated, or that the compensation is spread out among thousands of drivers and their insurance companies. To concentrate it all in a few parties, even at a level orders of magnitude less, is probably more than any firm can bear.

People feel they are in control on the road. Even if somebody else causes an accident, they like to feel they might have the power to avoid it with sharp driving.

This is sad, and perhaps the greatest RISK (in terms of loss of life) ever. Tens of thousands of people are killed and more are injured by auto accidents, and this system could make a dramatic reduction in this. We have the technology now to do it, but we won't for some time because of fear of computers and litigation.

Report problems with the web pages to the maintainer

Search RISKS using swish-e

THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

ACM Committee on Computers and Public Policy, Peter G. Neumann, moderator

Volume 11: Issue 50

Monday 22 April 1991

Contents

Dutch Intruders (courtesy of John Markoff)

Peter G. Neumann <neumann@csl.sri.com>
22 Apr 91 10:12:20 PDT

COMPUTER INTRUDERS TAPPING U.S. SYSTEMS, By JOHN MARKOFF
c.1991 N.Y. Times News Service

Beyond the reach of American law, a group of Dutch computer intruders have been openly defying United States military, space and intelligence authorities for almost six months. Recently they broke into a U.S. military computer while being filmed by a crew from Dutch television station.

The intruders, working over local telephone lines that enable them to tap American computer networks at almost no cost, have not done serious damage, federal investigators say. And they have not penetrated the most secure government computer systems. But they have entered a wide range of computers, including those at the Kennedy Space Center, the Pentagon's Pacific Fleet Command, the Lawrence Livermore National Laboratory and Stanford University via an international computer network known as the Internet.

While the information on these systems is not classified, the computers store a great variety of material, including routine memorandums, unpublished

reports and data from experiments. Federal officials said the group had tampered with some information stored on systems they have illegally entered.

U.S. government officials said that they had been tracking the interlopers, but that no arrests had been made because there are no legal restrictions in the Netherlands barring unauthorized computer access.

A reporter's efforts to reach Dutch government officials for comment have been unsuccessful.

``This has been a terrible problem,'' said Gail Thackeray, a former Arizona assistant attorney general who has prosecuted computer crimes. ``Until recently there have been few countries that have computer crime laws. These countries are acting as hacker havens.'' She said that just as offshore banks in certain countries have traditionally protected financial privacy, today some countries protect intellectual property violations.

American law-enforcement officials said they believed there were three or four members of the Dutch group, but would not release any names. A Dutch television news report in February showed a member of the group at the University of Utrecht reading information off a computer screen showing what he said was missile test information taken electronically from a U.S. military computer. His back was to the camera, and he was not named.

Military and intelligence agencies physically separate classified computer networks from those used by businesses and researchers to protect the data from electronic forays. When classified information is transmitted over unprotected computer networks or telephone lines it must be specially coded.

Because there are no computer crime laws in the Netherlands, American investigators said members of the Dutch group boasted that they could enter computers via international data networks with impunity. But some of the intruders have been identified, and a federal official, who spoke on the condition of anonymity, said there were numerous other criminal offenses for which the they could be prosecuted in both the United States and the Netherlands. One possible charge might be telephone fraud. But legal experts said that because there are no prohibitions against unauthorized computer entry in the Netherlands successfully prosecuting the group may still prove impossible.

The case is significant, legal experts said, because while the United States and many European countries have strict laws barring illegal access to computers, there are many nations that have no computer crime laws.

There is a proposed law before parliament in the Netherlands that would make unauthorized computer access a crime. Also, a governmental committee of the European Community is now working to standardize computer crime laws in Europe.

Because computer networks are accessible from anywhere in the world via a telephone call they are potentially vulnerable to those who cannot easily be prosecuted or convicted of a crime.

In the Netherlands case, the group was detected last year after an unusually skilled U.S. government computer researcher at a national laboratory tracked the group's every move using advanced computer security techniques. He notified U.S. authorities of the break-ins.

The researcher has been able to make computer records of the intruders' keystrokes as they have electronically prowled through U.S. military, NASA, university and dozens of other computers. It has then been possible to play this information back and gain an exact picture of the computer screen as it appeared to the intruders in the Netherlands.

From 1986 to 1988 Clifford Stoll, an astronomer at Lawrence Berkeley Laboratories traced a similar group of West Germans, who were illegally entering U.S. computers and selling computer data and software to a Soviet

intelligence officer. Stoll was able to persuade law enforcement officials to locate the group in West Germany and three arrests were made. A German court eventually convicted them, but gave them suspended sentences.

One computer expert who has watched the electronic recordings made of the activities of the Dutch group said they do not demonstrate any particularly unusual computer skills, but instead appear to have access to a compendium of documents that contain recipes for breaking computer security on many U.S. systems.

These documents have been widely circulated on underground computer systems.

A computer industry executive, who spoke on the condition that he not be identified, said that he had seen several recordings of the break-in sessions and said that one of the members of the group used an account named ``Adrian'' to break in to computers at the Kennedy Space Center and the Pentagon's commander in chief of the Pacific. ``You could tell that the guy wasn't conversant with the computer he was on,'' he said, ``It looked like he had a cookbook sitting next to him telling him what to do next at each step.''

The tactics of the group are of particular interest to computer security experts because they have repeatedly used security loopholes demonstrated by a program written by Robert Tappan Morris, a Cornell University student, more than two years ago.

Last month a federal appeals court upheld the conviction of Morris, who in 1988 unleashed a program that jammed several thousand computers in a nationwide network. He was convicted of violating federal computer crime statutes and was fined $10,000 and ordered to perform 400 hours of community service.

The fact that the same security flaws can be used to illicitly enter computers several years after they were widely publicized, indicates that many professional computer managers are still paying only minimal attention to protecting the security of the information contained on the computers they oversee, computer security researchers said.

Dutch crackers and irresponsible officials

Fernando Pereira <pereira@klee.research.att.com>
Mon, 22 Apr 91 11:09:14 EDT

A report today by AP writer Jerome Soclovsky about the Dutch crackers who, as reported by John Markoff in yesterday's NYT, have been been breaking into various Internet sites by using the usual tricks, quotes Maarten Rook, director of economics and personnel at Utrecht University as saying about the sites broken into: ``They should take care of their own secrets ... If they don't want to be called they shouldn't be hooked up to the system.''

Blame the victim again! Should a site whose officials show this kind of disregard for the common good of the network-using community be allowed to stay on the Internet? It is Utrecht, not the victims, who should not be allowed the benefits of the network, at least until its officials become more responsible and enforce rules of civilized network use, laws or no laws.

Fernando Pereira, 2D-447, AT&T Bell Laboratories
600 Mountain Ave, Murray Hill, NJ 07974 pereira@research.att.com

---

Computers Cause False Images

<[anonymous]>
Sun, 21 Apr 91

CHICAGO (AP) [21 April 1991]

Air-traffic controllers around the country say phantom images of airplanes often appear on cockpit computers, but the Federal Aviation Administration says safety isn't affected. The pilot of a United Airlines flight approaching O'Hare International Airport on Thursday tried to avoid a plane that wasn't really there, said Joel Hicks, national director of safety and technology for the National Air Traffic Controllers Association in Washington, D.C.

The incident began when a computer system called T-CAS Traffic Alert and Collision Avoidance System told the pilot another airplane was coming toward him, Hicks said. T-CAS ordered the pilot to descend from 7,000 feet to 6,000 feet, and the pilot began the move. At the same time, another aircraft leaving O'Hare was climbing from 5,000 feet to 6,000 feet. "The pilot advised (air-traffic controllers) as he was changing altitude," Hicks said Friday. "But more times than not they don't have time to do that. They're busy taking the plane up or down."

Controllers told the United pilot to return to 7,000 feet, and he did, although by law pilots can override information from T-CAS only if they see the other airplane. Controllers and the FAA say the standard separation the distance pilots must keep between their airplanes was maintained. Standard separation within 40 miles of O'Hare is three miles horizontally or 1,000 feet vertically.

FAA officials said the appearance of "ghost planes" might be caused by a software problem. They said it has posed no threat to air safety. "We're in the process of eliminating a problem in the software that might have caused this," said FAA spokesman Mort Edelstein. "From our standpoint, we know the system works the way it was designed to work," he said. "There was no problem with separation. There was no threat to safety." He said the FAA has recorded 750,000 hours of operational use of T-CAS, adding that in all those hours no incidents of planes flying too close together were discovered.

But Hicks charged that the system caused planes being handled by the Washington, D.C., air traffic control center to fly too close to each other earlier this year.

A retired pilot also said the habit of pilots to blindly trust the computer puts them in danger. "Pilots are in a spring-loaded position to act when one of these devices tells them to, regardless of rhyme or reason," said Dick Russell, a retired United captain with 26,000 hours of flying time.

After years of research, the FAA issued regulations in 1989 requiring all commercial aircraft with more than 30 seats to install T-CAS within three years. Officials gave commercial planes with 10 to 30 seats six years to install the system. T-CAS currently is used in about 20 percent of the nation's passenger planes, Hicks said.

Pilots convicted for libel in Habsheim controversy

Lars-Henrik Eriksson <lhe@sics.se>
Mon, 22 Apr 91 06:41:50 +0200

The following article is taken from the latest issue of a newsletter (Uppsikt) published by the flight safety department of the Swedish Civil Aviation Adminstration (Luftfartsinspektionen). It relates to the controversy about the fly-by-wire system of the Airbus A320 and the Habsheim accident.

Translated without permission by me. The quotes can not be completely trusted as they were first translated from French and English into Swedish, and then into English.

FRANCE: PILOTS CONVICTED FOR LIBEL

A French court of law has convicted two pilots for libel as they incorrectly attributed the blame for a fatal accident on technical malfunctions.

In a TV programme, the two pilots claimed that technical malfunctions, rather than mistakes by the pilots, was the cause of the accident during the air display at Habsheim on June 26th, 1988, when an Airbus Industries A320 crashed and three people were killed.

Michael Asseltine, pilot of the Airbus aircraft, and Norbert Jacquet, head of the French pilot union, were convicted for having defamed the "Direction Generale de l'Aviation Civile" and its director Daniel Tenenbaum during the TV program.

Asseltine and Jacquet had claimed that the accident was caused by a technical malfunction, and that the "black box" had been tampered with in order to free the manufacturer. The court decided on a fine of 10,000 francs (about $ 5,600).

After the verdict, Daniel Tenenbaum made an official statement: "The court has shown that the claims and insinuations made by the pilots about the so-called tampering with, and exchange of, the black box of the aircraft were completely unfounded."

Airbus Industries, having vehemently protested against the accusations in the TV programme, did not comment on the verdict. The spokesman for Airbus Industries in North America, David Venz, declined to make a comment as his company prefers to, as Venz put it, "let the decision of the court speak for itself."

[From Lars-Henrik Eriksson, Swedish Institute of Computer Science
Box 1263, S-164 28 KISTA, SWEDEN +46 8 752 15 09

[No puns on Luftfartsvergnugen, please. PGN]

"I can't work this ?#!!~* thing!"

Rodney Hoffman <Hoffman.El_Segundo@Xerox.com>
Sun, 21 Apr 1991 21:34:06 PDT

The cover of the current (29 April) issue of `Business Week' proclaims:

I CAN'T WORK THIS ?#!!~* THING!

> From VCRs and telephones to copiers and microwaves, poorly designed machines cluttered with unwanted features are driving consumers crazy. Whatever happened to user-friendly?"

No surprises for RISKS readers in the horror stories included. It's a good overview of the problems, and a preview of some of the simpler, cleaner products beginning to come out.

The cover story leads off with a quote from Don Norman's 1990 book, `The Design of Everyday Things'. The authors also plug the "new discipline of information design" and the two books by Edward R. Tufte: `The Visual Display of Quantitative Information' and `Envisioning Information'.

A few choice bits:

"Human engineering -- or the lack of it -- has always been a problem in some products, of course. But there's a reason why it bedevils us much more now than ever before: the microchip. Modern electronics has turned the economics of design on its head. No more does the cost of adding features limit the number of capabilities a designer can put into a machine.... so why not pile on the features?"

"All the rules boil down to one thing: Be obvious. A machine should be designed so that customers can look at it, understand it, and figure out how to use it -- quickly."

"People don't mind trouble as long as they can understand what's wrong and correct it. But for that they need feedback.... a machine must provide the user with tools to manage trouble."

[Says the owner of a high-end audio store:] "I don't know why the Japanese put so many buttons on their machines. They have given us programming, and programming is not music. Programming means computers."

"[Even in computers themselves,] survey after survey has shown that consumers want `plug-and-play' computers. They want to turn the machines on and get to work immediately. They don't want to spend hours consulting manuals."

Re: drive-by-wire

Martyn Thomas <mct@praxis.co.uk>
Mon, 22 Apr 91 16:22:56 +0100

In RISKS 11.49, brad@looking.on.ca (Brad Templeton) writes that drive-by-wire will not be introduced for many years because of the liability issues, and human intolerance to being killed by a computer.

Brad is clearly envisaging a system which takes over some or all of the decision and executive actions of the human driver, since he contrasts drive-by-wire fatalities with those caused by human error.

He continues:

> This is sad, and perhaps the greatest RISK (in terms of loss of life) ever. Tens of thousands of people are killed and more are injured by auto accidents, and this system could make a dramatic reduction in this. We have the technology now to do it, but we won't for some time because of fear of computers and litigation.

My own guess is that drive-by-wire wouldn't reduce deaths on the road, per million users or per million passenger-miles, but I haven't done the calculation (probability of failure per year * number of probable fatalities per failure * hours of drive-by-wire per year) because the assumptions are too difficult to make and justify.

A drive-by-wire system could enforce current guidelines for "safe" speeds and distances between vehicles (eg the UK "Highway Code"). This would certainly increase journey times and may reduce road capacity and throughput.

Alternatively, the system could use the assumed safer behaviour of software "drivers" to reduce spacing or increase speeds, in which case accidents from any cause would be likely to create more fatalities per accident (kinetic energy increases as the square of speed; more nearby vehicles mean more nearby people mean more casualties).

Remember that some accidents (what proportion?) are caused by mechanical failure, and that the drive-by-wire system would have many new failure opportunities (software, EMI, components, sabotage ...). We *might* eliminate driver error - but only if the driver has *no* override.

Have any calculations been carried out to estimate the effects of some drive-by-wire scenario on the fatality rates? If so, what were the assumptions and the conclusions?

If not, why assume that such a system would be safer?

Search RISKS using swish-e

Report problems with the web pages to the maintainer

Search RISKS using swish-e

THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

ACM Committee on Computers and Public Policy, Peter G. Neumann, moderator

Volume 11: Issue 51

Monday 22 April 1991

Contents

RE: Dutch crackers and irresponsible officials (RISKS-11.50)

"Dr. Tom @MKO, CMG S/W Mktg" <blinn@dr.enet.dec.com>
Mon, 22 Apr 91 15:23:35 PDT

I certainly agree with Fernando Pereira that there appear to be irresponsible officials involved in this incident, but I beg to differ with him about just who and where they are.

If the published accounts are accurate, then the systems being "cracked" are many of the same ones that have been "cracked" in the past, and the security loopholes that are being exercised are the self-same ones that have been used in past episodes.

The irresponsible officials are not at the University of Utrecht, as Fernando Pereira would have us believe; rather, they are the bureaucrats managing the systems who haven't closed the well-understood loopholes.

The risk? The continued belief that "security through obscurity" can work, that by prohibiting access (and making the open flow of unclassified data a crime) we can somehow eliminate the need to secure our systems.

This is *not* a matter of blaming the victim, when the victim is suffering from his (or her) own negligence. Mr. Pereira is correct: "Should a site whose officials show this kind of disregard for the common good of the network-using community be allowed to stay on the Internet?" Of course not, but it is NOT a problem in Utrecht, it is a problem in the systems that were compromised through their own lack of diligence in implementing known fixes for known security problems.

Tom

Dr. Thomas P. Blinn, Digital Equipment Corporation, Digital Drive, Merrimack, New Hampshire 03054 ...!decwrl!dr.enet.dec.com!blinn (603) 884-4865

Re: Dutch Intruders (RISKS-11.50)

Louis Todd Heberlein <heberlei@fuji.eecs.ucdavis.edu>
Mon, 22 Apr 91 16:13:53 PDT

I think before we can seriously worry about intruders using countries outside the United States (and other countries with computer crime laws) as places to hide, we need to take a close look at ourselves first.

I, along with a number of other organizations, have been working in the field of intrusion detection. I remember how excited I was when I detected my first honest to goodness intrusion. Several months later, and several HUNDRED intrusions later, I now feel like a guest on the hackers' networks. Why should I worry about hackers from other countries when we have thousands of them here at home?

Todd

Government control of information

Jerry Leichter <leichter@lrw.com>
Sat, 20 Apr 91 12:28:48 EDT

The recent discussions of proposed regulations on cryptographic equipment have approached a deep issue that I think has been inadequately discussed and thought through. People continue to discuss the specific issue of cryptography entirely through the traditional approaches of the First and Fifth amendments and ideas about personal privacy. There's a risk in doing this: The risk of missing new risks caused by application of ideas in new and different circumstances.

Societies have always claimed the right to control various objects and

substances that thet consider dangerous. Drugs, plants that produce drugs, explosives, guns, various kinds of precursors for dangerous things that are not in themselves dangerous, have all been regulated for many years. We are in the midst of an ongoing debate in the United States about the degree to which we should control access to guns - but in fact we've had some controls on them (machine guns and sawed-off shotguns are illegal) for a long time.

Many people have argued that we are in transition to an "information-based" society, that in the future the source of wealth and power will be, not material goods, but information itself. If this is the case, I posit that we will inevitably find that, just as we have found it necessary in the industrial age to control access to certain substances and devices, in an information age we will find it necessary to control access to and dissemination of certain classes of information.

In fact, we already do this. No one I know argues that you should have the right to distribute other people's charge account numbers; no one seems upset when credit card thieves are prosecuted for selling such numbers. (We may call the charges brought against them different things, but in practice what we are trying to prevent is trafficing in a certain class of information). We're concerned about companies that sell data - information - about us without our consent. The companies might argue that they are just exercising their rights of free speech, but somehow that argument doesn't seem enough.

The government has a massive establishment for classifying information and keeping classified information secret. Generally, if you come upon classified information from a non-classified source, you are free to do with it what you wish. It's little-known that there are two exceptions to this in the law: Certain information regarding nuclear weapons and cryptography is "born classified" - you are bound by restrictions even if you discover the information yourself. (There have been few attempts to enforce these laws; I don't think any attempt has been fought out to a Supreme Court decision on the obvious constitutional questions that arise.) You cannot export programs that implement cryptographic algorithms from the United States - you may think they are "information", but the government essentially classifies them as munitions. (And, no, "public domain" or "free" distributions are treated no differently from for-profit distributions.)

When NASA was created, it was required to make all its plans and designs available to anyone who asked. These days, there's increasing concern that a Libya or an Iraq can easily obtain full engineering drawings, specifications, manufacturing techniques, even lists of suppliers, for tested missiles with intercontinental range. Duplicating that work from scratch would be a formidable, if not impossible, undertaking for most countries in the world. (Actually building the missiles is still difficult, but it's much, much easier to build from complete plans.)

As information, in and of itself, becomes more and more central to our economies, our military, and every aspect of our lives, the clash between free speech and safety and privacy will inevitably increase. I believe it's naive to think that we can ignore this clash, or continue to claim that "openness" is ALWAYS the best policy. (In fact, I know of few people who really believe that, even if they say it: If you claim you believe openness is always the best approach, ask yourself whether you believe the store you rent VCR tapes from

should have the right to make public information about what you view. It all comes down to whose ox is gored, doesn't it?) (BTW, your VCR data IS private, by law. This little special-case law was, as I recall, passed in response to outrage about newpaper reports on Robert Bork's viewing habits while his Supreme Court nomination was being considered.)

The general issue of control of information has actually been discussed in science fiction for years. Larry Niven's novels have various references to agencies with the job of controlling the dissemination of information - that's one of ARM's jobs, for example.

The earliest, and still one of the best, discussions is in a story written by Isaac Asimov in the late fifties or early sixties. The title is something like "The Dead Past"; it appears in a collection titled "Earth Is Room Enough". I highly recommend it to anyone who thinks that these problems have trivial solutions.

-- Jerry

Letter to Senators (Re:Senate 266)

Edward_Engler@transarc.com <Ed Engler, ere@transarc.com>
Mon, 22 Apr 1991 10:55:09 -0400 (EDT)

After reading many posts about Senate bill 266, I have decided that this issue is worth writing to my senators about. I have drafted the enclosed letter, and I urge everyone to send a copy of it to their senators as well. Regardless of the immediate impact of this bill, the long term effects of the statement in question can only be to compromise both personal freedom and national security in the United States.

Dear Senator [Your senators name],

Recently, Senator Biden introduced a counter terrorism bill containing a very distressing provision. In Senate 266, section 2201 titled "Cooperation of telecommunications providers with law enforcement", that proposition is put forth that "It is the sense of Congress that providers of electronic communications service equipment shall ensure that communications systems permit the government to obtain the plain text contents of voice, data, and other communications when authorized by law."

I do not believe that requiring communications 'gear' (whether it be transmission equipment or communications software) to allow anyone 'authorized by law' to read data transmitted by such means will serve your constituents or our national interest.

I understand that the proposition is not specifically requiring manufacturers to do anything at this time. What it does is give the secret bureaucracies of the executive branch of our government free reign to create any such regulations that they see fit to write.

The only outcome of such power can be the enactment of one or more regulations diminishing the ability to transmit secure data via electronic means of

communication. No other form of communication has attached to it the universal ability to read any communication that it is used to transmit. I can send an encrypted letter through the mail, and the only way anyone other than the intended recipient can read that letter is by asking one of the two participants what it says. Why should electronic means of communication be any different?

Consider the following scenario: The Department of Defense makes heavy use of electronic communication both on and off the battlefield. If all communication systems were to have a method whereby an individual other than the intended recipient could read the message, an unfriendly organization will gain access to the contents of some (or all) of our military communication. This is a very serious breach of national security as well an affront to the personal privacy of millions of United States citizens.

By adopting that statement, the Congress will be adopting a stance that will inevitably result in the widespread use of communications systems highly susceptible to compromise not only by authorized government agencies, but by outlaws and antagonistic foriegn nationals as well.

You should ensure that the section in question is rewritten to read "It is the sense of Congress that communications via electronic means shall be protected from being read by any but the intended recipient by all reasonable means available to the transmitting device or authority." If you feel that it is important that the government have access to the data passed between individuals, then you may want to introduce a bill stating "The government may, with the permission of a judge, subpoena the contents of electronically transmitted messages. Anyone willfully destroying subpoenaed electronic information is subject to (some term of imprisonment and/or some fine)."

By all means let's protect ourselves from terrorism, but let's not give up any of our fundamental liberties in doing so.

Sincerely,

[your name]

Withholding cryptographic keys (Re: SB 266, Boudrie, RISKS-11.49)

<hkhenson@cup.portal.com>
Sat, 20 Apr 91 18:05:38 PDT

I am not a lawyer, and off-hand would have agreed with Bob's analysis. However, at the recent Computers, Privacy, and Freedom Conference, I had lunch with several lawyers (defense and prosecution). I brought up this very problem, and they delved into the reasoning a judge would use when confronted with law enforcement agents trying to pry a key out of someone. It was their solid conclusion--on Constitutional grounds--that a person could not be force to disclose a crypto key, because the *resultant* decrypted data would be the "product" (in some legal sense) of the key and the encrypted data, and would thus invoke the self-incrimination protection of the Constitution. I guess you can be forced to turn over physical items, and even safe combinations, but not

crypto keys which act directly upon information to make it useable, and possibly incriminating.

For all the reasurance, I am not eager to be a test case!

H. Keith Henson (hkhenson@cup.portal.com)

Encryption backdoor rule: hiding data

Ross Williams <ross@spam.ua.oz.au>
21 Apr 91 17:54:08 GMT

> Although US citizens have a right against self incrimination, it is unlikely
> that this right extends to withholding cryptographic keys encoding potentially
>...
> Establish a well documented, and publicized, policy of encoding numerous
> "dummmy files" (perhaps using man pages as source text) using your standard
> encryption algorithm, with random keys which are not recorded. This will
> produce a *DOCUMENTED SITUATION* in which you are not able to product
> decryption keys for the majority of your files, even if you wanted to.

Or how about this. Design a cipher system that allows n files along with some white noise to be jointly encrypted into a single file using several different keys. Use data compression and white noise to hide how many files and how much data is actually there. Then, when asked to decrypt, one can give any key or keys one pleases so as to decrypt to one of many documents, innocent or otherwise.

Or hide your data:
1) In large executable files.
2) In the grammar of large computer programs.
3) Using data compression techniques in other (non-compressed) data.

The possibilities for hiding data are endless. One way to police this sort of thing might be to demand that a ciphertext decrypt to a document, which when compressed, is about the same length as the ciphertext.

Ross Williams. ross@spam.ua.oz.au

Encryption

<Tony_Buckland@mtsg.ubc.ca>
Fri, 19 Apr 91 15:19:12 PDT

For those wanting secure encryption, a true one-time pad (with the key as long as the text), really used only once, remains as unbreakable as it ever was. It's tedious as hell to use, because you have to courier enough keys to your recipients in advance to cover all the messages you ever expect to send, but it is, if applied with absolute diligence, really safe. That is, it reduces spying back

to the good old low-tech methods of sex, blackmail,
burglary, corruption and personal violence.

Comment on "US Gov't is not careful with its supplies"

<haynes@cats.UCSC.EDU>
Sat, 20 Apr 91 00:11:55 PDT

That story reminded me of something that happened nearly 30 years ago,
but the the government is often accused of using data processing
technology that is 30 years behind the times.

The truck division of one of the automakers had a regional parts warehouse.
Dealers ordered parts from the warehouse by filling out a form on a machine
that made punched paper tape. The tape was then transmitted to the warehouse
with a telephone and modem setup. There was no checking, parity or anything
else.

One night the transmission made a single-bit error, changing ASCII zero to one.
This turned an order for 17 dipsticks into an order for 1017 dipsticks. The
warehouse computer processed the order, even generating a letter to the dealer
to the effect that there were only 234 dipsticks in stock, and they were
sending those and would order the rest from the factory and send them when they
came in.

The mistake was discovered when the guy packing the order for shipment wondered
why that small-town dealer needed so many dipsticks and brought it to the
attention of his boss. Perhaps by now packaging and shipping technology has
improved to the point that the 234 dipsticks could be shipped without anyone
having a chance to notice.

Re: Educating the Camiroi

George L Sicherman <gls@corona.att.com>
Sat, 20 Apr 91 20:11:10 EDT

In Risks 11:49, David Lamb alludes to a science-fiction story which he
misattributes to Cyril Kornbluth. "Primary Education of the Camiroi"
was written by R. A. Lafferty and published 25 years ago in _Galaxy._
The story does indeed mention a child who reads too fast:

> "Only the other day there was a child in the third grade who
> persisted in rapid reading," Philoxenus said. "He was given an
> object lesson. He was given a book of medium difficulty, and he
> read it rapidly. Then he had to put the book away and repeat
> what he had read. Do you know that in the first thirty pages he
> missed four words? ..."

As a mere Earthling, Mr. Lamb may be forgiven his error; but Philoxenus
later mentions that at Camiroi schools slow learners are executed. Usenet
is more humane -- slow learners are merely ex-communicated!

Col. G. L. Sicherman gls@corona.att.COM

Search RISKS using swish-e

THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

ACM Committee on Computers and Public Policy, Peter G. Neumann, moderator

Volume 11: Issue 52

Tuesday 24 April 1991

Contents

Another commuter train wreck in London

Jonathan I. Kamens <jik@pit-manager.MIT.EDU>
Tue, 23 Apr 91 16:59:42 -0400

(Posted with permission from the ClariNet electronic newspaper service & UPI. People who want more info on ClariNet can mail to info@clarinet.com or phone 800-USE-NETS.)

Date: 22 Apr 1991 08:46:20 GMT
From: clarinews@clarinet.com
Subject: Computer-controlled commuter trains collide in east London
Newsgroups: clari.news.trouble,clari.news.europe
Message-ID: <Ubritain-railway_265@clarinet.com>

LONDON (UPI) -- Two computer-controlled commuter trains collided at the height of morning rush hour in London's Docklands district, shutting down the railway system and forcing the evacuation of dozens of passengers, police and witnesses said.

One two-car shuttle traveling through the Isle of Dogs from London's Tower Gateway was struck by a second-two car train approaching from the east at a junction on the West India Quay bridge, rocking the first train and throwing it off the track.

Police had to erect a ladder to get passengers out of the tilting cars.

No serious injuries were reported but police said two passengers were taken to hospital for treatment of shock. One commuter said passengers in the first train, which was stopped, yelled ``hold on'' and ``watch out'' as the second driverless train continued toward them.

``It was bloody frightening, because you could see it unfolding before your eyes,'' said commuter Tom Bromhead.

The Docklands Light Railway, intended to serve thousands of commuters in the district, usually operates by computer, allowing the drivers to check tickets and open the doors.

The newly built system has been plagued by cost overruns and frequent shutdowns in the growing business district east of London.

Jonathan Kamens, MIT Project Athena jik@Athena.MIT.EDU 617-253-8085

No beepers under 21

Max Tardiveau <root@nextserver.cs.stthomas.edu>
Tue, 23 Apr 91 05:39:14 CDT

I saw on a news program (it may have been 48 hours) this weekend that there was a law being debated in Congress that would forbid the possession of electronic pagers (beepers) under the age of 21. The idea being that a lot of drug dealers use these devices. This strikes me as a perfect example of cause-and-effect confusion. How can any mildly intelligent person believe that forbidding the use of beepers under the age of 21 will in any way affect drug trafficking? I would appreciate any detail anyone might have, I am afraid this is all I know, but it is so mind-boggling I couldn't let it pass unnoticed.

Max Tardiveau, Department of Computer Science, University of St.Thomas, St.Paul, MN 55105 Internet : m9tardiv@cs.stthomas.edu

[In a lighter vein [!], almost all beepers around today are under the age of 21. Maybe the older beepers will sue for age discrimination. PGN]

Monitoring in the workplace

Jerry Leichter <leichter@lrw.com>
Sat, 20 Apr 91 14:52:14 EDT

The issue of automated monitoring of workers has been discussed many times in this forum. The current BusinessWeek (April 29, 1991) provides some important new information about this practice: As many of us may have suspected, not only is it bad for employees, it's not even good business. The article, "How to Motivate Workers: Don't Watch 'Em" appears as a sidebar (page 56) to a larger article on white-color work quality (which I recommend, along with an interesting cover article on the unusability of too many technological objects):

> Electronic eavesdropping is a tempting tool for boosting office productivity. Airlines, insurers, and telecommunications companies, among others, often clock every second that workers spend on computers or on the phone with customers. From a handful a decade ago, the number of monitored employees has reached 10 million, according to the Office of Technology Assessment.
>
> But now, the search for quality is abridging this trend. Federal Express, Bell Canada, USAA, and Northwest Airlines, among other major employers, are finding that too much speed spoils service.
>
> HANDLE TIME
> They have begun to stress quality over quantity, or to end monitoring entirely. THe result seems to be happier customers and employees. Proponents also say that a focus on quality does as much as monitoring to keep productivity high and rising. "A lot of people ask, which do you want, quality or quantity?" says Rebecca Olson, head of customer service for Federal Express Corp.'s southern region. "We found that you can have both, though it took a while to sink in."
>
> FedEx was among the first to see this. In 1984, it was worried about United Parcel Service Inc.'s move into overnight deliveries. Management realized that it could save money by slicing just one second off the average time its 2,500 customer-service agents spent on each call. So, FedEx began to monitor the average "handle" time per call - and made beating the clock 50% of an agent's performance review.
>
> Two years later, the strategy came home to roost. Employees griped that limiting every call to 140 seconds created too much stress - and made them cut of customers before questions were answered....
>
> A new system cleared that up. Today, a supervisor listens in on a random call twice a year. Afterward, the discussion with the agent focuses on quality: The length of the call isn't mentioned. Both employees and executives say that service has improved - without hurting speed. The average call even dropped to 135 seconds....

The article continues with a description of another positive result, at Bell Canada's operator services.

-- Jerry

"University Exec Backs Hacking" (Dutch crackers, RISKS-11.50,51)

<[anonymous]>
Mon, 22 Apr 91 10:30:39 xxx

UTRECHT, Netherlands (AP)
A Dutch university official on Monday defended a student hacker's purported use of a computer network used by his school to penetrate a U.S. military computer.
The Netherlands has no law against computer intrusion, making it a hacker's paradise. However, Parliament is expected to pass a law this year that forbids unauthorized entry into computer systems, the Justice Ministry said.
The New York Times reported in Sunday editions that over the past six months, three or four Dutch hackers have broken into a range of U.S.-based computers. The computers include those at the Pentagon's Pacific Fleet Command, the Kennedy Space Center, and the Lawrence Livermore National Laboratory and Stanford University in California. [see RISKS-11.50]
U.S. officials said they had identified some of the intruders, but that no arrests had been made.
Maarten Rook, the director of economics and personnel at Utrecht University, was present during the February filming of a hacking incident shown on a late-night Dutch television show. It showed the hacker breaking into what purportedly was a U.S. Navy computer installation in San Diego.
During the broadcast, the hacker, whose face was not shown and whose voice was scrambled, linked his personal computer to the Surfnet data network used by Dutch universities. Surfnet in turn is linked to the U.S.-based Internet bulletin board, through which the intrusion was made.
The televised hacker, an Amsterdam student, obtained data that he claimed pertained to U.S. Navy ships and ballistic missiles, said Rook. However, Rook said he did not believe that the break-in resulted in access to confidential information.
It could not be determined if the target of the televised break-in was the Pacific Fleet Command computer.
Rook said installations using computers had a responsibility to devise secure systems to protect themselves against hackers. "They should take care of their own secrets ... If they don't want to be called they shouldn't be hooked up to the system," he said. Rook said most Dutch universities encourage their students to probe other systems as much as they can as part of their computer training. Several years ago, the prestigious Delft University of Technology even offered a course in computer hacking. "In our teaching system we try to endorse exploration and make our students enthusiastic about it," he told The Associated Press.

Hacking a la Neerlandaise

"Herman J. Woltring" <UGDIST@nici.kun.nl>
Tue, 23 Apr 91 03:35 MET

Last week, I committed a series of terrible crimes. While sitting behind my PC in the wee hours of the night, I hacked into a number of university and

military libraries all over the world, both in the USA and in Australia, using the TELNET facilities recently advertised in the bimonthly SURFnet Bulletin from SURFnet Inc of Utrecht, The Netherlands. In this manner, I was able to snoop around on the shelves of these libraries, and to find out what books were on hold, booked for borrowing, not to be removed from the premises, or free to be lent for shorter or longer periods.

In this way, I was able to pry into the librarians' private domains, well beyond the reach of American and Australian Law. Since the Gouvernment of The Netherlands is trying hard to persuade Parliament that Computer Hacking is a capital offence, it is my solemn duty to ask the Dutch Press to film and publicly denounce my asocial behaviour, so as to convince the Legislative that the proposed revision of the Netherlands Penal Code is timely and quite appropriate. Even worse, SURFnet Inc has been aiding and abetting with my crime, because instructions on how to hack into these overseas computers are freely available by networking. Just sending the one-line query GET INTERLIB CATALOG to LISTSERV@NIC.SURFNET.NL (or to LISTSERV@HEARN.BITNET) will provide all information needed for TELNETting, FTPing, and similar lone-ranging computer intrusion activities. It is particularly shocking that the INTERLIB CATALOG even provides login-in data and passwords such as "anonymous" or "guest".

Herman J. Woltring

Responsibilities of Internet sites (was Dutch crackers)

Fernando Pereira <pereira@klee.research.att.com>
Tue, 23 Apr 91 11:30:35 EDT

I don't want to start a whole discussion on this matter, which has in other guises been covered extensively on previous RISKs, but I would like to respond briefly to T. Blinn and L. T. Heberlein's responses to my recent posting.

1) I know of no area of human activity in which wilfull intrusion or condoning intrusion are seen as no more condemnable as failure to protect one's domain from intrusion to the best of one's ability. Furthermore, it has been often pointed out that many Internet sites, for economic or other reasons, do not have the resources to keep up with security updates. The Internet has never been seen as a secure environment, to my knowledge. In fact, one might well take it as an wide-open environment in whose existence depends on the restraint and common courtesy of its users. Those that do not understand these ground rules don't belong there.

2) Indeed there are intruders all over the place. The special issue with respect to Utrecht is that an official of that site condoned behavior harmful to the community of Internet users.

Fernando Pereira, 2D-447, AT&T Bell Laboratories
600 Mountain Ave, Murray Hill, NJ 07974 pereira@research.att.com

---

Re: Dutch crackers and irresponsible officials (RISKS-11.50)

<smb@ulysses.att.com>
Mon, 22 Apr 91 22:38:43 EDT

I think that Thomas Blinn has missed the point. Yes, systems on the Internet are insecure, often to a scandalous degree. And yes, that's often the fault of careless or irresponsible system administrators, though vendor culpability should not be neglected. Disregarding for a moment the activities of the hackers, the offense committed by the Dutch university officials is ethical: they are failing to condemn activities that are at the least immoral, and at best downright criminal.

The traditional defenses of hackers simply do not apply here, assuming that the facts have been reported accurately. There was no ingenuity or exploration demonstrated; we are told that the intruder appeared to have a ``cookbook sitting next to him telling him what to do next at each step.'' Nor was the intrusion harmless; the article mentions tampering with data. Under what moral codes are such activities acceptable? Arguably, a university is not the place to teach basic ethical behavior; it should have been learned long before. But there is at the very least the imperative to refrain from encouraging unethical behavior. I will agree that some forms of hacking are educational. Given that, schools should provide the proper targets to be probed. (By analogy, I have not heard of locksmith schools urging students to engage in unofficial lab sessions at the neighborhood bank. Why is this different?)

Before I return to the ``merely'' technical, let me belabor the obvious one more time. A landowner (in the U.S.) who does not wish visitors may simply post ``No Trespassing'' signs; he or she is under no obligation, legal or moral, to install barbed-wire fences. To be sure, if the person is sufficiently concerned about privacy or protection of property, stronger measures may be taken, with the distinct encouragement of the insurance companies. So what? A lack of prudence (or paranoia) is not an invitation to burglary.

Let us now consider the problem of insecure systems. Yes, they exist. Often, there's no justification for that, especially when the holes are as well-known as the ones apparently used here. But system administrators are often overworked, and -- most important -- computer systems do not exist for the purpose of being secure, any more than cars exist for the purpose of being locked. A computer system has a mission, an end-user community to serve. If its mission involves an application that won't run on a later version of the operating system -- and we've all seen those -- the operating system won't be (and shouldn't be) changed. Very often, no one has the time or energy to upgrade things, especially when the current applications are running satisfactorily. Are the latest security bug fixes even available for old releases? Does the vendor even have the capability to perform thorough testing on such fixes? Very often, with the best will in the world, the answer is ``no''.

The claim has been made on RISKS that vendors should warrant their systems to be bug-free, just as is done for other products. Presumably, this applies even more to security holes. I have my doubts that this can be done -- I just don't think the state of the art of software engineering is good enough. (If it were that good, much of the RISKS digest would go away....) For the forseeable

future, we will be faced with systems that, most likely, have serious holes. Administrators of systems containing precious data react by withdrawing them from the electronic community, or hide them behind gateways. Others venture forth, but keep their alarms on and their phasers at the ready. Still others place their trust in the shared values of the electronic community, and take only minimal precautions. And that trust still exists, at least in the minds of some users. A quick quiz: how many readers will set up a ``vacation'' message announcing how long they'll be away, and where they're going? How many people would put the same information on their home answering machines? In a sign on the front door of their houses?

Yes, computer security is important. (I certainly think so; it's my area of research.) And yes, people shouldn't be surprised when loosely-administered systems are hacked, any more than than they should be surprised at muggings in some of the more dubious neighborhoods. But it is a fallacy, I think, to equate lack of prudence with solicitation to intrusion.

--Steve Bellovin

Re: Dutch crackers and irresponsible officials (RISKS-11.50)

<haz@leland.stanford.edu>
Tue, 23 Apr 91 10:09:30 PDT

In reference to Mr. Blinn's letter, to call administrators of computers irresponsible for allowing "well-known" security holes to continue to exist is understandable. No one wants "bad guys" to have bases from which they can mount more systematic attacks on other, perhaps more secure, machines.

However, you are missing the point. When an intruder is detected, what is the appropriate response? Should one make an effort to locate the muncher at all? If not to punish him/her, then simply to thank them for pointing out the flaws in your system, and then proceed to close the opened holes?

Given the complexity of today's networked systems, it is no more easy to secure a computer than it is to secure one's own home. It seems that the same code of ethics should apply. One shouldn't be faulted for having failed to implement the latest security patch any more than one should be faulted for not having locked all the windows, not having high security locks, and not having deadbolts in place.

What we are discussing here, is a case of someone who has been breaking into computer systems, and has, to some degree, been LOCATED. Given the time scales mentioned in the NYT article, the feds had known for six months about the intrusion, and had begun relatively sophisticated work to attempt to track down the intruder, and succeeded, only to discover that they could not actually pursue legal recourse.

An analogy might be an anonymous flasher (who does no actual physical damage, but is potentially disruptive) who turns out to be a teenager of the family down the street. The question is whether the family has a responsibility to discipline their children or not.

-castor fu castor@embezzle.stanford.edu

re: Dutch hackers and KSC [Kennedy Space Center]

Bruce Oneel <oneel@heawk1.rosserv.gsfc.nasa.gov>
23 Apr 91 12:57:07 GMT

I don't believe that KSC is on the internet. bruce

Bruce O'Neel, Code 664/STX,NASA/GSFC Bld 28/W281, Greenbelt MD 20771
(301)-286-4585 compuserve: 72737,1315 oneel@heasfs.gsfc.nasa.gov

CERT Warning on Spoofs

<WHMurray@DOCKMASTER.NCSC.MIL>
Fri, 19 Apr 91 22:42 EDT

A recent RISKS carried a warning by the CERT about spoofs. Reading it you might conclude that they were surprised by these nasty attacks. (I described these spoofs, at least in abstract terms, in "IEEE Spectrum" more than a decade ago. Landreth described them in elaborate detail in "Out of the Inner Circle" at about the same time.) The CERT proposed a remedy which was labelled in RISKS as "Social Engineering."

By labelling their remedy "Social Engineering," I expect that the CERT intended to suggest that the problem of vulnerability to spoofs is one of human behavior. Nonetheless, whether they intended to or not, what they succeeded in communicating was the futility of their remedy. While it is possible to protect a user from a spoof by warning him about it, you cannot adequately protect a system with a large user population by doing so.

It is attributed to Phineas T. Barnum: "There is a sucker born every minute." Far fewer than that are required to defeat the CERT's remedy. Certainly there are more than enough in the user population of any large system, let alone the internet, to ensure that all those systems that rely upon reusable passwords can be compromised by even a trivial spoof.

Lincoln said "Human nature will not change." If Lincoln was wrong, it is because human nature changes too slowly to notice. The CERT, and the system managers it is exhorting, are not likely to change it in time to cope with these attacks. In attempting to solve the problem of spoofs by changing user gullibility, the CERT is attempting to prop up a house of cards.

While the problem of these spoofs is aggravated by user behavior rooted in reusable passwords. Reusable passwords are fundamentally flawed: they have lasting value and the right to use them includes the right to make and give away, accidentally or intentionally, both the password and the associated privileges. Spoofs, and all other attacks against passwords, rely upon these two flaws for their efficiency. One can afford to attack them because they have residual value. The success of the attack does not deny the password's use to the legitimate user, so he is not bound, or even likely, to notice.

The reliance on reusable passwords is the biggest single computer security vulnerability that we have. It dwarfs all others. It finesses all our other efforts; nothing else that we do is effective as long we are vulnerable to these spoofs. Continued exclusive reliance on reusable passwords puts all our systems at hazard. Indeed it puts public and management confidence in our systems at hazard.

While spoofs are favored by insiders, most of the highly publicized penetrations by outsiders have involved attacks against reusable passwords. While most of these began with attacks against weak passwords, many subsequently went on to spoofs in order to expand the attacker's new privileges.

The solution to this problem will not be found in trying to change user behavior; while it is a fundamental condition of the problem, it is not one that is subject to change. The solution will be found in one-time passwords. If the CERT really wants to address the problem, it will recommend something that has a chance of success. It will recommend the use of reusable passwords.

They can enjoy the distinction of being the first authoritative institution to do so. (NIST has not done so, in spite of persistent urging from yours truly. NCSC has not done so, though of course they use them on their own systems. IBM has not done so, though they have said that they will not do anything to discourage or inhibit their use nor to favor one product over another.)

While there continue to be environments and applications in which reusable passwords can be made to work, they do not include the internet or user programming. While one-time passwords are not free, they are effcient; their use covers their own cost. Their cost is trivial when compared to other costs of using computers, and when compared to the cost of continued exclusive reliance on reusable passwords. Their cost is regular and predictable, particularly when compared to the cost of the uncertainties against which they protect.

William Hugh Murray, Executive Consultant, Information System Security
21 Locust Avenue, Suite 2D, New Canaan, Connecticut 06840
203 966 4769, WHMurray at DOCKMASTER.NCSC.MIL

Broadcast telephone calls

Iain Douglas <iain@tharr.UUCP>
Fri, 19 Apr 91 23:44:47 GMT

Thursday evening (18-4-91) the BBC popular science program Tomorrow's World ran an article of particular interest. Reserchers for British Telecom have developed a system that uses tuneable lasers and optical fibres to connect telephone calls. Each subscriber is allocated a frequency, and when making a call the umber you dial tunes up the subscribers frequency on the laser in your phone. Gone is the electromechanical and electronic switching gear currently in use, all calls are BROADCAST across the whole system. Nobody is going to produce a reciever that is tuneable over the whole bandwidth, are they? :-)

Iain

Parity and SCSI (RISKS-11.18,22)

<ts@cup.portal.com>
Wed, 13 Mar 91 03:06:59 PST

Martin Minow recently wrote in RISKS about the lack of error detection in SCSI.

In practice, this does not seem to be a problem. Each data byte has a parity bit associated with it. Thus, you would need two or more errors in a single byte to cause a problem.

In three years of extensive SCSI use (I work for a company that writes firmware for SCSI host adaptors and SCSI target devices), including very badly wire wrapped prototypes, I've never seen a single random error, let alone multiple errors in a single byte.

The only times I've seen an error is when something like a cable or a pin breaks, causing a stuck bit. Parity catches these very quickly.

No one else in the company has seen an error either, and at SCSI-2 standard committee meetings and CAM committee meetings we've asked other people, and they too report that errors are very rare.

Tim Smith

Search RISKS using swish-e

THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

ACM Committee on Computers and Public Policy, Peter G. Neumann, moderator

Volume 11: Issue 53

Wednesday 24 April 1991

Contents

Canada may computer-pick personnel for constitutional problem-solving

Dan Freedman <dan@cpsc.ucalgary.ca>
Tue, 23 Apr 91 20:59:18 MDT

The Calgary Sun (April 23 1991) reports that:

> A new plan to ease Canada's constitutional woes would see 260 people randomly picked by computer holding 'a constitutional jam session.'

Canada's constitutional woes revolve mostly around Quebec, a Canadian province which is considering seperation from Canada. The politicians want to let The People solve the problems, since they have failed pretty dismally themselves as of late. The suggestion for the computer selection of people to discuss (and presumably solve) the issues is strange to say the least, but comes from a retired Supreme Court judge, and is supported by various politicians from both major parties.

The risks are not with the computer-based selection itself, but with

the incorrect perception that such a selection is indeed random. Are those who are picked forced to participate? Are they paid, and if so, how does the payment compare to their job salary? Perhaps only those righ enough or dedicated enough to take a pay cut for a month or so will choose to participate. Are people who do not speak English or Franch (Canada's official languages) allowed to be "randomly selected"? Will the travel expenses of those who are selected but who are working out of the country be paid? At best, it would be a random selection from what amounts to a biased pre-selection.

Dan Freedman

"Risks" in selection of filenames!

<[anonymous]>
Tue, 23 Apr 91 12:43:13 XXT

Computer File Key To Murder?
ALEXANDRIA, Va. (AP)
Prosecutors said Tuesday that a former Marine captain was plotting his wife's death when he wrote computer entries including "How do I kill her?" and "What to do with the body?" Witnesses at the murder trial of Robert Peter Russell testified Tuesday that he also showed a lot of interest in his new wife's insurance policy, was found with another woman getting dressed in his quarters the weekend before his wedding, and asked a friend questions about how fast a body decomposes. He also asked about technique, inquiring of at least a couple of his fellow Marines whether it was true you could electrocute someone by lobbing a TV or radio into the bathtub with him, witnesses said.
But the key piece of evidence, exhibit 19A, is a 5 1/4 inch floppy disk on which Russell stored a file labeled "Murder." Assistant U.S. Attorney Lawrence J. Leiser said in his opening statement at Russell's trial that the defendant was concocting a "recipe for murder" when he created the computer entries under the heading "murder." Russell has pleaded innocent, contending the computer file was merely part of a mystery novel he was working on. He is free on $50,000 bond.
Sgt. Maj. William Joseph Kane, a 24-year Marine, testified that he found the computer disk when cleaning out Russell's office after the captain had been relieved of duty in February 1988, more than a year before his wife disappeared.
Most of the files on the disk were clearly military, but several caught Kane's interest, including one about him labeled with the sergeant major's name and one called "Murder." He read them, and a day later during a phone conversation with the captain's wife, Shirley, who was herself a Marine captain, Kane told her what he had found. "I told her if I was you, I'd be careful," Kane said. "I'd watch out for myself."
Other entries in the "Murder" file, according to court documents, include: "Make it look as if she left... Rehearse... Mask? Plastic bags over feet... Check in library on ways of murder electrocution?? Wash tarp!! I may need to cut it?"
Mrs. Russell, 29, disappeared from the Quantico Marine Corps Base in Virginia on March 4, 1989. Despite intense searches, her body has not been found. Russell, 34, is being tried in U.S. District Court in Alexandria, because, according to authorities, a crime was committed on federal property.

Russell's wife was stationed at Parris Island, S.C., in 1988, but she was later reassigned to Quantico and they were reunited. In the meantime, the Marines were moving to dishonorably discharge Russell, accusing him of alcoholism and misconduct that included filing false reports.

Premature ground contacts -- airplane software

Roland 24-Apr-1991 1604 <ouellette@tarkin.enet.dec.com>
Wed, 24 Apr 91 18:31:26 EDT

SEATTLE, WASHINGTON, U.S.A., 1991 APR 11 (NB) -- Honeywell has announced that it has issued new software to various US and foreign registry aircraft to correct a defect in a computerized flight navigation system that federal authorities said could send airliners off course. The problem arises when attempting a non-directional beacon approach for landing.

John Clabes, from the Oklahoma City Federal Aviation Office, read portions of a document issued by the FAA in Washington to Newsbytes. In part the document stated that "there has been a report of an erroneous course display on the navigation display map when the non-directional beacon approach was activated from the Honeywell Flight Management System database." The report continued, "This condition not corrected can result in the airplane deviating from the published course to the runway, which could lead to premature ground contact before reaching the runway." When Newsbytes asked Clabes if that was a euphemism for "crash" Clabes replied, "I guess that is what you could call that."

The airworthiness directive issued by the FAA mentioned the Boeing 747-400, 757 and 767 and the McDonnell Douglas MD-11 as being equipped with the faulty software. It states that 400 of these aircraft are US registered. Clabes told Newsbytes that a total of 795 aircraft worldwide are equipped with the system.

[...] The FAA airworthiness directive requires airlines to place placards next to the control panels of their aircraft, warning pilots not to attempt the nondirectional beacon approach. FAA spokesperson David Duff said nondirectional beacon approaches were rarely used in the United States because most airports have instrument landing system (ILS) approaches. The FAA airworthiness directive says it may consider further rule-making at a later time.

"`Traffic crystal ball' may be in your car's future" (Chi. Trib. 4/23/91)

Jeff Helgesen <jmh@morgana.pubserv.com>
Wed, 24 Apr 91 12:37:00 -0500

The following article appeared in the Chicago Tribune. I have taken the liberty of omitting non-salient paragraphs. Jeff

"`TRAFFIC CRYSTAL BALL' MAY BE IN YOUR CAR'S FUTURE"
Chicago Tribune - Tuesday, April 23, 1991 (Gary Washburn)

Announcement of an experimental traffic management project here, which would

have computers in cars to tell drivers when to get off one highway and onto another to avoid tie-ups, could come as early as next month, transportation sources said Monday. The futuristic system could be installed and operating in about two years, they said.

U.S. Transportation Secretary Samuel Skinner touched on the system at a speech in Chicago on Monday, saying it is called ADVANCE. ``I don't want to get into all the details,'' Skinner told reporters after the speech. ``A lot of people need to be involved. But I think there is good news to come...You will be hearing more about it soon.''

One person who is familiar with the project explained further. ``In layman's terms, this would provide an on-board computer for you that would give you real-time traffic conditions ant tell you what alternate routes to select,'' he said. In addition, the car computers would contribute new data to the central computer based on traffic conditions that they encounter, and this information would quickly become available to other drivers, he said. Transportation experts say that such ``intelligent vehicle'' systems may be able to smooth traffic flow and ease congestion without any new pavement being laid.

The details about the ADVANCE project include:

- It has been under study for at least a year, under the auspices of the state and federal governments, with participation from researchers from the University of Illinois at Chicago, Northwestern University and Motorola, Inc.

- It will involve 4,000 specially-equipped vehicles.

- It will cover 250 square miles in the highly congested northwest suburbs, targeting oft-clogged arterials that could include such bust thoroughfares as Palatine, Algonquin, Golf and Higgins Roads.

The Chicago area's expressway system already has sensors embedded in the pavement. Those sensors feed congestion information to a central computer operated by the Illinois Department of Transportation. In turn, this computer supplies data to radio stations and traffic reporting services. But the metropolitan area's suburban arterials do not have such sophisticated monitors, and motorists often have no way of knowing up-to-the-minute conditions on the road they use.

When people visit the supermarket, they choose their checkout lanes based on the length of lines, the speed of clerks and baggers and other data, Skinner said in his speech, one in the Bright New City lecture series. ``We make an informed decision,'' he said. ``That same logic [should apply] to the highways of this country,'' he asserted. ``Why shouldn't you have a computer in your car that shows you how fast traffic is moving...where it is moving quicker, where the delays are, where the accidents are, where the congestion is, where the construction is? Why shouldn't we let you make informed decisions?''

European and Japanese companies are rushing to develop smart-car technology as efforts in this country advance.

A year ago, Skinner announced an $8 million project to install computerized traffic displays in 100 cars in Orlando. More recently, a $1.7 million project called Pathfinder has begun on a 13-mile stretch of California freeway between Los Angeles and Santa Monica. Twenty-five specially-equipped cars receive up-to-date information about accidents, congestion, highway construction and alternate routes.

But the proposed project here would be much larger.

The potential for computerized traffic management systems is ``immense,'' said Rich Schuman, manager of technical information for the Intelligent Vehicle Highway Society of America, a not-for-profit group that promotes the new approach.

Response to Rude Behavior

<WHMurray@DOCKMASTER.NCSC.MIL>
Wed, 24 Apr 91 08:45 EDT

It is time to decide what kind of a network we want.

Given the age of our users, the novelty of the environment, and the absence of authority, the internet is a surprisingly orderly place. Who would have believed that a multi-institutional, multi-national network of peers could be so orderly?.

However, now we stand challenged by a group of puerile rogues, in a rogue institution, in a rogue nation. They insist upon their right to behave in a rude and disorderly manner. They flaunt their behavior and invite those of us who do not like it to withdraw from the field.

They must be made to understand that that is the natural consequence of their behavior. The marginal propensity to connect to the net is a function of how useful and how orderly it is. If it becomes too disorderly, it will collapse.

The rest of us also need to understand it. If we tolerate this behavior, the network may collapse.

What are our options? We seem to be paralyzed. We have followed Cliff Stoll's "scientific/law-enforcement" approach for six months. Having found that the rogues are in a rogue institution in a rogue nation, where law enforcement is powerless, we do not seem to remember what to do next.

Unless we want a network that depends upon law enforcement for its order, and which is subject to their authority, we should not have turned to them in the first place. Cliff's skill and daring notwithstanding, his model is wrong. He did the wrong thing. We have done the wrong thing in following his example.

If you observe rogue behavior at the perimeter to your system, break the connection. Inform the adjacent node why you have done so. If they are not the source of the behavior, encourage them to follow your example. The closer we break the connection to the source of the behavior, the sooner it will stop.

I guarantee it.

We should not, we must not, we dare not tolerate this behavior. If we must isolate the University of Utrecht, then we must. If we must isolate all of Holland, then so be it. We must not shrink. The order and the future of the network depend upon it.

Ostracism has always been the most powerful and successful of all social controls. It dwarfs law enforcement in its power. In the modern world it is so Draconian that we are reluctant to use it. We may have forgotten how to use it. We may have forgotten all about it. However, this is a case that justifies its use. The protection of the order and organization of the network justify its use. In a community of peers, it is the only one with any opportunity of success. It is the only one that will preserve the community.

William Hugh Murray, 21 Locust Avenue, Suite 2D, New Canaan, Connecticut 06840
203 966 4769, WHMurray at DOCKMASTER.NCSC.MIL

Re: Dutch crackers and irresponsible officials (Blinn, RISKS-11.51)]

Brinton Cooper <abc@BRL.MIL>
Wed, 24 Apr 91 15:30:24 EDT

The time has come to put this debate behind us. Clearly, as with burglary of an unlocked home or theft of a car with keys hanging from the ignition, carelessness by the owner does not set aside the guilt of the perpetrator. Conversely, carelessness by the owner does not relieve her/him of responsibility for the loss. In the "Dutch cracker" incident, perhaps BOTH the cracker's host and the host with known, repairable security holes should be barred from the Internet.

_Brint

One-time Passwords

<*WHMurray@DOCKMASTER.NCSC.MIL*>
Wed, 24 Apr 91 19:45 EDT

It seems (from the amount of "hate mail" that I have received) that I erred when I assumed that most readers of RISKS would recognize the concept of (token-based) one-time passwords. I have now been disabused of this assumption. I will explicate this concept as quickly and as briefly as I can.

However, there are many ramifications to the use of these mechanisms that I will not go into. Please try not to infer too much from what I do not say. My experience is that many people are intuitively hostile to this idea, that it is difficult to describe in words, and and that it is very easy to demonstrate. Please give me credit for trying, and the benefit of the doubt when necessary. Remember that what we are comparing is not working.

These mechanisms rely upon the fact that attacks passwords would not be

efficient if the password had no residual value. The only time that this will be true is if the password is only used once.

Therefore, the mechanisms generate and expect a new password for each session. While computers are very good at this, people are very poor (for many of the same reasons that they are bad at selecting and managing reusable passwords.) Therefore, we provide them with little tiny computers, tailored to this purpose, and generically called "tokens."

These special purpose computers are used by the computer user to determine what password to use for a given session. The user need not generate the password. He need not remember it. He need not write it down. He must carry the token.

Each token is "seeded" with one or more values (one for each independent security domain in which the user must operate). The value(s) that the token contains makes it unique. It is not like any other in the world. There is no non-destructive way to determine the value from the token. Therefore, the token cannot be counterfeited.

The token uses the seed value, and perhaps other values, to determine the instant password. (For those of you familiar with the concept, it employs a "non-disclosure" or "zero-knowledge" proof to demonstrate that is has beneficial use of the seed value.) The optional values may include time, a challenge, and/or a personal identification number. (These provide protection against "play-back" or "mid-night" attacks.)

Tokens come in many forms. Users may sometimes choose the form that they prefer. Popular forms include credit cards, calculators, and keys.

In one scenario, when prompted for the password, the user looks at the token, reads the current password from the display, and enters it at the keyboard. In another, the password prompt is replaced by a "challenge" value. The user reads the challenge from the terminal, enters it on the token's keyboard, reads the "response" to the challenge from the token's display and enters it on the terminal's keyboard.

If the token is lost, it can be revoked. Since the user cannot use the target system without the token, unlike the compromised password, he will notice. Thus, the window of vulnerability is very narrow. It can be narrowed further through the use of personal identification numbers, signature verification, and speaker verification. However, the marginal security of the latter two may be small when compared to their cost.

This technology is mature, widely available, and widely supported. It is clearly supported on the popular platform types within the internet. It is both effective and efficient. That is, it works, and it covers its own cost.

The cost is measured in the tens of dollars per user. While this seems high when multiplied by the number of users, anything seems high when multiplied by the users. When compared to the other costs of computing, it is trivial. When compared to the cost of losses offset, it is attractive.

It is much more effective and efficient than other security measures, such as access control, that we take for granted. It is clearly more effective and

efficient than these other are in its absence, since in its absence the other mechanisms are not effective.

Search RISKS using swish-e

THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

ACM Committee on Computers and Public Policy, Peter G. Neumann, moderator

Volume 11: Issue 54

Thursday 25 April 1991

Contents

"Alleged Cable Pirates Caught in Electronic Trap"

"Peter G. Neumann" <neumann@csl.sri.com>
Thu, 25 Apr 91 9:09:06 PDT

An article by George James probably from today's New York Times (I saw it replayed in today's San Francisco Chronicle, p. A6) describes a successful effort by American Cablevision of Queens (NY) to trap customers who had illegally installed chips that let them pick up a variety of premium cable channels for free. After analysis of ONE of the bogus chips, American Cablevision was able to construct a signal (an "electronic bullet") whose

transmission disabled just the bogus chips, leaving the legitimate access control boxes unaffected. They then simply waited to catch the 317 customers who called in to complain that their screens had gone dark -- and who were asked to bring in their boxes, which American Cablevision then kept. "If convicted, the subscribers could face fines of up to $100,000."

[Able Cable-Caper Sting-Thing Zaps Chips, Nabs Fabs.
Potential Variety headline? PGN]

Dutch nation portrayed as a bunch of network bashers

Ralph 'Hairy' Moonen <rmoonen@hvlpa.att.com>
Thu, 25 Apr 91 09:59 MDT

As a citizen of the Netherlands, I must take offense at the remarks made by several people that the Netherlands are a law-less and a-social country.

Bill Murray portrayes Holland in this way in RISKS 11.53. While I agree with him that the behaviour of the Dutch crackers isn't correct, you have to understand that unlike America has shown in it's operation Sundevil, Holland has a legislative system wherein someone is innocent untill proven guilty. This means that not the laws fail in Holland (the crackers could easily be busted for telephone-wire fraud) but that the burden of proof lies with the Dutch State. As you can imagine, this is a delicate matter. How does one prove, short of catching someone in the act, that Mr. A. was behind the keyboard at that time, doing such-and-such?

Furthermore, I might add, that the media information has been incomplete, in that the Dutch crackers used Utrecht to crack several universities in the States, and _proceeded to crack other systems from there_. Following the line of argument that Bill Murray used, these universities should also be barred from the net, and yes, perhaps the whole of America should be.

The problem is not that one single country lacks a powerfull law enforcement and acts as a rogue nation and hacker-haven. The problem is that as long as people can get onto the net, (students, 'authorised' personnel, outsiders, and whatever) security will have to be a major issue. Not just the issue of one single university like Utrecht, but of ALL sites on the internet. Because you do realise that a smart cracker could get away with this just as easily in the States as in Holland? So don't lay any guilt-trip on the Dutch will you?

* Ralph Moonen, (+31) 35-871380

Re: "University Exec Backs Hacking" (Dutch crackers, RISKS-11.50,51)

Piet van Oostrum <piet@cs.ruu.nl>
Thu, 25 Apr 91 17:03:58 met

I don't think Mr. Rook knows much about computer networks. From what I know about the incident (I haven't seen the TV program) this could have been done from Every site on the Internet that has a Decnet node. And I agree that it is

the responsability of each site to prevent break-ins into their own computers.

Well, apparently he doesn't know that his own university does not condone any attempt to break into other systems. Our (computer science) students know this very well, and risk being excluded from computer access if they try. Delft University (not: the prestigious ..) had (or has) a course in computer security (not in hacking), where one of the assignments of the students was to find security weaknesses in computer systems. Yes, we try to encourage exploration but also responsability and ethical behaviour.

Piet* van Oostrum, Dept of Computer Science, Utrecht University, Padualaan 14, 3508 TB Utrecht, The Netherlands. +31 30 531806 uunet!mcsun!ruuinf!piet

---

Re: response to rude behavior

<mike@vort.cpsc.ucalgary.ca>
Thu, 25 Apr 91 01:26:27 MDT

I too am part of this community, and I dismiss WHMurray's recent article (comp.risks 11.53) as a blatantly obvious piece of fear-mongering.

Murray's attempt to isolate an entire nation from the free flow of information would be scary if it weren't so wretchedly silly and patently self-serving.

>William Hugh Murray, Executive Consultant, Information System Security
^^^^^^^^^^^^^^^^^^^^^^^^^^^^

And guess who'd love to take on the job of setting himself up as the Leader of the DataPolice? Kids, be the first one on your block to have an Empire! Follow in the steps of Hitler, Stalin, and Hoover. You too can have a full and exciting career as a demogogue.

P.S. Who said: "Those who give up a little freedom for a little security will soon have neither freedom nor security." ?

Mike Nemeth VORT Computing (403) 261-5015 ...calgary!vort!mike

---

trespassing and common law

Phil Agre <phila@cogs.sussex.ac.uk>
Thu, 25 Apr 91 11:56:09 +0100

Steve Bellovin (RISKS-11.52) points out that the US only requires a landowner to put up a "no trespassing" sign to make trespassing illegal. A complementary point to make is that both English and American common law gives me the permanent right to walk across your property if I have been doing so regularly with your knowledge for some substantial amount of time. If the trespassing analogy is to apply to computer cracking, then this flip-side would seem to apply as well.

Phil Agre, University of Sussex

Free Speech and Government Control of Information

Larry Hunter <hunter@nlm.nih.gov>
Tue, 23 Apr 91 14:23:36 EDT

In RISKS 11.51 Jerry Leichter claims that "in an information age we will find it necessary to control access to and dissemination of certain classes of information. In fact, we already do this." He proceeds to argue that defending encryption on free speech grounds is misguided. He is wrong both about the current state of government control of information and about what is desirable policy. The first amendment quite explicitly prohibits government controls of expression (i.e. communication of information) with very few exceptions, and I suggest that the current governmental attacks on this most basic right are pernicious and must be fought.

Leichter's examples from crime and commerce are deceptive. One's first amendment rights of free speech do not exempt all expressive acts from prosecution. There is a large body of law that addresses the issue of when expression becomes action. Some examples include conspiracies, slander, copyright violations, and reckless endangerment (e.g. yelling "fire" in a crowded theater). What is prohibited is prosecution for _mere_ expression, even if individuals, organizations or the government would rather keep the information secret. As long as I am not conspiring to commit fraud or some other crime, I can publish your credit card number, or your swiss bank account number, or your income, etc. in a magazine article without fear of government prosecution. And I believe that ability to express things that make some people uncomfortable is a vital part of basic American liberty.

Leichter's second example involves restrictions on a company selling credit or other private records. Commercial speech is regulated very differently than individual speech. For example, commercial advertising must not be false or deceptive (well, at least in law), and there are specific legal limits on the disclosures that credit bureaus, common carriers, doctors, lawyers, etc. can make under most circumstances. Commercial entities do not have the same free speech rights that individuals do.

Finally, Leichter points out the National Security exception to freedom of expression, which, as he notes, is both pervasive, and, in the case of "born classified" information, constitutionally suspect.

Leichter concludes by recommending a couple of science fiction stories about social control of information. Interesting as those stories are, let me suggest that you also read Thomas Emerson's "The System of Freedom of Expression."

Any abridgement of a constitutional right must either balance a competing right or serve some compelling state interest. What compelling state interest could be sufficient to infringe on our rights to free expression and privacy by effectively prohibiting effective encryption? Surely the routine prosecutorial needs of the state can be met without recourse to such invasive, undiscriminating measures. Terrorism may be a threat, but not such a compelling one that we as a society ought to sacrifice one of our most basic constitutional rights in order to _possibly_ reduce the chance of a _potential_

attack.

Technology can be used either to enhance or degrade the status of rights such as freedom of expression and privacy. Inexpensive, effective encryption is a basic enabling technology that empowers individuals in an increasingly technologically invasive society. I believe it should be defended against government attack in the strongest possible terms.

Lawrence Hunter, National Library of Medicine

[Please note that I am neither a lawyer nor am I speaking as a representative of the government.]

Re: Responsibilities of Internet sites (Pereira, RISKS-11.52)

Mike Godwin <mnemonic@eff.org>
Wed, 24 Apr 91 10:29:47 EDT

>1) I know of no area of human activity in which wilfull intrusion or condoning
>intrusion are seen as no more condemnable as failure to protect one's domain
>from intrusion to the best of one's ability.

In tort law, the law of trespass is balanced by the law concerning the negligence of those who maintain attractive nuisances.

The issue is not whether computer trespass is wrong, but whether it is just to punish the trespassers without imposing any liability upon those who failed to meet minimum standards of computer security.

It is a fact that every generation faces the challenge of overcoming a wave of barbarians--its own children. Is it wise social policy to send young men to prison for doing the kinds of things that not-yet-fully-socialized young men invariably do while imposing no social responsibility upon those charged with maintaining system security? That is a question that has not been fully debated.

It will never be fully discussed so long as too many people suppose that the wrongness of trespass decides all the legal and ethical questions raised by computer intrusion. It does not.

--Mike

Mike Godwin, EFF, Cambridge, MA, mnemonic@eff.org, (617) 864-0665

[oneel: re: Dutch hackers and KSC [Kennedy Space Center]]

Brinton Cooper <abc@BRL.MIL>
Wed, 24 Apr 91 20:31:24 EDT

Brice O'Neel writes

> I don't believe that KSC is on the internet.

Try 128.217.11.25 (nasa2.ksc.nasa.gov). More are vulnerable than you dreamed of. I never dreamed, for example, that OSHA is on the Internet (not that it matters, mind you).

_Brint

[KSC's presence on the Internet was also noted by Ari Ollikainen (ari@OldAhwahnee.Stanford.Edu), as reported somewhat red-facedly by oneel@heawk1 (Bruce Oneel).

Re: Dutch hackers and KSC

301)286-5223 <TENCATI@NSSDCB.GSFC.NASA.GOV (NSI Security Manager>
Tue, 23 Apr 1991 19:32:46 EDT

I have received NO incident reports indicating that any KSC systems were hacked, or involved in any hacking incidents relating to the Dutch hacker case.

Ron Tencati, Security Manager, NASA Science Internet (NSI)
Coordinator, NSI-CERT, STX/Code 930.4/Goddard Space Flight Center/Greenbelt,MD

Re: Letter to Senators on SB 266 (Engler, RISKS-11.51)

Theodore Ts'o <tytso@ATHENA.MIT.EDU>
Tue, 23 Apr 91 02:09:55 EDT

As previous posters have noted when the Lotus Marketplace controversy was taking place, sending form letters to your representatives is not terribly productive; the Senators' or Represatitive's staff are fairly good about detecting (and disregarding) form letters. If, however, you write your own letter and send it off, it will be given much more weight, since presumably it mattered enough to you to write your own letter. I do urge everyone to write his/her own letter and send it off to Biden as well as your own Senators and Representatives. If we raise enough fuss, hopefully the bill will be allowed to die while it's still in committee.

- Ted

Re: Trains collide in east London (RISKS-11.52)

Ian G Batten <I.G.Batten@fulcrum.bt.co.uk>
Thu, 25 Apr 91 08:37:36 BST

With respect to the London Docklands Light Railway incident, the report in RISKS-11.52 ("Computer-controlled commuter trains collide...") misses one vital point. The train that was hit was under manual control, following an earlier failure.

ian

Search RISKS using swish-e

Report problems with the web pages to the maintainer

Search RISKS using swish-e

THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

ACM Committee on Computers and Public Policy, Peter G. Neumann, moderator

Volume 11: Issue 55

Monday 29 April 1991

Contents

Four-digit address causes NYC death

Ed Nilges <EGNILGES@pucc.princeton.edu>
Thu, 25 Apr 91 12:11:32 EDT

The television news program News 4 New York, this morning, reported the death of a man because EMS (emergency medical service) technicians could not locate his apartment building. It was reported that the man lived at a building with a five digit address but the system used to dispatch EMS technicians only allows a four digit address.

I will report more on this risk story if it appears in the New York Times today and no-one else on the network has further details, but I'd remark that most programming languages encourage the apparent error responsible for this tragedy. To my knowledge, only REXX and certain Basic interpreters allow completely variable length strings, which would have perhaps avoided the problem (barring screen design considerations, of course.) In C, you must either malloc or decide in advance the maximum length of a field, and in practice this decision is usually made in secret by the programmer rather than reviewed by the end user.

Since truncation of fields usually affects "the real end user" (that is, the general public in the form of customers, students, victims, and in this case patients) I believe that there is not enough commercial motivation to provide programming languages and systems that avoid the preconditions for this problem. How about legislation concerning responsible display and capture of COMPLETE information? Or, at the level of civil lawsuits, the fact that a defendant's system truncates data should always weigh against the defendant.

Almost Humorous Fly-by-Wire Glitch

Joseph Nathan Hall <jnh@eceugs.ece.ncsu.edu>
Sat, 27 Apr 91 01:36:40 EDT

>From the pages of Popular Science, April 1991:

"...Spectators at the first flight of Northrop's [YF-23] prototype noticed its huge all-moving tails--each larger than a small fighter's wing--quivering like butterfly wings as the airplane taxied out to the runway. Test pilot [Paul] Metz says this occurred because the early generation flight-control software didn't include instructions to ignore motions in the airframe caused by pavement bumps. The answer, he adds, is inserting lines of computer code that tell the system not to try to correct for conditions sensed when the fighter's full weight is on its nose gear."

I'll grant that in the 1990s we can analyze wind-tunnel tests in a few hours (or less) and can even simulate untested airframes with some success. In the 1950s pilots frequently flew prototypes before the final results of early wind-tunnel tests were completely analyzed--a process that sometimes took weeks or months. But am I alone in thinking that in some respects it takes more chutzpah to test-fly one of these modern fly-by-wire wonders?

<shudder>

Joseph Hall, Student, sometimes Applications Programmer, NC State University

---

Another article: Freedom of Information vs Computers

Bob Frankston <Bob_Frankston%Slate_Corporation@mcimail.com>
Mon, 29 Apr 91 15:36 GMT

The article is in Computerworld April 29th, 1991, page 1. The leadin is a battle over whether an agency should release its data in the original machine readable tape format or on "more than 1 million sheets of paper". The article touches on some real issues of representation -- how much work should be done to transform representations to what the requestor wants and the costs of paper-intensive approaches.

In the case of the initial example, part of the rationale for not releasing the information in machine readable format is that "it wanted to discourage commercial enterprises from making big profits off of the city's data-gathering efforts". This does acknowledge that information in machine readable form is

very different from paper. Did the authors of the Freedom Of Information Act foresee the differences between paper and machine-readable data? What does the mean to privacy? The census bureau works hard to protect privacy when it releases its data. Does the FOI mean that raw, less guarded, data will become readily available? Can I search real-estate databases to find out where someone has lived for the last 20 years? To search arrest (not conviction, simply arrest) records?

The article ends with "In the long run, it would be best for FOI requesters and agency FOI officers if government information systems were designed from the outset to allow for ad hoc queries and public access, according to several experts. Ideally, that would be just good IS management practice, but Podesta said that agencies need the prodding of a legislative mandate to consider the [technical??] issues of public access at the start of systems design.". While this is true, they should also consider the implications of such access.

Re: Cable TV "bullet"

<[anonymous]>
Mon, 29 Apr 91 09:09:06 xxx

Some people have asked how a "pirate" receiving cable channels illegally could be dumb enough to turn themselves in when the service stops? Pirates who know what they're doing WOULDN'T be turning themselves in.

But most of these folks in question are otherwise legitimate cable subscribers who have been "sold" a modification to their cable boxes, MOST OFTEN BY A CROOKED CABLE COMPANY INSTALLER or other "legitimate" sounding entity who tells them that it is perfectly legit--that it's just another way of paying for the service. OK, so these people are gullible--but look at all the other scams people fall for every day. Their box goes out-- they call the cable company. These are most often ordinary folks, not "sophisticated" pirates.

Similar scenaries have occurred with satellite TV, where crooked dealers tell their customers that instead of paying a monthly fee for services they can pay a lump sum and that it's all legit. Of course it's not. And just like in the cable case, if the service is cutoff these folks will usually call up the service wondering what went wrong.

The news stories on the "cable bullet" are making a big deal acting as if this technique could be easily applied to all systems. The incident in question involved one PARTICULAR BRAND of cable box, which was being subverted by a particular technique. There is no "broad spectrum" method for doing the same thing on a wide variety of boxes (of which there are many types), and many existing designs would make such a "bullet" approach impossible. Also, even for the affected boxes, the odds are that the folks making the modifications will find an alternate method for illicit enabling of the boxes, and so the war of the countermeasures escalates into the future...

Re: London Automatic Train Crash

Rupert Goodwins <rupertg@cix.compulink.co.uk>
Sat, 27 Apr 91 16:11 GMT

More on Docklands Light Railway (DLR), that was reported in RISKS-11.52 as having had two of its unmanned trains collide. This was reported in UK newspapers, together with a picture which looked like nothing so much as two model trains having collided on a set of points. This hasn't been the first incident; during testing, a train over-ran its buffers. Since a large part of the DLR is elevated, the train in question ended up hanging off the end of the track some thirty feet above the ground.

I got an indication of the state of the routing software when I travelled on the DLR about three years ago (during that time, I worked in Docklands). The train drew to a halt on an empty bit of elevated track, waited for a couple of minutes, and then carried on. On checking with a DLR official, it transpired that there was due to be a development there at the time the routing software was written; due to various financial factors the building had been delayed but DLR had already included it in the software which, having been tested, they were unwilling or unable to modify. There is now a building at that site (the infamous Canary Wharf), but I haven't been back on the DLR subsequently.

Rupert Goodwins, East Ham, London.

1st CFV: comp.lsi.testing

<koo@tcville.HAC.COM>
29 Apr 91 21:05:58 GMT

Below is a Call For Votes to create a newsgroup on testability/reliability issues. Please send your Yes/No vote to the address indicated below.

Frances (koo@tcville.hac.com)

- - 8< - - - - - - - cut here - - - - - - - - cut here - - - - - - - - - >8 - -

Date: 26 Apr 91 18:19:48 GMT
From: gouders@du9ds3.uni-duisburg.de (Nikolaus Gouders)
Newsgroups: comp.lang.vhdl
Subject: 1st CFV: comp.lsi.testing (was: comp.lsi.cat)
Summary: call for votes
Keywords: comp.lsi.testing
Organization: Rechenzentrum Uni-Duisburg

CALL FOR VOTES for comp.lsi.testing (was: comp.lsi.cat)
==========

SUMMARY:
Newsgroup: comp.lsi.testing
Yes votes to: yes@du9ds3.uni-duisburg.de
No votes to: no@du9ds3.uni-duisburg.de
Voting period: April 29th, 1991 to May 20th, 1991 (inclusive)

NAME/GROUP:
comp.lsi.testing

STATUS:
unmoderated

CHARTER:
This newsgroup is intended to cover all aspects of the testing of electronic circuits such as (but not restricted to)

* Testing of Digital and Analog Devices
* Automatic Test Pattern Generation
* Fault Modeling and Fault Simulation
* Design for Testability
* Scan Design and Built-in Self Test
* PCB-Test and Boundary Scan
* Design Verification

Important topics are (again not restricted to)

* Announcements (conferences, workshops, special issues)
* Books on testing
* Standards
* Tools
* Benchmarks
* Questions and answers
* Discussions concerning technical or algorithmic problems

WHY A NEW GROUP:
The ever increasing number of publications on testing shows a vivid and growing interest in that subject. A newsgroup on testing will stimulate and accelerate the exchange of related information among interested network users. It makes it easier to recognize current trends in testing, especially for novices.

The discussion period showed a general agreement on the theme. Our first proposal for the name of the group was comp.lsi.cat, which is similiar to comp.lsi.cad. A number of contributors remarked that this name is not generally understandable or misleading. Among the proposed alternatives were: comp.lsi.test, comp.lsi.testing, comp.lsi.ate, comp.lsi.ft (fault tolerance). Taking into account that ".test" may sound like "alt.test", "news.test" which have a specific function within the USENET hierarchy, the proposed name "comp.lsi.testing" should be the most understandable and general one.

Some authors commented that there are existing groups like comp.lsi which do not have an extreme news flow to date. Splitting therefore should not be necessary. We have never intended to split any group due to "net bandwidth", comp.lsi.testing is a new thread. A closer look at comp.lsi[.cad] shows that these groups are mostly design oriented, and this probably raises the level for participation of non-designers. Shortly: there was and is no forum for testing yet.

SCHEDULE OF THE VOTE

The voting period begins on monday, april 29th and ends at (including) sunday, 20th.
Everybody is allowed to send one and only one vote for (YES) or against (NO) comp.lsi.testing. All votes reaching the addresses described below during the voting period will be counted. Votes arriving not during the period, duplicate votes, votes containing additional comments ("I vote YES, but...") are VOID.

HOW TO VOTE

Please send your vote to one of the following addresses:
YES votes to:
yes@du9ds3.uni-duisburg.de
NO votes to:
no@du9ds3.uni-duisburg.de

Please put your vote in the subject of the mail-header. Format:
subject: YES comp.lsi.testing or
subject: NO comp.lsi.testing

Your mail MUST contain an e-mail adress to contact you (e.g. a .signature) to allow verification of the results.

DO NOT SEND ANY VOTE TO A NEWSGROUP (for instance the group where you read this call for votes).

RESULTS

After the end of the voting period, the voting results will be published in the newsgroups "news.groups" and "news.announce.newgroups" including names, e-mail addresses and votes of the voters.

To create the newsgroup "comp.lsi.testing" it is necessary that there are at least 100 more YES than NO votes, and there must be a 2/3 majority of YES voters.

PUBLICATION

This call for votes will be sent to
news.announce.newgroups
news.groups
comp.lsi
comp.lsi.cad
comp.simulation
comp.lang.vhdl
and some e-mail addresses.

You may freely distribute, translate, republish, crosspost etc. this article as long as the parts SCHEDULE OF THE VOTE and HOW TO VOTE remain unchanged and the names of the authors are included.

Please send us your vote soon!

The authors:

Nikolaus Gouders (gouders@du9ds3.uni-duisburg.de)
Holger Veit (veit@du9ds3.uni-duisburg.de)
--
Nikolaus Gouders		***
University of Duisburg		INTERNET: gouders@du9ds3.uni-duisburg.de
Fac. of Electr. Eng.		BITNET: gouders%du9ds3.uni-duisburg.de@UNIDO
Dept. f. Dataprocessing		***

- - 8< - - - - - - - cut here - - - - - - - - cut here - - - - - - - - - >8 - -

Search RISKS using swish-e

THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

ACM Committee on Computers and Public Policy, Peter G. Neumann, moderator

Volume 11: Issue 56

Monday 29 April 1991

Contents

Jerry Sweet: [comp.dcom.telecom: Prodigy and GEnie hate and rumors]

the terminal of Geoff Goodfellow <geoff@fernwood.mpk.ca.us>
Mon, 29 Apr 91 07:31:47 MST

------- Forwarded Message

Date: Sun, 28 Apr 91 22:44:01 MST
From: Jerry Sweet <jns@fernwood.mpk.ca.us>
Subject: [comp.dcom.telecom: Prodigy and GEnie hate and rumors]
To: "Jerry's Clipping Service":;@fernwood.mpk.ca.us

3 items:
- Prodigy or Fraudigy ???
- Prodigy Questions
- GEnie Management Acting a la Prodigy Management?

- ------- Forwarded Messages

Date: 26 Apr 91 19:09:50 GMT
From: overlf!emanuele@kb2ear.ampr.org (Mark A. Emanuele)
Subject: Prodigy or Fraudigy ???

I just downloaded this from a local bbs and thought it might be interesting.

BEGIN BBS FILE

218/250: Fraudigy
Name: George J Marengo #199 @6974
From: The Gangs of Vista (Southern California) 619-758-5920

The L. A. County District Attorney is formally investigating PRODIGY for deceptive trade practices. I have spoken with the investigator assigned (who called me just this morning, February 22, 1991).

We are free to announce the fact of the investigation. Anyone can file a complaint. From anywhere.

The address is:

District Attorney's Office
Department of Consumer Protection
Attn: RICH GOLDSTEIN, Investigator
Hall of Records Room 540
320 West Temple Street
Los Angeles, CA 90012

Rich doesn't want phone calls, he wants simple written statements and copies (no originals) of any relevant documents attached. He will call the individuals as needed, he doesn't want his phone ringing off the hook, but you may call him if it is urgent at 1-213-974-3981.

PLEASE READ THIS SECTION EXTRA CAREFULLY. YOU NEED NOT BE IN CALIFORNIA TO FILE!!

If any of us "locals" want to discuss this, call me at the Office Numbers: (818) 989-2434; (213) 874-4044. Remember, the next time you pay your property taxes, this is what you are supposed to be getting ... service. Flat rate? [laugh] BTW, THE COUNTY IS REPRESENTING THE STATE OF CALIFORNIA. This ISN'T limited to L. A. County and complaints are welcome from ANYWHERE in the Country or the world. The idea is investigation of specific Code Sections and if a Nationwide Pattern is shown, all the better.

LARRY ROSENBERG, ATTY

Prodigy: More of a Prodigy Than We Think?
By: Linda Houser Rohbough

The stigma that haunts child prodigies is that they are difficult to get along with, mischievous and occasionally, just flat dangerous, using innocence to trick us. I wonder if that label fits Prodigy, Sears and IBM's telecommunications network?

Those of you who read my December article know that I was tipped off at COMDEX to look at a Prodigy file, created when Prodigy is loaded STAGE.DAT. I was told I would find in that file personal information form my hard disk unrelated to Prodigy. As you know, I did find copies of the source code to our

product FastTrack, in STAGE.DAT. The fact that they were there at all gave me the same feeling of violation as the last time my home was broken into by burglars.

I invited you to look at your own STAGE.DAT file, if you're a Prodigy user, and see if you found anything suspect. Since then I have had numerous calls with reports of similar finds, everything from private patient medical information to classified government information.

The danger is Prodigy is uploading STAGE.DAT and taking a look at your private business. Why? My guess is marketing research, which is expensive through legitimate channels, and unwelcomed by you and I. The question now is: Is it on purpose, or a mistake? One caller theorizes that it is a bug. He looked at STAGE.DAT with a piece of software he wrote to look at the physical location of data on the hard disk, and found that his STAGE.DAT file allocated 950,272 bytes of disk space for storage.

Prodigy stored information about the sections viewed frequently and the data needed to draw those screens in STAGE.DAT. Service would be faster with information stored on the PC rather then the same information being downloaded from Prodigy each time.

That's a viable theory because ASCII evidence of those screens shots can be found in STAGE.DAT, along with AUTOEXEC.BAT and path information. I am led to belive that the path and system configuration (in RAM) are diddled with and then restored to previous settings upon exit. So the theory goes, in allocating that disk space, Prodigy accidently includes data left after an erasure (As you know, DOS does not wipe clean the space that deleted files took on the hard disk, but merely marked the space as vacant in the File Allocation Table.)

There are a couple of problems with this theory. One is that it assumes that the space was all allocated at once, meaning all 950,272 bytes were absorbed at one time. That simply isn't true. My STAGE.DAT was 250,000+ bytes after the first time I used Prodigy. The second assumption is that Prodigy didn't want the personal information; it was getting it accidently in uploading and downloading to and from STAGE.DAT. The E-mail controversy with Prodigy throws doubt upon that. The E-mail controversy started because people were finding mail they sent with comments about Prodigy or the E-mail, especially negative ones, didn't ever arrive. Now Prodigy is saying they don't actually read the mail, they just have the computer scan it for key terms, and delete those messages because they are responsible for what happens on Prodigy.

I received a call from someone from another user group who read our newsletter and is very involved in telecommunications. He installed and ran Prodigy on a freshly formatted 3.5 inch 1.44 meg disk. Sure enough, upon checking STAGE.DAT he discovered personal data from his hard disk that could not have been left there after an erasure. He had a very difficult time trying to get someone at Prodigy to talk to about this.

Excerpt of email on the above subject:

THERE'S A FILE ON THIS BOARD CALLED 'FRAUDIGY.ZIP' THAT I SUGGEST ALL WHO USE THE PRODIGY SERVICE TAKE ***VERY*** SERIOUSLY. THE FILE DESCRIBES HOW THE PRODIGY SERVICE SEEMS TO SCAN YOUR HARD DRIVE FOR PERSONAL INFORMATION, DUMPS IT INTO A FILE IN THE PRODIGY SUB-DIRECTORY CALLED 'STAGE.DAT' AND WHILE YOU'RE WAITING AND WAITING FOR THAT NEXT MENU COME UP, THEY'RE UPLOADING YOUR STUFF AND LOOKING AT IT.

TODAY I WAS IN BABBAGES'S, ECHELON TALKING TO TIM WHEN A GENTLEMAN WALKED IN, HEARD OUR DISCUSSION, AND PIPED IN THAT HE WAS A COLUMNIST ON PRODIGY. HE SAID THAT THE INFO FOUND IN 'FRAUDIGY.ZIP' WAS INDEED TRUE AND THAT IF YOU READ YOUR ON-LINE AGREEMENT CLOSELY, IT SAYS THAT YOU SIGN ALL RIGHTS TO YOUR COMPUTER AND ITS CONTENTS TO PRODIGY, IBM & SEARS WHEN YOU AGREE TO THE SERVICE.

I TRIED THE TESTS SUGGESTED IN 'FRAUDIGY.ZIP' WITH A VIRGIN 'PRODIGY' KIT. I DID TWO INSTALLATIONS, ONE TO MY OFT USED HARD DRIVE PARTITION, AND ONE ONTO A 1.2MB FLOPPY. ON THE FLOPPY VERSION, UPON INSTALLATION (WITHOUT LOGGING ON), I FOUND THAT THE FILE 'STAGE.DAT' CONTAINED A LISTING OF EVERY .BAT AND SETUP FILE CONTAINED IN MY 'C:' DRIVE BOOT DIRECTORY. USING THE HARD DRIVE DIRECTORY OF PRODIGY THAT WAS SET UP, I PROCEDED TO LOG ON. I LOGGED ON, CONSENTED TO THE AGREEMENT, AND LOGGED OFF. REMEMBER, THIS WAS A VIRGIN SETUP KIT.

AFTER LOGGING OFF I LOOKED AT 'STAGE.DAT' AND 'CACHE.DAT' FOUND IN THE PRODIGY SUBDIRECTORY. IN THOSE FILES, I FOUND POINTERS TO PERSONAL NOTES THAT WERE BURIED THREE SUB-DIRECTORIES DOWN ON MY DRIVE, AND AT THE END OF 'STAGE.DAT' WAS AN EXACT IMAGE COPY OF MY PC-DESKTOP APPOINTMENTS CALENDER.

CHECK IT OUT FOR YOURSELF.

END OF BBS FILE

I had my lawyer check his STAGE.DAT file and he found none other than CONFIDENTIAL CLIENT INFO in it.

Needless to say he is no longer a Prodigy user.

Mark A. Emanuele V.P. Engineering Overleaf, Inc.
218 Summit Ave Fords, NJ 08863 (908) 738-8486
emanuele@overlf.UUCP

[Moderator's Note: Thanks very much for sending along this fascinating report for the readers of TELECOM Digest. I've always said, and still believe that the proprietors of any online computer service have the right to run it any way they want -- even into the ground! -- and that users are free to stay or leave as they see fit. But it is really disturbing to think that Prodigy has the nerve to ripoff private stuff belonging to users, at least without telling them. But as I think about it, *who* would sign up with that service if they had bothered to read the service contract carefully and had the points in this

article explained in detail? PAT]

- ------- Message 2

Date: 27 Apr 91 19:53:00 GMT
From: 0004133373@mcimail.com (Donald E. Kimberlin)
Subject: Re: Prodigy Questions

In article (Digest v11, iss303), Arnette P. Baker

Search RISKS using swish-e

THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

ACM Committee on Computers and Public Policy, Peter G. Neumann, moderator

Volume 11: Issue 57

Tuesday 30 April 1991

Contents

Reverse engineering and testing of students

<ark@research.att.com>
Tue, 30 Apr 91 09:45:12 EDT

I was talking recently to someone who told me about his experience taking a multiple-choice test. There were a lot of questions, most of which he knew, but some of which were so poorly designed that he could not tell which of several alternatives was the right answer. Of course, he left those blank on his first

pass.

After he had answered the ones he knew for sure, he noticed a pattern beginning to emerge on the answer sheet. The spaces for answers were arranged in two columns, and he saw that the left column had exactly the same pattern of answers as the right column, not counting the gaps, except that it was inverted and reversed. The pattern was too consistent to be a coincidence, so he used that information to fill in the rest of the answers. Sure enough, each answer indicated by the pattern matched one of the answers he had considered possible for that question.

When it came time to grade the test, the grading procedure explained everything. The grader took a sheet of opaque plastic with a bunch of holes in it, placed it over the answer sheet, and marked as wrong all the questions where an answer didn't show through a hole. He then flipped the template over, turned it upside down, and repeated the process for the second column.

--Andrew Koenig, ark@europa.att.com

Re: Another commuter train wreck in London

Dave Roberts <dwr@ssl-macc.co.uk>
Tue, 30 Apr 91 16:44:05 GMT

Following the report in RISKS-11.52 from ClariNet I thought that the Forum readers might like to know that the trains were not both under computer control at the time. The train which was on the receiving end of the bang was under manual control at the time because of "previous failures" according to the UK Daily Telegraph.

The question which occurs to us is "Why did the computer driving the second train not know where the first one was?" No answers available in the UK at the moment because the inquiry is still in progress. The speed of impact was about 5mph and no one was hurt but the whole line was down for 7 hours.

Re: Cable TV "bullet"

David A Ladd <ladd@iwsgw.att.com>
Tue, 30 Apr 91 12:28:41 EDT

>But most of these folks in question are otherwise legitimate cable subscribers
>who have been "sold" a modification to their cable boxes, MOST OFTEN BY A
>CROOKED CABLE COMPANY INSTALLER

Note that the installer need not be crooked, but may be merely incompetent or generous. When I was in high school, before everyone had cable-ready equipment, it was common to have a cable box fail, call for service, and end up with unaccounted-for and unrequested cable services. In fact, of the three households I was aware of with cable, all three eventually had the full set of movie channels without paying for them or in some cases even wanting them. To have this sort of case turn into a ``theft of cable services'' prosecution

seems ridiculous.

Re: Free Speech & Govt. Control of Information

Peter Marshall <peterm@halcyon.UUCP>
Tue, 30 Apr 91 08:42:15 PDT

Larry's response to Jerry Leichter's earlier post on this topic is
well-reasoned and compelling. Yet, while it may generally be the case, as Larry states, that "commercial entities do not have the same free speech rights that individuals do," this observation must, perhaps unfortunately, be qualified in part by the little matter of "corporate First Amendment rights." Amazing what you can do after defining "corporation" as "person" in legal terms. See, for example, THE INCORPORATION OF AMERICA.

Peter Marshall
halcyon!peterm@seattleu.edu
The 23:00 News and Mail Service - +1 206 292 9048 - Seattle, WA USA

Re: Another article: Freedom of Information vs Computers (RISKS-11.55)

<Daniel_C._Swinehart.PARC@xerox.com>
Tue, 30 Apr 1991 08:40:11 PDT

Bob Frankston commented on the relative utility of data when provided in "the original machine readable tape format or on 'more than 1 million sheets of paper.'" Paper is becoming ever more machine-readable these days. It won't be long before these decisions can again be made solely on the basis of the message, not the medium.

Email, Privacy, and `small print'

Herman J. Woltring <UGDIST@HNYKUN53>
Tue, 30 Apr 91 10:24:00 N

Considering yesterday's issue of the RISKS-Forum Digest (volume 11, No. 56) on breach of privacy, email censoring, and improper `small print' in contract clauses, I am reposting part of my note of last February on public access to email facilities. [...]

> Date: Sat, 23 Feb 91 11:10:00 N
> Sender: Biomechanics and Movement Science listserver <BIOMCH-L@HEARN>
> From: Herman J. Woltring" <ELERCAMA@HEITUE5.BITNET>
> Subject: Public access to Internet etc.
>
> Dear Biomch-L readers,
>
> While email communication is usually available for free to account holders
> on EARN/BITNET, Internet, etc., (log-on time, disk usage, paper output
> typically being charged), it may be useful to mention that email access is

> also becoming increasingly available through PC and modem facilities by
> telephone [...; typically, number of transmitted bytes and/or logon time
> being charged -- HJW].
>
> Interestingly, one such service (PRODIGY) has been accused of censoring
> email to and from its subscribers. Whether this allegation is true or
> not, such issues do raise concern about freedom of opinion, free access
> to information, and similar fundamental rights in a networking context,
> especially if (with some justification, perhaps) `network harrassment' is
> used as an argument to counter network `flaming'. As said at a previous
> occasion: "verba volent, scripta manent" ...

The allegations in RISKS-11.56 against Prodigy and GEnie, two commercial email service providers in North America, warrant considering the question whether it is about time that Postal legislation (i.e., postal services are not entitled to refuse, (unnecessarily) delay, read, or censor your mail, or to divert it from its destination without a proper court order) shall also apply to electronic mail, whether through private or public channels.

I do not propose to have this topic as a debate on this list; however, I think that a pointer to the relevant debate is not out of place even on a discussion list like ours, and I shall be happy to consider any comments sent to me privately. I might mention in this respect that the Dutch legislative is currently considering a Computer Crime Bill in which unauthorized access to computers, e.g., by networking, is considered a felony, and that some of the proposals remind more of the U.K.'s Official Secrets Act than of the U.S.A.'s Freedom of Information Act. One heavily debated topic is to what extent computer trespassing will be declared a criminal offence if no appropriate security is provided by system management. If not, private (and public) interests can afford to neglect system security and yet call upon public authorities for free to protect their interests once they observe that their sloppyness has been `used'. This is unusual in Civil Law as any insurance company will be happy to point out, and not very compatible with the classical view that Criminal Law is the Ultimate Resort, `when all else fails'.

Herman J. Woltring, Biomch-L co-moderator & (former) member, Study-committees on s/w & chips protection / Computer crime, Neth. Society for Computers and Law

---

Prodigy commentary

Jeremy Epstein <epstein%trwacs@uunet.UU.NET>
Tue, 30 Apr 91 09:43:47 EDT

I found the comments on Prodigy very enlightening. I'm glad I'm not a subscriber. However, I was very concerned by one comment:

> I invited you to look at your own STAGE.DAT file, if you're a Prodigy
>user, and see if you found anything suspect. Since then I have had numerous
>calls with reports of similar finds, everything from private patient medical
>information to classified government information.

If you have classified government information on your PC, you should

not be using it to call *anywhere* using *any* comm package. That's just good sense (and it may even be the law, I'm not sure).

I'm certainly not defending Prodigy...if what was described is accurate, it certainly sounds like a mass invasion of privacy, theft, and some nice big lawsuits. Has any of this made it into the non-technical press (e.g., Wall Street Journal, NY Times, LA Times).

Jeremy Epstein, Trusted X Research Group, TRW Systems Division, Fairfax VA +1 703/876-8776 epstein@trwacs.fp.trw.com

---

Prodigy and STAGE.DAT strangeness

Tom Neff <tneff@bfmny0.bfm.com>
30 Apr 91 15:18:47 EDT (Tue)

The simplest explanation for private customer data appearing quasirandomly in the Prodigy STAGE.DAT file is that the access program may allocate buffers without clearing them, then write a comparatively little bit of binary data into them and flush to disk. The unused buffer areas still contain whatever was lying around in memory before Prodigy was started, and this "garbage" will end up on disk.

This neither proves malfeasance or innocence on Prodigy's part; but, at worst, carelessness. Clearly their program *could*, if it wished, transmit your computer's entire memory and/or disk contents back home to the Prodigy host. And it could do so *without* storing anything in a file like STAGE.DAT! That's simply a RISK of accepting some black box piece of software in the mail and running it. "Run me," Alice?

Re: Prodigy, etc. (RISKS-11.56)

Robert Hartman <rhartman@thestepchild.esd.sgi.com>
Tue, 30 Apr 91 11:32:55 PDT

WRT the controversies over censoring e-mail and selectively denying service to customers who complain, there already are some laws that should be applicable. It seems to me that there's nothing all that different between an e-mail service and a phone company--except the format of the data being carried. The various phone and long-distance companies are common carriers, and governed by FCC rules. Am I wrong in thinking that a common carrier is not allowed to interfere with the communications they carry, and that they cannot easedrop without a court order? Now, broadcast mail may be open for public scrutiny and rebuttal, but if a carrier offers a "conference call" service, I don't believe that they can restrict anyone from using it, or from saying what they like in the course of such a call. Bulletin board postings seem to me to be analogous to conference calls in the same way that private e-mail messages are akin to private calls.

A sharp lawyer ought to be able to convince a judge or jury in a civil suit (where a preponderance of evidence is all that is necessary to win) that

Prodigy and the others, in offering their e-mail and BBS services, are operating as de-facto carriers for electronic communications. As such, they should be held accountable under the same rules as any other carrier, and liable for any breaches. Esp. when they are run by large corporations with legal staffs. They can't plead ignorance. I can't understand why they'd risk legal exposure in this way, not to mention the negative publicity of a trial!

A risk in obtaining such a ruling would be that all BBS operators--at least those using the phone lines, might have to be licensed. But then, if there are enough of them who write enough letters to legislators, a new class of licenses for "amateur e-mail and BBS carriers" could be mandated. We could even make it an automatically-granted license, so long as there is no charge for the service.

As far as the issue of Prodigy uploading private data goes, this sounds like a clear case of wire fraud to me. Wish I were the lawyer to get that case! Can you spell "class action?" I knew you could. Mr. and Mrs. Middle Class America will be mightily annoyed if this is true.

Four-digit address causes NYC death (Nilges, RISKS-11.55)

W.A.Simon <alain@elevia.UUCP>
Tue, 30 Apr 91 14:56:06 EDT

I have a hard time accepting this. I have designed and programmed applications for the military, for banks, for large corporations, for government administrations, and even for a hospital. I have never encountered a situation where this limitation could have been a problem. If a 9 position field was required, it showed on the screen as a 9 position field, or the analyst (and later the users) would catch it. Testing would also take care of internal field truncations (due to programming errors rather than design weaknesses). Blaming the language for poor discipline is like blaming Henry Ford for road casualties.

From a different perspective, there is no way to garantee that a program will be error free (in respect to field truncation) simply by mandating dynamic field length. There can be other sources for this kind of error. And we should remember that it is not possible to outlaw human failures or plain stupidity.

> How about legislation concerning responsible display and capture of
> COMPLETE information?

And legislation concerning the proper use of toilet seats...

> Or, at the level of civil lawsuits, the fact that a
> defendant's system truncates data should always weigh against the defendant.

It is very probable that, should such error be documented, a civil court judge would find sufficient ground against the defendant.

Alain UUCP: alain@elevia.UUCP

Re: Four-digit address causes NYC death

Brinton Cooper <abc@BRL.MIL>
Mon, 29 Apr 91 23:22:58 EDT

Ed Nilges reports on the death of a man in NYC because the computer system which dispatches emergency personnel was not programmed to handle 5 digit addresses. Ed goes on to make a well-reasoned argument on what might and might not be done about this.

I have another suggestion: I believe that cases such as this argue my theses that there should be less "programming," in the traditional sense of the word. It seems to me that spreadsheet and database tools which permit a limited number of "well-defined" and "obvious" operations by the user may well inhibit many of the errors permitted, even encouraged, by so-called "powerful" languages.

This is just a hunch; I wonder if Risks folks know of data to refute or support this bias?

_Brint

---

static memory allocation causes NYC death

Steve Strassmann <straz@media-lab.media.mit.edu>
Mon, 29 Apr 91 22:52:12 EDT

One RISK of using C and unix extensively, so it would seem, is that it makes it hard for some people to distinguish between "C does this incredibly stupid thing" and "most languages do this incredibly stupid thing."

For example, since C is a de-facto standard, these people make so-called "general-purpose" CPU's, saying "of course it's general-purpose, it's optimized to run C, isn't it?"

---

re: truncation of fields (Risks 11.55)

Martin Minow 29-Apr-1991 2226 <minow@ranger.enet.dec.com>
Mon, 29 Apr 91 19:32:22 PDT

In Risks 11.55, Ed Nilges comments that only a few programming languages allow completely variable-length strings.

The problem isn't quite as bad as Ed suggests. In addition to "REXX and certain Basic interpreters," one might add Ansi Mumps (which is quite suitable for database applications), Pascal (which supports variable length strings up to 255 bytes), PL/I, the VMS command language, and many, if not all, personal computer database packages.

In many cases, however, the problem is not due to the programming language, but to the original database design. Many of these systems grew, one small step at a time, from punch-card based address lists, without the benefit of -- or opportunity for -- a redesign.

Martin Minow

CPSR Washington Seminar, "Social Importance of Privacy," May 3, 1991

Robert Jacobson <cyberoid@milton.u.washington.edu>
Tue, 30 Apr 1991 05:38:07 GMT

* CPSR Seminar Series *
"The Social Importance of Privacy"

Priscella M. Regan, Department of Public Affairs, George Mason University

CPSR Washington Office, Friday, May 3, 1991, noon - 2 pm

Most legal and philosophical writing views privacy as important to the individual, as a safeguard that allows for personal self-development, and a political freedom that protects private or intimate relationships. But this emphasis on the importance of the individual has concealed another aspect of privacy P its social importance. Professor Regan will explore the philosophical and legal basis for the social or public importance of privacy, and will examine the policy implications of viewing privacy from a social perspective.

CPSR Washington Office, 666 Pennsylvania Ave., SE, Suite 303, Washington, DC, 202/544-9240 (one block from the Eastern Market metro)

In cooperation with The United States Privacy Council

[if you would like to be notified of future CPSR Seminars, please send a note with e-mail address to mrotenberg@csli.stanford.edu]

Search RISKS using swish-e

THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

ACM Committee on Computers and Public Policy, Peter G. Neumann, moderator

Volume 11: Issue 58

Tuesday 30 April 1991

Contents

Hacking, Civil, and Criminal Law

"Herman J. Woltring" <UGDIST@nici.kun.nl>
Fri, 26 Apr 91 09:54 MET

My recent posting `Hacking a la Neerlandaise' <RISKS 11(52)> gave rise to a couple of private comments, and an invitation for a telephone interview with Unix Today. One comment thought that I was too subtle, the other accused me of network abuse:

>Oh, gimme one giant break. No one cares whether or not you log in to Libra-
>ries on the Internet so you can look up a book. That's why they are on the
>Internet, and that's part of the reason the Internet exists. The articles
>that have been flying around lately seem to indicate that {you, your com-
>patriots, someone in The Netherlands} has been doing a little bit more than
>that, and more to the point, bragging about it.

>Stop trying to bull**** the rest of the net. This isn't a RISK anymore, it's
>an annoyance.

> [names omitted] @think.com and ...harvard!think!...

Maybe, PGN had different thoughts, because he released my tongue-in-cheek item to the readership. What I wanted to do is to show how the way things are described in newspapers, in debates like the current one, and in philibustering can bias arguments into a certain direction -- of course, this is standard practise in (televised ?) litigation: you're accused of all sorts of nasty things, and the court (or the jury ...) has to make up its mind what facts are behind the rhetoric.

For one thing, I don't see that my compatriots have been `bragging' -- they merely demonstrated possibilities under current law, in a time that the Dutch Parliament is trying to make up its mind how to balance between Freedom of (access to) Information and Computer/Network Trespassing. Information and its use have always been `free' unless special protections are provided for. Patents law (information is public, with free review and research, but its routine use is protected), trade secrecy law (independent discovery is free, improperly obtaining trade secrets is not -- e.g., through bribes or blackmail), copyright law (pure information is free, its expression is not, but the underlying information may be recovered under Fair Use / Fair Dealing in Anglo-American, Common Law) are examples of this freedom, protected under the USA's First Amendment and under various International Treaties. Society is dynamic, and new possibilities call for (new?) freedoms and new protective regimens.

One hot issue in the current, parliamentory proceedings is the extent to which `computer trespassing' has appropriate protection as a mandatory prerequisite. If you open your vaults, dismiss the guards, turn off the alarm, and if your name is Dagobert Duck, you are equally liable for solliciting criminal behaviour as is #789-123 for committing a felony while he purloins your bullion. Crying wolf without even guarding the sheep will not raise much sympathy... In my book, simplistic passwords, retaining known system passwords or not plugging known, remote-access loopholes are tantamount to the same.

The point is important because legislators tend to write law books in a generic fashion, leaving it to the courts to determine which paragraph applies in what case (that's what appeals are about so often: in The Netherlands, lower courts assess the facts, and the higher and supreme courts then may have to determine whether the Law has been applied properly; beyond that, you may even go to the European Court). Thus, criminalising `computer trespassing' might, in principle, apply not only to the Pentagon or Watergate, but also to your cooking machine or Swiss/Japanese watch. Determining boarderlines in Noman's land between what's in the private and common interests is what we should be concerned with.

We are a property-biased society, where civil law gives us our own responsibilities to protect our goods (and note that Information is not a material good but an immateriality which cannot be `stolen' but only kept secret, shared, or destroyed). With Information more and more becoming a valuable `thing', the `owners' wish to increase their grip on what they wish to hold. Because they are often too lazy to accept their civil responsibilities

and to sue privately (it's expensive, too!), they try and fall back on criminal law where public authorities can be called upon for free to protect their private interests. However, Criminal Law is (or should be), the Ultimate Resort only, when all else fails.

I have been told that Shakespeare once described a technique for artificially creating the sound of thunder in the manuscript for a future play. When attending the premiere of a colleague's play who had been privately reviewing his manuscript for him, he heard to his exasperation a very familiar sound. Jumping up, he roared "YOU STOLE MY THUNDER!", much louder than his `stolen' contraption.

There are many alternatives to criminalising computer trespassing: breach of privacy is one of them, but this does not apply if you make public access to your secrets too easy.

Herman J. Woltring, Eindhoven, The Netherlands, (Former) member, study comms on s/w protection and computer crime Netherlands Society for Computers and Law
Tel. (private) +31.40.480869, +31.40.413744 ugdist@hnykun53.bitnet

Utrecht crackers and the law

Fernando Pereira <pereira@klee.research.att.com>
Thu, 25 Apr 91 22:30:34 EDT

In my two postings on the Utrecht crakers, I took pains to mention only ethics, rather than the law (which I do not feel qualified to discuss), with respect to my suggestion that sites whose *officials* condone Internet-wrecking activities do not belong in the Internet. However, several RISKS readers, in particular Mike Godwin (RISKS 11.54) read my postings as coming on the side of heavy-handed legal approaches to the problem of cracking. I worry that discussion of these matters on RISKS degenerates often into fights between ``libertarians'' and ``string-them-uppers''. I was looking instead at the Internet as a voluntary association. My point would have applied to any member of any club that promoted activities against the club's norms. Most of the restraints we observe in social intercourse are not in the law, but life without them would be much, much harder. Those informal restraints and sanctions form the first line of defence against destructive behavior, when bringing in the law serves only to radicalize positions and create victims/heroes.

Fernando Pereira, AT&T Bell Laboratories, Murray Hill, NJ 07974

Comments on computer trespassing (Dutch hackers)

"LARRY SEILER, DTN225-4077, HL2-1/J12 25-Apr-1991 1558" <seiler@rgb.enet.dec.com>
Thu, 25 Apr 91 14:05:13 PDT

People are making several analogies between network breakins and other sorts of situations that fairly cry out for comment.

1) Common law access. In my part of the US, if you openly and flagrantly use

someone's property for 20 years, you have the right to keep doing it. Phil Agre suggests that this applies to those who don't block security holes. Nonsense. If a specific user is on a system, and the administrators know about it and continue to allow that user to be on the system, this reasoning might apply. But crackers in general do not work openly. A security hole is like a hole in a fence. The law does not require me to patch all holes to be protected, or even to put up a fence. It requires me to tell people I see using my property that I don't want them to. Attempting to prosecute a cracker surely satisfies that criteria...

2) Tort law. If you come onto my property and get injured, you can sue me if I was maintaing an attractive nuisance. If you come onto my property and injure me or someone else, you cannot sue me, so it is silly to say that sites should be punished simply for having security holes. HOWEVER, if you use my property to injure someone else, that other person could sue you, and possibly me as well. So it is reasonable to cut off from the network sites that are commonly used to break into other sites -- especially if those in charge of that site express reckless disregard for the problem. But none of that excuses the cracker who actually causes the damage.

3) Socializing the youth. Mike Godwin correctly points out that we have a responsibility to socialize the younger generation, and putting them in jail for doing what comes naturally (e.g. cracking?) is a bad way. I respectfully point out that saying that it's ok by leaving them unpunished is also a bad way. Other sorts of penalties should be applied, such as taking away their computer access until they learn to be responsible. Also, while sites should be more secure, and people should build fences around atrtractive nusiances, it isn't a solution to the problem of trespassing to require that *all* property be surrounded by sturdy fences.

Larry

Re: Dutch nation portrayed as a bunch of network bashers

David Collier-Brown <davecb@nexus.yorku.ca>
Fri, 26 Apr 91 08:22:15 EDT

rmoonen@hvlpa.att.com (Ralph 'Hairy' Moonen) writes:
... Not just the issue of one
| single university like Utrecht, but of ALL sites on the internet. Because you
| do realise that a smart cracker could get away with this just as easily in the
| States as in Holland? So don't lay any guilt-trip on the Dutch will you?

Alas, it happens all the time on this side of the atlantic: earlier this year some

---

Re: Dutch crackers and irresponsible officials

<dik@cwi.nl>
Tue, 30 Apr 91 09:06:22 +0200

>From Volume 11, Issue 53:
> Clearly, as with burglary of

> an unlocked home or theft of a car with keys hanging from the ignition,
> carelessness by the owner does not set aside the guilt of the perpetrator.
> Conversely, carelessness by the owner does not relieve her/him of
> responsibility for the loss. In the "Dutch cracker" incident, perhaps BOTH the
> cracker's host and the host with known, repairable security holes should be
> barred from the Internet.
>

Some clarification. Dutch law specifically distinguishes 'insluiping' (sneaking into) and 'inbraak' (breaking into). The second being a worse crime than the first (but both are crimes). Separate from this again is 'stealing' and 'tampering'. Also somebody who leaves his car/home unlocked is guilty of 'uitlokking' (inviting? I do not know the correct English term), which serves as a means to diminish the guilt of the guy 'sneaking in'.

So in terms of Dutch law this appears to be a case where some hacker 'sneaked into' a system without actually 'stealing' or 'tampering'. The system was guilty of 'inviting'. But as such it is only a minor offense.

dik t. winter, cwi, amsterdam, nederland

Utrecht (Re: Cooper, RISKS-11.53)

Richard A. O'Keefe <ok@goanna.cs.rmit.OZ.AU>
29 Apr 91 02:11:10 GMT

In article <CMM.0.90.1.672538040.risks@chiron.csl.sri.com>, several people commented on the Utrecht break-ins. Brinton Cooper, for example, wrote

> The time has come to put this debate behind us. Clearly, as with
> burglary of an unlocked home or theft of a car with keys hanging
> from the ignition, carelessness by the owner does not set aside the
> guilt of the perpetrator.

The underlying attitude here is that some blame _does_ attach to the sites that were broken into, for being the equivalent of an "unlocked home". I'm responding because this attitude rather worries me, and I think the analogy is invalid. Let me cite three homely examples.

1) When I was flatting in Edinburgh, I locked myself out once. The locksmith took *seconds* to get in.
2) When I was working in Palo Alto, I locked my keys in my car once, with the engine running. The AA man took *seconds* to get in.
3) The flat I'm in now has (several) locks on both doors, and special fasteners on the few windows that open. But a man with a crowbar (or a good strong knife) would take seconds to break in, and someone who was prepared to smash a window would have as little trouble.

I put it to the readers of comp.risks that running a SparcStation or a UNIX/386 system "straight out of the box" but with passwords on all accounts is the moral equivalent of an ordinary home with Yale locks and latched windows, _not_ the equivalent of an "unlocked" home. Ordinary locks hardly even slow down a determined and knowledgable intruder. They are, in effect, little more than "keep out" signs which block the

idly curious.

I put it to the net that "well known" security holes in operating systems as shipped to customers are the moral equivalent of a lock manufacturer shipping locks known to be defective, _not_ the moral equivalent of a home-owner failing to install any locks. I have been using UNIX since the days of V6+. But I have no idea what the "well known" security holes are (well, setuid scripts, uucp setup, a few things). What is J. Random Luser to do with his UNIX/386 box that doesn't even come with a C compiler? Why should _he_ be held negligent if there are "well known" holes in his O/S, and why should such people be kept off the net, either by law or by fear? (I should point out that I have an actual charity in mind, that would benefit quite a bit from a TCP link, but they aren't programmers, and I certainly haven't the skill to make their system secure.)

RE: rude behavior

Andrew Marchant-Shapiro <marchana@UNVAX.UNION.EDU>
Thu, 25 Apr 91 08:52 EDT

Bill Murray's suggestions regarding disconnecting rogues from the net make good sense; they are similar in form to a Japanese management technique called ``reverse feedback'' -- in an auto plant, each station has the responsibility to determine whether or not what it receives from the previous station is acceptable. This means that if you send me (for example) a damaged engine block, I have a choice. I can either accept that damaged part and do my bit of work on it, or I can send it back to you and insist that YOU fix it. If I choose to do my work and send it on, even though I know it is damaged (or because I fail to notice) and the next station DOES notice, they can send it back to ME (and I have to fix it; since I didn't back it up to you, it is now MY responsibility).

This approach make quality control a distributed process with real responsibility, instead of a centralized process that can't attribute responsibility. In general, it results in higher-quality products.

The same can be said for controlling net access. If I find a rogue coming in through UCB, then I should cut off UCB until they do something about it. UCB should then take steps to eliminate the problem from their system and back it up, and so forth.

This sort of distributed responsibility might at first cause problems (a lot of people might lose the internet all at once!) but would help create a sense of responsibility relatively quickly.

I don't know if any of this is useful to you, but I did want to say that I endorse your approach to maintaining the net (at least in theory!).

Andrew Marchant-Shapiro / Departments of Political Science & Sociology
marchana@union.bitnet / marchana@gar.union.edu / marchana @unvax@union

---

Re: RISKS of being rude...

Brad L. Knowles <blknowle@frodo.jdssc.dca.mil>
Fri, 26 Apr 91 13:14:26 EDT

I have read the recent comments on Bill Murray's article in RISKS Digest 11.53, and find I must side with Mr. Murray. Perhaps he is being more radical than I would be, but he has the right idea anyway. If we find someone who is committing a crime (trespass of either the physical or electronic sort), and we cannot prosecute them (for whatever reason), then must ostracize them.

As an example, let us suppose that the front doors to the Pentagon are not locked, and someone who has Diplomatic Immunity (DI), say Saddam Hussein's little brother, slips in. He is caught on the premises a number of times, and each time he is escorted out of the building (sometimes rather forcefully). Mind you, the halls of the Pentagon are supposed to be Unclassified, as we have public tours that go through the Pentagon every thirty minutes from 9:00 in the morning to 4:30 in the afternoon (when a crisis like Desert Shield/Storm is not in progress). Nevertheless, Mr. Hussein continues to try to break into the Pentagon illegally. What can we do? Our only alternative is to send him packing, and not grant him a Visa (no, not a CitiBank Visa) to return to the US. If everyone Saddam Hussein sends to the US under the cover of DI tries to break into the Pentagon (or where ever), then our only course of action is to send ALL of his diplomatic personnel back to Baghdad.

Likewise, if someone from the University of Utrecht keeps breaking into computers at Lawrence Livermore Labs, or NASA, or where ever, and we can't get the local police to prosecute them (assuming that we have collected enough information to identify the perpetrators), then our only course of action is cut the Univerisity of Utrecht off from the Internet in the US. If most every University in the Netherlands has people trying this, then we must cut them all off. Since the Defense Communications Agency (DCA, soon to be changing our name to Defense Information Systems Agency (DISA)) has the right, nay the RESPONSIBILITY to keep up (and presumably to police) the Internet, then I think I can safely say that this might actually get implemented if the folks over at the University of Utrecht keep it up. Also, the Internet Activities Board (IAB) might get a little upset with these folks if they don't stop their mischief.

We must *not* punish the victims for the crimes of others! As was stated by another author, some folks simply don't have a choice -- they *must* stay with an old version of their OS becuase some mission-critical piece of software runs *only* with that version of the OS. We must not say to these people "Sorry, you have an old version of the deadbolt lock, and therefore any crime of trespass or resulting from trespass will not be prosecuted." Just think if this were you, how would *you* react to that statement? You would have two choices -- let the crackers continue to victimise you, or completely disconnect yourself from the rest of the world. Could you live with either result?

-Brad

Re: Response to Rude Behavior

Tim Wood <tim@sybase.com>
Mon, 29 Apr 91 11:22:33 PDT

In Bill Murray's call for ostracism (sanctions?) against the University of Utrecht, he may have found the limits of ostracism as an effective tool for reform of the socially destructive. Because of the high degree of interconnectedness of producers and consumers in these times, to implement fully a policy of ostracism against this institution is infeasible, politically if not practically.

Recent history shows us the tenuousness of the ostracism argument. It took years of economic sanctions against South Africa before the leadership there changed sufficiently to allow the beginning of the dismantling of apartheid. It took far more time before there was the international will to begin imposing them. And those sanctions were accompanied by continual, vocal and sharp denouncements of that social policy. If there was such great difficulty in coming to terms with the need to oppose such a manifestly cruel system as apartheid, how long will it take to reach a consensus, from the currently divided dialogue between reasonable people, that all computer cracking is reprehensible and evil?

Development of the Persian Gulf war is just the most recent example of the lack of faith in sanctions. The UN, steered by the US, decided that the certainty of mass destruction in Iraq was preferable to the uncertainty of months (years?) of sanctions as the way to--rightly--dislodge Saddam Hussein's army from Kuwait. The argument against sanctions went to the effect that "the world can't afford to wait for them to start hurting, nor afford the risk of their not being uniformly observed." If it is so easy to undermine a sanction by selling a few tons of military equipment, how much easier is it to do so by editing a few lines in a communications configuration file?

The call to impose sanctions on China after Tienamen Square didn't even approach international consensus, let alone be implemented.

The ethics of computer use are not well-enough understood or agreed-upon for there to be a political consensus against the University, IMHO. And as long as there is even one site that refuses to disconnect, that site can perform the equivalent of money-laundering on whatever comes out of Utrecht, disguising their mail and hiding the origins of the connections they make. Once the political will is there, the practical part is easy. But without the will, which is in short supply these days anyway, the technology can do nothing.

Tim Wood, Sybase, Inc. / 6475 Christie Ave. / Emeryville, CA / 94608
{pacbell,pyramid,sun,{uunet,ucbvax}!mtxinu}!sybase!tim 415-596-3500

One-time passwords (RISKS-11.53)

Steve VanDevender <stevev@greylady.uoregon.edu>
Sun, 28 Apr 91 15:36:04 PDT

Bill Murray's article on one-time passwords generated by what he calls "tokens" describes an interesting approach to improving system security, although he

recognizes some of the ways in which such a system could be compromised, such as stealing a user's password generator.

There are some ways of defeating a one-time password system that he did not describe, though. Although a password generator is individually seeded with a unique value that makes its generated passwords unique, both the host computer and the password generator must algorithmically generate password values for comparison, or the host computer can extract the unique identifying information from any random password generator password. Therefore, one-time passwords just add a layer of security by obscurity to the authentication process, since determining the password generation algorithm allows one to generate correct passwords without a password generator.

Security always depends ultimately on secret information. A one-time password system may reduce the possibility of security breaches by requiring password crackers to hit a moving target, but I suspect that any widespread implementation of one-time password systems would cause password crackers to change from finding ways to obtain passwords to finding one-time password generation methods.

Steve VanDevender stevev@greylady.uoregon.edu

One-Time Passwords

Barry Schrager <71370.2466@compuserve.com>
26 Apr 91 11:04:41 EDT

Regarding: Risks 11.53 - WHMurray - One time Passwords

Mr Murray is totally correct. All enforcable security mechanisms are based on the user knowing something (like a password) or having something (like a badge for a reader) or having some personal attibute (handwriting, retina analysis, etc.). More modern security mechanisms identify the user first and then via some mechanism determine what he can or cannot access.

But the basis for all this is knowledge of the identification of the user. The more confident you can be of a user's identitiy, the more secure your system will be.

The problem with signature, fingerprint, or retina analysis is that the hardware is relatively expensive and on a diverse and unsecured network, one can easily duplicate the information transferred via a simple program in one's personal computer.

The token Mr Murray refers to -- really a small specialized calculator -- is designed to take one key as input and produce another key as output. Therefore, the security (or lack of it) of the network itself will not jeopardize the security of the computer system attached to the network. Someone can listen in on the network and will not be able to project what the next password produced by the token will be.

I do happen to disagree with Mr Murray in that it is my opinion that the tokenized challange and response should be in addition to a user changable

password which he knows.

Thus, we have a secure system in that user identification is based on something the user knows (his password) and something he has (the token) and this all works on a network that does not have to be absolutely secure.

And we have all this at a fairly small cost -- much less than the costs of the more sophisticated hardware devices for fingerprint, signature, etc.

Search RISKS using swish-e

THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

ACM Committee on Computers and Public Policy, Peter G. Neumann, moderator

Volume 11: Issue 59

Wednesday 1 May 1991

Contents

"Losing" a Warehouse

Jane Beckman <jane@stratus.swdc.stratus.com>
Wed, 1 May 91 16:14:52 PDT

I've been meaning to post this for a while, as it is a perfect illustration of the hazards of a system that gets too dependant on computer programs.

In 1989, Mongomery Ward had a sale of "discontinued, one-of-a-kind, and out-of-date merchandise." A fellow I was dating, who was a Wards employee, told me the story of where it had come from. Around 1985, Wards had reprogrammed their master inventory program. Somehow, the entry for the major distribution warehouse in Redding, California, was left out. One day, the trucks simply stopped coming. Nothing was brought into the warehouse, and nothing left. Paychecks for the employees, however, which were on a different system, kept coming. While this was baffling to the employees, they figured it was better not to make waves. (Rumor has it that they were afraid the warehouse had

been phased out, and they had "forgotten" to lay them off, and figured it was better to stay employed.) They went to work every day, and moved boxes around the warehouse, and submitted timecards, for three years, until someone doing an audit finally wondered why major amounts of merchandise had simply disappeared. Tracing things back, the missing warehouse was finally re-found. They were then stuck with an entire warehouse full of white elephants--- merchandise that was three years out of date. Thus, Wards stores throughout California ended up with major amounts of discontinued merchandise to sell at deep discounts. Wards, being majorly embarrassed, tried to downplay how the merchandise was "found." Or, more specifically, why it had become lost in the first place.

The store employees got a big chuckle over the warehouse employees being afraid to mention this oversight to the higher-ups, for fear of becoming unemployed. Many references to "like jobs with the government."

Of course, the question is: is this the only case like this? Are there more places where an operator entry glitch has caused some function to simply disappear? Things like this happen when live people are accidentally classed as "dead," etc. What happens if someone types the wrong thing, and the local branch of your bank, or MacDonalds, or whatever, simply ceases to exist, to the central computer?

Jane Beckman [jane@swdc.stratus.com]

Soon, ATMs May Take Your Photograph, Too

Michael W. Miller <mikeym@well.UUCP>
Wed, 1 May 91 08:06:51 pdt

Soon, ATMs May Take Your Photograph, Too, By Paul B. Carroll,
Wall Street Journal, 25 April 1991, Page B1 (Technology)

Smile when you use that automated teller machine. Miniature cameras may soon become widespread in ATMs and elsewhere.

At Edinburgh University in Scotland, researchers have produced a single computer chip that incorporates all the circuitry needed for a video camera. Even with a lens that fits right on top of the chip, it's still just the size of a thumbnail. When they become available in a year or so, such cameras may carry as little as a $40 price tag.

NCR thinks these tiny cameras could find their way into lots of ATMs in the next few years. The computer maker already sells ATMs that include cameras, allowing banks to doublecheck on people who contend their account was debited even though they didn't use an ATM that day. But those cameras are expensive, especially because the big box with the electronics has to be so far back in the ATM that it requires a long, elaborate lens. The lens also gives away to potential cheats the fact that the camera is there, whereas the new tiny cameras will just need a pinhole to peep through.

"We see this as a breakthrough," says Greg Scott, an engineer with NCR in Dunfermline, Scotland.

The Scottish Development Agency, which supplied some of the initial research funds, says the tiny cameras may also find their way into baby monitors,

picture telephones, bar-code readers and robotic vision systems.

Old O/S and Network Security

"351M::ESTELL" <estell%351m.decnet@scfb.nwc.navy.mil>
1 May 91 07:59:00 PDT

For years now, there has been a reasonable solution to the problem of "an old O/S" and network security: Install a newer, much improved O/S (WRT network security) _between_ the open network, and the "closed" community that uses the old O/S to process valuable information.

If you REALLY want security, install a Honeywell SCOMP between the internet, and your local host, LAN, or whatever; at less cost, and more risk, install any C2 or better O/S host at that connection site. Then the would-be hacker has to penetrate something a bit better than the "standard out of the box" 5-pin lock that yields in *seconds*.

Such a connection can be layered; e.g., one can put a "C2" host (such as a DEC VAX running VMS 5.x, with security options turned on) on the internet, as a MAIL host; then a "B2" (or better) system between that MAIL machine on the internet, and another MAIL machine on the local network; and even other "B2" (or better) nodes within the local net protecting the most "valuable" hosts on it. This is the electric analog to the fence around the base, the lock on the building door, the locked office, and the safe inside the office.

The continuing reluctance of "management" (both "general" and "system") to adopt this (or other, better) solutions is perhaps one key to the continuing lack of security. Are we still "hung up" on the cost of hardware, versus cost of personnel time to chase intruders? Are we too proud to admit that we need to improve? Is the old aphorism right: "Never attribute to malice anything that can be explained by stupidity."

Bob

> [The Honeywell SCOMP -- still the only A1 evaluated system -- is now the Bull SCOMP.

Genie: (was Re: Email, Privacy, and `small print')

Chuq Von Rospach <chuq@Apple.COM>
1 May 91 06:17:40 GMT

By the way, to clear things up before the flaming starts, GEnie has recently clarified its user policies for acceptable behavior (in the wake of the Linda Kaplan affair, of which I'm trying to avoid speaking about). Their policy on email is quite clear -- they say that junk mail, chain letters, offensive or libelous mail, etc etc are unacceptable -- but they also make it perfectly clear that GEnie does not under any circumstances monitor or read email on their systems. They will investigate and deal with inappropriate mail ONLY after complaints from the recipients.

Please don't start lumping GEnie and Prodigy together. They are like Night and Orange Juice.

chuq (not attached to GEnie in any official way, although they do subsidize one of my GEnie accounts. Aren't disclaimers silly?)

Chuq Von Rospach >=< chuq@apple.com >=< GEnie:CHUQ or MAC.BIGOT >=< ALink:CHUQ
SFWA Nebula Awards Reports Editor =+= Editor, OtherRealms
Book Reviewer, Amazing Stories ---@--- #include <standard/disclaimer.h>
Recommended: ORION IN THE DYING TIME Ben Bova (Tor, Aug, ***-); SACRED VISIONS Greeley&Cassutt (Tor, Aug, ****+); MEN AT WORK George Will (****); XENOCIDE Orson Scott Card (August, ****)

Prodigy Problem in Major Press

Bill J Biesty <wjb@edsr.UUCP>
Wed, 1 May 91 16:21:52 CDT

This is the summary of the WSJ article I get mailed to me on a daily basis. Interesting that Prodigy does NOT deny that it sends customer data to their host; ONLY that they DO NOT USE it. If they "haven't any interest in getting there" as the summary says, why are they spending their own money to get customer data in the first place? (Prodigy charges a lump fee for unlimited connect time, so they are absorbing the cost of sending this extra data.)
Bill Biesty

SUBJECT: WSJ DAILY EXTRACT 5/1/91 POSTED 05/01/91 16:09
FROM: EDS BULLETINS
WALL STREET JOURNAL DAILY EXTRACT 05/01/91

The following "extracts" are taken from Wall Street Journal (WSJ) articles and are posted on the eMail Bulletin Board daily. Technical Resource Acquisition (TRA), assumes no responsibility for the accuracy of the extracts, which are simply provided as a service to those who do not have the time to read the WSJ. The extracts do not represent the opinion of EDS nor TRA, and are posted for informational purposes only.

[...other summaries deleted...]

o Subscribers to the popular Prodigy computer service are discovering an unsettling quirk about the system: It offers Prodigy's headquarters a peek into users' own private computer files. The quirk sends copies of random snippets of a PC's contents into some special files in the software Prodigy subscribers use to access the system. Those files are also accessible to Prodigy's central computers, which connect to users' PCs via phone lines. Prodigy, a joint venture of IBM and Sears, Roebuck & Co., offers nearly one million users electronic banking, games, mail and other services. The service's officials say they're aware of the software fluke. They also confirm that it could conceivably allow Prodigy employees to view those stray snippets of private files that creep into the Prodigy software. But they insist that Prodigy has never looked at those snippets and hasn't any intention of ever doing so. "We

couldn't get to that information without a lot of work, and we haven't any interest in getting there," says Brian Ek, a Prodigy spokesman. Nevertheless, news of the odd security breach has been stirring alarm among Prodigy users. Many have been nervously checking their Prodigy software to see what snippets have crept into it, finding such sensitive data as lawyer-client notes, private phone-lists, and accountants' tax files. Even though Prodigy users' privacy doesn't appear to have been invaded, the software problem points up the security risks that can arise as the nation races to build vast networks linking PCs via telephone lines.

Re: Prodigy, etc. (RISKS-11.56)

Chuq Von Rospach, only here for the beer <chuq@Apple.COM>
1 May 91 06:32:03 GMT

>It seems to me that there's nothing all that different between an e-mail
>service and a phone company--except the format of the data being carried.

There are actually a LOT of differences. Phone companies are regulated, quasi-governmental agencies with guaranteed monopolies where the regulating agency has build a set of regulations to make sure that the phone company doesn't take advantage of their monopoly.

E-mail services are private businesses that are doing businesses with individuals in an unregulated industry.

Now, you can argue that e-mail companies *OUGHT* to be regulated like phone companies -- but they aren't, and to do so would require legislation (and probably court fights and other associated legal stuff).

>but if a carrier offers a "conference call" service, I don't believe
>that they can restrict anyone from using it, or from saying what they like in
>the course of such a call.

Sure they can. They are a company doing business. When you sign up with them, you make an agreement to do business with them within the guidelines that are set down in the agreement. If you abrograte that agreement (be it "not pay the bill" or "put the company in a situation of legal liability") then that company has the right to terminate the agreement.

There is no guarantee of service. Even with the phone company, there is no guarantee of service -- you don't believe me, go a few months without paying your bill and argue that you have a right to continue using your phone.

>A sharp lawyer ought to be able to convince a judge or jury in a civil suit
>(where a preponderance of evidence is all that is necessary to win) that
>Prodigy and the others, in offering their e-mail and BBS services, are
>operating as de-facto carriers for electronic communications.

Sorry, I don't buy it. First, when you sign up for GEnie (and others), you sign an agreement which stipulates the services rendered and the responsibilities to both parties. What you're trying to do here is convince

a judge/jury that the legal contract you signed is, in fact, not valid. Not likely to happen.

Second, "de-facto carrier" is, to me, a non-statement. An entity is either a common carrier legally or it is not. If it is not a common carrier, it can be held liable for what YOU do on ITS computers. There's no defacto attached -- unless it is given real, legally binding (through legislation or legal precedent) common carrier status, a company HAS to have the right to refuse you service and monitor your behavior for appropriateness, becaus otherwise you are in a position of putting them in legal liability without them having any recourse to protect themselves.

Sounds good -- but your thoughts don't seem to be well thought out as to how things are in real life.

Chuq

PRODIGY

A. Padgett Peterson <padgett%tccslr.dnet@uvs1.orl.mmc.com>
Wed, 1 May 91 12:03:26 -0400

In the current issue of the Prodigy Star (newsletter sent out from Prodigy to users) there is a two page article from Harold Goldes (one of the Prodigy EXPerts) on computer viruses. While it is quite informative, the issue of online updating of executables/data is skated though one point seems clear - they do not guarentee that you will not get a virus from Prodigy, and if you do, it is your problem.

Prodigy

"Mary Culnan" <mculnan@guvax.georgetown.edu>
1 May 91 11:40:00 EDT

Prodigy recently ran an ad in DM News, a weekly direct marketing trade newspaper with the header "..But you can't miss with Prodigy Direct Mail." The ad is encouraging companies to use Prodigy for direct marketing and says in part,

> "Now, for the first time, marketers can deliver electronic mail to targeted segments of the PRODIGY service member file..."

Prodigy service members are highly-responsive, highly-qualified prospects. They are young, well-educated, well-paid and well-traveled. And they're active users of the PRODIGY service, signing on 10 times a month on average, for about 20 minutes each time.

Members' demographic data is merged with their PRODIGY service usage information to offer yo more than a dozen selections based on their interests and activities, such as personal finance, sports, computers, travel, etc....

PRODIGY Direct Mail offers you the most sophisticated application available of

high-tech, high-touch direct-to-consumer marketing."

Clearly they are looking over the shoulders of every user--a point that was also made in the recent NOVA show, "We Know Where You Live."

Mary Culnan

A Prodigy experiment

Bill Seurer <seurer@rchland.vnet.ibm.com>
Wed, 1 May 1991 11:01:59 -0500 (CDT)

Because of all the rumors flying around of Prodigy uploading data off of user's harddisks I decided to test if this was indeed happening.

All of these rumors are based on the fact that the staging file (STAGE.DAT) Prodigy uses to buffer its screens on the harddisk sometimes is found to contain bits and pieces of user files and directories. Some users claim this proves Prodigy is uploading the data while others just say it is an artifact of the way that DOS allocates files and because Prodigy does not initialize the file when it is created.

I devised and carried out the following experiment in order to test if this was happening.

The results are:
Prodigy does not appear to be uploading any data.
The STAGE.DAT file contains bits and pieces of ERASED files.

The experiment went as follows:

1) Re-installed Prodigy. I erased all of the files Prodigy had installed on my system.
2) Modified CONFIG.SYS and AUTOEXEC.BAT to remove all TSRs and have 0 DOS buffers. I removed the disk caching software I usually use. This was to prevent any leftovers in buffers or caches from showing up in STAGE.DAT and so that I could monitor what the harddisk was doing more easily.
3) Defragmented the harddisk so that all files were in contiguous blocks.
4) I ran CLEANDSK and CLEANEND to write zeroes over all the unused parts of the disk and over the unused ends of DOS files.
5) Powered the PC off and then on. All memory was therefore flushed and the minimal system with no buffers was in use.
6) I created several large (500k) files each containing a different pattern of characters. After all were created, I erased them. This was to test whether STAGE.DAT is picking up bits of erased files.
7) I installed Prodigy using a large buffer. This created a STAGE.DAT file that was just under 1 meg in size.
8) I browsed STAGE.DAT to see what was inside. The first 250k or so had interesting stuff and the other 750k was 0's. The interesting stuff was mostly buffered Prodigy windows (I could tell by the text that was mixed in) along with scattered pieces of one of the files I had created and deleted in step 7. This file made up about 100k of STAGE.DAT. and given where the data was I'd guess that the first 200k or so of STAGE.DAT had

been overlaid on the disk where this file used to be. The *ONLY* non-Prodigy thing that I saw was a copy of my environment variables (COMPSEC, PATH, and PROMPT). I noted that the windows that were buffered were the "old" windows (Prodigy has changed many of its windows since I got my installation kit).

9) Made a copy of STAGE.DAT so that I could compare it with an updated copy after I signed on.

10) I again powered the PC off and on to clear all the memory.

11) I signed on Prodigy. While on I read some mail, sent some mail, read a few BBS appends, and looked at a couple of ads. Then I signed off. I noticed some things when I signed on. First of all, it took a looooong time. I surmised that all those "old" windows I had seen in STAGE.DAT were being updated. I carefully watched my modem lights and harddisk light (remember, I had no buffering). About 95% of the time (at least!) the modem was receiving data. At the end of each long receive (some were 4 or 5 seconds long) the hard disk would be used briefly and the modem transmit light would flicker on. Then there would be another long receive and etc. At no time was my modem transmitting for more than a fraction of a second.

12) Using a hex/ASCII file comparison tool I compared the contents of the STAGE.DAT that I had saved with the updated one after I logged off Prodigy. Many of the menus I had noticed the first time I looked were changed to the newer formats. Also, the sign off menus and some of the messaging menus had either overwritten some (but not all) of the data from the file I had created and deleted in step 7 or been added at the end of the 250k of initially used area in STAGE.DAT. STAGE.DAT now had about 280k of used area less perhaps 80-90k of data from the file in step 7.

This experiment shows to me that all the stuff about Prodigy uploading files is rumors started by people ignorant of how DOS works. Some people said that they reinstalled Prodigy to see if that changed STAGE.DAT but they didn't defragment/zero out their disks first so their data is highly suspect. If they had watched their modem lights they would realize that almost no time is spent sending data to Prodigy when signing on but is almost all sent receiving it.

If I were to run this again I would change step 7 to completely fill up the unused portion of my harddisk with the dummy files and then erase them all. My guess is that the 750k of space at the end of STAGE.DAT would then contain bits from those files. Later this week I think I'll try this and see.

My set-up in case you're interested is:

IBM PC-1 (the original) with an Intel Inboard/386, 40 meg harddisk, 2400 baud modem, DOS 3.2, and Prodigy 3.1 (which is the latest I believe).

If you have any questions about the experiment I'm more than happy to answer them. Also, if you have suggestions for more things to try next time let me know.

- Bill Seurer IBM: seurer+@rchland Prodigy: CNSX71A
Rochester, MN Internet: seurer+@rchland.vnet.ibm.com

Search RISKS using swish-e

Report problems with the web pages to the maintainer

Search RISKS using swish-e

THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

ACM Committee on Computers and Public Policy, Peter G. Neumann, moderator

Volume 11: Issue 60

Thursday 2 May 1991

Contents

Battle of the computers

Jerry Leichter <leichter@lrw.com>
Thu, 2 May 91 11:39:43 EDT

As some players in the economy use massive computation to improve their position, will those without access to such resources be left behind? This issue has arisen in the past in discussions of program trading in the stock market. About two weeks ago, in an article in the New York Times that I forgot to clip, an interesting new example came to light.

It seems that airlines are making heavy use of "load management" software. An airline wants to fill as many seats on each flight as possible with passengers paying full fare. However, if there are any seats left over, it is better to fill them with people flying at a discount than to leave

them empty, as the incremental cost of flying the extra passengers is essentially nil.

In the past, airlines have had to guess how many seats on each flight to make available at a discount. These days, they have enormous amounts of data on the past history of all their flights. Further, they have the computational capacity to do an essentially continuous recomputation of the optimal number of seats to offer at a discount. The result is that, on the "desireable" flights - late Friday afternoon, for example - it's extremely difficult to get a discount seat. On Saturday, on the other hand, discount seats are usually no problem. The techniques involved have proved very effective - studies show that for many airlines such load management makes the difference between profit and loss.

Many state regulators see this as a "bait and switch" by the airlines - they advertise seats that are simply not available to most of their customers. One side-effect of airline deregulation, however, was to make the airlines just about totally immune to state regulations, and the Federal government has so far shown little interest in getting involved in this matter.

This leaves consumers on their own. Sure enough, a countervailing force has appeared: Travel agencies have begun to develop programs that continually watch for discount seats to appear and grab them for their customers. The computers battle it out - and anyone without computer assistance is likely to be left on the ground.

An old cartoon shows two people standing on the ground, luggage at their feet, looking up at a plane. The words: "If God had meant us to fly, He would have given us tickets." Perhaps today we should substitute "a PC" for "tickets".

-- Jerry

The risks of risks and leverage

Bob Frankston <Bob_Frankston%Slate_Corporation@mcimail.com>
Wed, 1 May 91 23:44 GMT

The article in today's Wall Street Journal on Prodigy's STAGE.DAT and CACHE.DAT files makes it very obvious how central Risks (and similar discussion groups and journals) have become in this society. Risks itself is very widely read, published and cited. Other lists (e.g. Telecom digest) are read at the agencies such as the FCC.

We are what we what are talking about. Not only in the MacLuhan sense of the media being the message but also in a more literal sense. At one level we look at examples of bad (and sometimes good) engineering and wonder about the design decisions. Yet here we have an example of phenomena rather than engineering. (Are 900 numbers a phenomena or did the implementors foresee the implications?)

I don't know if the WSJ article was a direct result of Risks (or similar media) but all this happened within a few days. A number of the most visible

reporters do read this digest and participate in the electronic media (emedia). Among emedia, Risks is one of the more responsible. (What is the National Enquirer of enews?) (Let's see how long it takes the terms "emedia" and "enews" to become popular -- start tracking).

(Rereading this letter, I'm reminded of the old ads for the Hitchcock saying "The Birds is coming")

[Larry and his brother (Moe?) ...]

Free Speech and Government Control of Information

Jerry Leichter <leichter@lrw.com>
Thu, 2 May 91 11:22:27 EDT

In RISKS-11.54, Larry Hunter responds to my article on control of information. His article provides examples of exactly the kinds of limited approaches that I was trying to get beyond.

There are two basic areas in which we differ. First, Hunter believes I'm attempting to prescribe appropriate actions. If I gave this impression, let me correct it: I'm trying to PREDICT. My claim is not that stricter controls are a good idea. Rather, I suggest that they are an inevitable result of the direction in which our technologies are headed. (There's certainly room for a good deal of debate about "technological determinism" here. It's not that I don't believe that alternative paths are POSSIBLE; I'm just projecting what I think is by far the most likely path.)

The second issue grows from the first, and Hunter's view of how the fundamental laws of our society are determined. To state it starkly: If "society" comes to believe that government controls on information are necessary, will constitutional limitations still prevent them from coming into being? Hunter believes so; I think he's being naive.

The Constitution protects "speech", "religion", "the press". It never defines any of these terms; case law does. We think we know what they mean, and that the "clear meaning" will not change, but history makes it clear that these terms are quite malleable. The authors of the Constitution were mainly thinking of political speech when they wrote (though claiming that it's only political speech they intended to protect is a much different, and probably indefensible, claim). They probably thought they were protecting the right to choose one's religion, most likely so long as it was some variation of Christianity (or maybe Judaism); they were probably not thinking of a right to choose no religion at all. Curiously, their view of "the press" was probably broader than that of most people today, as "pamphleteers" were important contributers to public debate.

Over the years, we've come to construe these terms in very different ways. I very much doubt any of the constitutional authors would have found even comprehensible the argument that a striptease was deserving of First Amendment protection as "symbolic speech". We've chosen to define that "in", just as we've chosen to protect atheism under "freedom of religion".

On the other hand, we have also chosen to leave certain things OUT of our definitions. Television news isn't quite "the press", and is subject to FCC regulation. Freedom of religion doesn't protect Christian Scientists from child abuse claims when they refuse medical treatment for their children. Note that we don't need a constitutional amendment to effectively change the definitions of crucial terms in the Constitution - all we need is a majority of the Supreme Court.

Hunter's examples - conspiracies, slander, copyright violations, and reckless endangerment, commercial speech - all illustrate "speech" that we have chosen, as a society acting through our legal system, to leave out of the definition of that single, simple word in the Constitution. This is a subtle process, and much of it is surprisingly recent: The reckless endangerment exception - the famous "shouting fire in a crowded theatre" - comes, if I recall, from an opinion by Justice Holmes, which puts it early in this century. I don't know how far back the "commercial speech" exception goes, but note that there have been a number of important decisions defining the bounds of that exception in the last 15 years. (The whole reason the commercial speech exception exists is to curb the unfairly loud voice that rich corporations have, given today's media. Before mass marketing, there was little reason to create such an exception, and in fact the traditional concept of "seller's talk" - which basically said "you can't rely on what a salesman tells you (since we all know they exagerate)" - created an area in which "commercial" speech was particularly free.)

Historically, the courts have even been quite prepared to make distinctions based on communications media: Peeking through the keyhole requires a warrant but tapping a phone line - well, we needed to pass a special law for that one. Why else is Lawrence Tribe now suggesting a constitutional amendment on just this matter?

So: I see little reason to suppose that the courts will blindly accept that all computerized information is "speech", if society decides that some limitations on it are necessary.

In the past, we've generally been able to draw the line between things or acts and information - "mere speech": The First Amendment protects your right to publish instructions for building bombs, so we draw the line at the materials you need. In the information age, this line becomes fuzzy. For export, a description of DES is OK, a chip implementing it is not. How about a good software implementation? Should a computer virus - simultaneously speech (pure information) and a potentially dangerous "thing" - be freely publishable?

Let me give a non-computer example of the kind of problem we will face: Mr. M is a numerologist and conspiracy theorist. He believes that he can track down conspiracies in the world by examining various numerical data related to people. He starts a magazine, OutNumber, in which he regularly publishes any numbers he can find concerning (mainly) the rich and powerful. Mr. M has a following, and he has money to pay for tips, so he has no problem finding all sorts of interesting numbers concerning people. Soon he is publishing people's charge account numbers, checking account numbers, PIN's, private telephone numbers, cellular phone numbers, and so on. At no time is there any question of Mr. M's involvement in any attempt to use this data for fraudulent purposes - he is sincerely interested only in his numerological research.

OutNumber, and Mr. M, are probably protected under the Constitution as we currently construe it. My question is, should they be? Do you think there's really a social concensus that it's essential to protect the ravings of a Mr. M, even in the face of (let us imagine) clear evidence of massive fraud by OutNumber readers against those "profiled" in the magazine? How long do you think the courts will stand up in the face of a new concensus that says, hey, get rid of this guy?

Finally, Hunter responds to my suggestion of some fiction stories with readings on political theory. I have no problem with this. The reason I suggest fiction is that social concensus, and ultimately law, grow as much out of the gut as out of the head. Good fiction lets you explore your own gut feelings.

Along those lines, let me suggest Jack McDevitt's "The Hercules Text", which raises the question of whether some information might be so dangerous that one might feel morally compelled to supress it. Also, Fred Hoyle's classic "A For Andromeda" demonstrates how one can wage interstellar war by sending "mere information". (The equally good sequel, "Andromeda Breakthrough", turns the discussion in a different direction, but the point remains.)

Since my first posting, I've found my copy of Asimov's "Earth Is Room Enough". It was first published in 1957, and story I cited is, indeed, called "The Dead Past". Since a summary would destroy the "gut" impact that makes me recommend the story to begin with, I still leave to readers the pleasure of the original. (I'll relent if sufficiently pressed.)

-- Jerry

Re: Four-digit address causes NYC death (Nilges, RISKS-11.55)

Flint Pellett <flint@gistdev.gist.com>
1 May 91 16:50:25 GMT

One poster suggested a more limited set of operations, as in spreadsheets, rather than what you have in "powerful" languages: I don't follow this at all, since 1) I you can set your column width to 4 characters in the spreadsheet and get the same sort of problem, 2) the collection of books I have on Quattro use are about 3 times as thick as any other book I have on any of several programming languages: if anything, a lot of spreadsheets are a lot more likely to cause problems due to being complex than the programming languages are.

Dynamic field lengths supported by languages aren't going to prevent this type of problem, because your screen displays are still a finite size, and operating system utilities that have various fixed limits still abound. (Ever try to work with files that have 2000 characters in the file name in UNIX, and figure out what things handle them and what ones don't?) Availability of more powerful ways to control screen real estate (like the ability to put up a scroll-bar that would let you scroll thru the file name looking at 80 characters of the 2000 at a time) are a first step, but even if every variable had infinite length and the only way you could display it was using a scrollable method, you'd still have problems: now you have something so complex

a human can't digest it or remember it or deal with it. 5 Digit addresses may be the same thing: maybe the problem there is that someone should have created addresses with no more than 4 digits in the first place. It reminds me of people who put 2000 different files into one directory, rather than organizing that directory into several lower level directories: why didn't someone organize the hierarchy of addresses so that they had groupings (towns, precincts, whatever) in which the addresses were kept smaller? By the time you let things grow to where you have 1000001 Fifth Ave and 100001 Fifth Ave (did you notice those aren't the same address!?) it isn't the computers causing the problem.

Flint Pellett, Global Information Systems Technology, Inc. 1800 Woodfield Drive, Savoy, IL 61874 217-352-1165 uunet!gistdev!flint flint@gistdev.gist.com

---

Four Digit Addresses in NYC

Ed Ravin <eravin@panix.UUCP>
Wed, 1 May 91 12:31:18 EDT

I can't believe this one -- large sections of Queens have addresses along the lines of XXX-YY, where XXX is the number of the cross street, and YY is the address unique only within that block. For example, if you lived on 89th Avenue in the Jamaica section of Queens and the nearest numbered street was 169th Street, your address might be 169-25 89th Avenue. The house on the next block, near 170th Street, could have an address 170-25. And so on. Although it's easy to see how an incompetent or poorly trained emergency operator could mix up one of these addresses that sound more like IBM error messages than places to live, I don't think it's possible that the computer system the operators and dispatchers use could have a fixed limitation to four digits on an address -- as you can see, the address above (and there are plenty like it in Jamaica and nearby) is six characters if you include the hyphen.

Remember, the original posting came from a press report, where the reporter may well have just repeated without critical examination of what someone said, or mixed up what someone said. This kind of inaccuracy in reporting extends to all fields, not just technical.

Ed Ravin cmcl2!panix!eravin philabs!trintex!elr +1 914 993 4737

Re: Four-digit address causes NYC death

Bob Frankston <Bob_Frankston%Slate_Corporation@mcimail.com>
Wed, 1 May 91 16:02 GMT

Representation is a nontrivial issue. While it may be "obvious" that one should allow for five digit addresses, what about fractional addresses due to subdivided lots (how do you say "384 3/8e 1St SW" in ASCII, how does it sort?? Apartment addresses? Alternative addresses (6th Ave vs Avenue of the Americas)? Why not require full color graphics and then discover you can't present it on a belt-mounted radio?

Then there are the problems of real design against performance and cost constraints? And design cycles that involve committees and 20 years of studiously ignoring technology change

I'm more concerned with superhuman requirements and a "hang 'em by their thumbs" attitude discouraging attempts at system design. Safer to kill by omission than commission. While it is necessary to encourage and even enforce responsible system design, it is not magic.

While much is made of better techniques for creating bug free systems through better technical tools, you can't anticipate all the quirks of mapping the design to the real world. I'm much more interested in the whole design cycle including reintegrating experience from the field. How does a fix like supporting 5 digit addresses get integrated back into the E911 system? How long does it take?

At some point in a system's life cycle fixing bugs tends to increase the total number of bugs. What methodologies mitigate this problem and, in effect, continually refresh a system? Part of the problem is that engineering and learning does involve taking risks (as Petrovsky as noted in some of his books). Systems where risk is not allowed do not grow and refresh. At least not internally. (I better stop here, otherwise I'll get into a discussion of the dangers of military/government procurement vs comme rcial/academic experimentation).

Re: Hacking, Civil, and Criminal Law

Jim Giles <jlg@woodsy.lanl.gov>
Wed, 1 May 91 09:44:40 MDT

"Herman J. Woltring" <UGDIST@nici.kun.nl> writes:
> [...]
> If you open your vaults, dismiss the guards, turn off the alarm, and if your
> name is Dagobert Duck, you are equally liable for solliciting criminal
> behaviour as is #789-123 for committing a felony while he purloins your
> bullion. [...]

Not by the laws of any modern nation. What Mr. Woltring is saying is the same as: "If a woman puts on a dress and walks into a bar, she's as guilty of gang-rape as the men in the bar." To be sure, the bank manager who dismisses the guards and the woman who enters the sleazy bar are negligent, perhaps criminally so, but that doesn't mitigate the guilt of the robbers or the rapists.

> [...] In my book, simplistic passwords, retaining known system passwords
> or not plugging known, remote-access loopholes are tantamount to the same.

To take Mr. Woltring's analogy between physical property and computer networks into account, what are the analogous structures? Simplistic passwords are analogous to easily picked locks, known system passwords: emergency access doors, remote-access loopholes: loose boards in the

wall. Now, if I leave the door open, and you come in - you are _still_ guilty of trespass. If I lock the door and you come in, you are quilty of breaking and entering. This is a much more serious crime than trespass since the fact that you entered in spite of the lock shows intent. It doesn't matter how easily the lock was to pick, the emergency exit to break, or the loose board was to find, the fact of breaking through any of those shows that you _intend_ to trespass.

The only difference between this and the computer network issue is that some countries have not yet extended the laws of property to computational facilities. In my book, breaking into a system that is guarded by passwords should be criminal. I shouldn't matter how easy the passwords were to guess or to crack. That is an issue of negligence on the the part of the authorized users - it does not mitigate the guilt of the hacker that breaks in.

J. Giles

Research Project

<P.A.Taylor@edinburgh.ac.uk>
01 May 91 14:16:14 bst

I'm in the second year of a PhD which is looking at the rise of the computer security industry and the various groups which make up the "computer underground" or whatever term should be used.

There are two questionnaires I've been using in the research. The first is a very short yes/no type one, designed to produce a data-base of raw statistical information. The second gives a lot more room for opinions and if the respondents are amenable could form the basis of e-mail discussions/ interviews.

If you would like to help in the research then please drop me a line.

ALL RESPONSES WILL BE TREATED IN TOTAL CONFIDENCE, THE WORK IS FOR SOLELY ACADEMIC PURPOSES. A FULL ANALYSIS OF RESULTS WILL BE MADE AVAILABLE TO ANYONE WHO IS INTERESTED.

Verification of my academic status can be sought from my main supervisor Dr. R. Williams, Director of the Research Centre for Social Sciences, here at Edinburgh University, at the same e-mail site as myself.

Paul A. Taylor, Depts of Economics and Politics, Edinburgh University.

Larry Hirschhorn, Beyond Mechanization, MIT Press, 1984.

Phil Agre <phila@cogs.sussex.ac.uk>
Tue, 30 Apr 91 14:56:36 +0100

Larry Hirschhorn, {\em Beyond Mechanization: Work and Technology in a Postindustrial Age}, Cambridge: MIT Press, 1984.

This is an extremely relevant book that I don't recall seeing mentioned on RISKS before. It's by a management professor, about the new styles of work that are required by new market structures and by the risks inherent in feedback-based technologies. Here are some quotes about RISKS:

We see that watchfulness and attention must be mobilized, because cybernetic-automatic systems introduce new and unexpected ways of failing. Work takes on a new meaning in this context. ... in cybernetic systems machines and workers complement each other with respect to a typology of errors: machines control expected or `first-order' errors, while workers control unanticipated or `second-order' errors (page 72).

If, as I believe to be the case, error is inevitable in automatic systems---if there are always to be modes of failure that cannot be automatically regulated by feedback-based controls---then learning must be instituted in order to prepare workers for intervening in moments of unexpected systematic failure. Failure, in turn, is a specific example of discontinuity and developmental change. Thus we could define postindustrial work as management at the boundaries of systems and physical realities. Historically, we would then see the worker moving from being the controlled element in the production process to operating the controls to controlling the controls (page 73).

We can find an analogy in daily life. A young child, learning to walk, constantly trips over her own feet. Once she has mastered walking, she may still hurt herself; indeed, because she has mastered walking, she enters new environments that strain her skill in new ways. Each increase in self-regulating capacity is matched by a new context that stretches the newly developed capacity to new limits. Thus the system, always functioning at its limits, is always vulnerable to failure (pages 82-83).

The new technologies do not constrain social life and reduce everything to a formula. On the contrary, they demand that we develop a culture of learning, an appreciation of emergent phenomena, an understanding of tacit knowledge, a feeling for interpersonal processes, and an appreciation of our organizational design choices. It is paradoxical but true that even as we are developing the most advanced, mathematical, and abstract technologies, we must depend increasingly on informal modes of learning, design, and communication (page 169).

2nd PDCS Open Workshop, Newcastle/Tyne - 28-30 May 1991.

Nick Cook <Nick.Cook@newcastle.ac.uk>
Mon, 29 Apr 91 12:34:24 BST

ESPRIT BASIC RESEARCH ACTION 3092
PREDICTABLY DEPENDABLE COMPUTING SYSTEMS (PDCS)
ANNOUNCEMENT - 2ND PDCS OPEN WORKSHOP
(WORKSHOP PROGRAMME INCLUDED)

28-30 MAY 1991
THE COPTHORNE HOTEL, THE QUAYSIDE, NEWCASTLE UPON TYNE, UK

The Workshop Programme, details of venue etc., Registration Form and PDCS Project Synopsis follow.

There are still places at the Workshop and there is still time to register for a place. So if you wish to be considered for a place, or have any queries, simply contact me for registration form, information, etc. (by s-mail, email, phone or fax - details below).

Nick Cook, Administrative Coordinator, PDCS

The Computing Laboratory, The University,
Newcastle upon Tyne NE1 7RU, UK Tel: +44-91-222-7827 Fax: +44-91-222-8232
Email: Nick.Cook@newcastle.ac.uk

----------WORKSHOP PROGRAMME----------
2ND PDCS OPEN WORKSHOP, 28-30 MAY, 1991

THE COPTHORNE HOTEL, QUAYSIDE
NEWCASTLE UPON TYNE

The Workshop will be based on presentations from PDCS grouped under eight subject headings pl.us about ten demonstrations. The final session of the Workshop, Assessment of Very High Dependability Software, will include prepared responses from two guest speakers.

The presentation sessions will be introduced by a moderator, who will also conduct the discussions that follow. They will be held in series and consist of a number of talks from PDCS covering: Dependability Requirements, Fault Tolerance, Real-Time Issues, Proving and Testing, Software Engineering Environments, Security, Evaluation and Ultra-high Dependability.

Demonstrations currently planned are: Paralex (Universita' Bologna), Recalibrating Software Reliability Models (City University), Authentication - secure LAN (EISS/Universitaet Karlsruhe), Statistical Testing and SOREL (LAAS-CNRS), Tool for Relating Dependability Requirements to Organisational Structure and a demonstration based on the Laboratory's train-set (as seen at FTCS-20) (University of Newcastle upon Tyne), Design Environment for Real-Time Systems and a video presentation of rolling ball experiment (Technische Universitaet Wien), Z-checking (University of York).

In addition to the main Workshop business there will be a reception by the Lord Mayor of Newcastle at 18.00 on Tuesday and a banquet dinner at approx. 20.00 on Wednesday (leaving Newcastle at 18.45).

The full, preliminary, programme is given on the following pages. Please note: some details are not available yet, such as exact session/presentation titles, and will change before the Workshop. However, all the subject areas indicated will be covered. Also, at this stage the timings are given as indicators of session/presentation length only and are liable to change.

TUESDAY 28 MAY 1991

10.30-11.15 Welcome address and Overview of PDCS and the Workshop
- Brian Randell, University of Newcastle upon Tyne

11.15-12.00 DEPENDABILITY REQUIREMENTS
Moderator: Brian Randell, University of Newcastle upon Tyne
Presentations and speakers:
11.15-11.45 Frameworks for expressing non-functional requirements
- John McDermid, University of York
11.45-12.00 Discussion conducted by the moderator

13.30-15.30 METHODS AND PARADIGMS FOR FAULT-TOLERANT SYSTEM DESIGN
Moderator: Jean Arlat, LAAS-CNRS
Presentations and speakers:
13.30-14.00 Fault Assumptions and Assumption Coverage - David Powell,
LAAS-CNRS
14.00-14.30 Structuring Fault Tolerance in Software Design
- Lorenzo Strigini, IEI del CNR
14.30-15.00 Frameworks for Fault Tolerance - Tom Anderson,
University of Newcastle upon Tyne
15.00-15.30 Discussion conducted by the moderator

15.45-17.25 REAL-TIME ISSUES
Moderator: Luca Simoncini, Universita' di Pisa
Presentations and speakers:
15.45-16.25 Time Triggered Architectures - Hermann Kopetz and
Peter Puschner, Technische Universitaet Wien
16.25-16.55 Predictability and Flexibility in Hard Real-Time Systems
- Alan Burns, University of York
16.55-17.25 Discussion conducted by the moderator

18.00 Reception by the Lord Mayor of Newcastle upon Tyne
at the Civic Centre

WEDNESDAY 29 MAY 1991

08.45-10.15 PROVING AND TESTING
Moderator: Norman Fenton, City University
Speakers:
08.45-09.15 Marie-Claude Gaudel, LRI-Universite de Paris Sud et CNRS
09.15-09.45 Pascale Thevenod-Fosse, LAAS-CNRS
09.45-10.15 Discussion conducted by the moderator

10.30-12.00 SOFTWARE ENGINEERING ENVIRONMENTS
Moderator: Santosh Shrivastava,
University of Newcastle upon Tyne
Presentations and speakers:
10.30-11.00 An Engineering Approach to Hard Real-Time System Design
- Ralph Zainlinger, Technische Universitaet Wien
11.00-11.30 Paralex: An Environment for Parallel Programming in
Distributed Systems - Ozalp Babaoglu,
Universita' di Bologna
11.30-12.00 Discussion conducted by the moderator

13.00-13.30 Buses (or walk) to Computing Laboratory for Demonstrations

13.30-18.00 DEMONSTRATIONS IN COMPUTING LABORATORY
Including in groups of 3 (exact arrangements to be determined):
Paralex (Universita' Bologna)
Recalibrating Software Reliability Models (City University)
Authentication - secure LAN (EISS/Universitaet Karlsruhe)
Statistical Testing and SOREL (LAAS-CNRS)
Tool for Relating Dependability Requirements to Organisational Structure and a demonstration based on the Laboratory's train-set - as seen at FTCS-20 (University of Newcastle upon Tyne)
Design Environment for Real-Time Systems and a video presentation of rolling ball experiment (Technische Universitaet Wien)
Z-checking (University of York).

18.45 Buses leave for Banquet at Redworth Hall, County Durham

THURSDAY 30 MAY 1991

08.45-10.15 SECURITY
Moderator: John Dobson, University of Newcastle upon Tyne
Speakers:
08.45-09.15 Yves Deswarte, LAAS-CNRS
09.15-09.45 Dieter Gollmann, EISS/Universitaet Karlsruhe
09.45-10.15 Discussion conducted by the moderator

10.30-12.00 EVALUATION
Moderator: Pierre-Jacques Courtois, Philips Research Laboratory Brussels
or Isi Mitrani, University of Newcastle upon Tyne
Presentations and speakers:
10.30-11.00 Analysis of Software Failure Data - Sarah Brocklehurst, City University and Karama Kanoun, LAAS-CNRS
11.00-11.15 Discussion conducted by the moderator
11.15-11.45 Towards Cost Models for Security Evaluation - Bev Littlewood, City University and John McDermid, University of York
11.45-12.00 Discussion conducted by the moderator

13.30-15.40 ASSESSMENT OF VERY HIGH DEPENDABILITY SOFTWARE
Moderator: Alain Costes LAAS-CNRS
Speakers:
13.30-14.00 Jean-Claude Laprie, LAAS-CNRS
14.00-14.30 Bev Littlewood, City University
Discussants responding to presentations:
14.30-14.50 John Meyer, University of Michigan
14.50-15.10 Martyn Thomas, PRAXIS plc
15.10-15.40 Discussion conducted by the moderator

15.40 Closing address - Brian Randell, University of Newcastle upon Tyne

Mr Nick Cook, Administrative Co-ordinator, PDCS

The Computing Laboratory, The University,
Newcastle upon Tyne NE1 7RU, UK
Tel: +44-91-222-7827
Fax: +44-91-222-8232
Email: Nick.Cook@newcastle.ac.uk

Search RISKS using swish-e

THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

ACM Committee on Computers and Public Policy, Peter G. Neumann, moderator

Volume 11: Issue 61

Friday 3 May 1991

Contents

The means justify the ends? (piracy probe)

Jim Cheetham <jim@oasis.icl.co.uk>
Thu, 2 May 91 15:35:59 BST

From the front page of "Computing", 2 May 1991, comes the following report (quoted with permission). Comments/indications of unquoted text are in []s.

DEC raids consultant in piracy probe (by Joanne Evans)

DEC has searched the office and home of a training consultant in Reading [England -jim], confiscating hardware, software and paper files to find evidence of alleged software piracy.

> A number of people from DEC and it's solicitors, Linklaters & Paines,
> searched the home of Greg White [...] on 5 April while he was out.
> They had obtained a civil search warrant.
>
> Earlier in the day, they searched the office of Syntellect, an arm of
> a US training company which Greg White runs in the UK. [...]
>
> DEC was granted the Anton Piller order, a warrant granted without the
> subject's knowledge, by the High Court of Justice Chancery Division
> in London on evidence alleging that Syntellect was using unlicensed
> software to provide training courses. [...]
>
> The evidence was obtained by a consultant employed by DEC at attend
> a Syntellect training course in February. He copied it's system
> software which was later examined by DEC. [...]

Besides the problem of someone holding unlicensed proprietary software, what strikes me here is the subterfuge used by DEC to gain the evidence they needed in the first place. Surely the consultant attending Syntellect's training course didn't ask for permission to copy their system? In which case, is the evidence not inadmissable by virtue of being gained by illegal means?

This seems to be a case where "the ends justify the means", which is most definitely *not* acceptable in the legal system normally. Another example of the law not being in touch with computers, perhaps?

Jim Cheetham, jim@oasis.icl.co.uk, +44 344 424842 x3121 (ICL ITD 7263 3121)

Re: Almost Humorous Fly-by-Wire Glitch

Mary Shafer <shafer@skipper.dfrf.nasa.gov>
Thu, 2 May 91 13:55:59 PDT

Joseph Nathan Hall (jnh@eceugs.ece.ncsu.edu) writes:

> From the pages of Popular Science, April 1991:
>
> "...Spectators at the first flight of Northrop's [YF-23] prototype noticed
> its huge all-moving tails--each larger than a small fighter's wing--quivering
> like butterfly wings as the airplane taxied out to the runway. Test pilot
> [Paul] Metz says this occurred because the early generation flight-control
> software didn't include instructions to ignore motions in the airframe caused
> by pavement bumps. The answer, he adds, is inserting lines of computer code
> that tell the system not to try to correct for conditions sensed when the
> fighter's full weight is on its nose gear."

Talk about a pack of slow learners. I remember sitting in the control room watching the AFTI/F-16 waving its canards and tail at every expansion joint in the taxiway. They finally stopped it with a squat switch. But I shouldn't criticize the YF-23 team too much, because the X-29 didn't have one originally,

either.

> I'll grant that in the 1990s we can analyze wind-tunnel tests in a few hours (or less) and can even simulate untested airframes with some success. In the 1950s pilots frequently flew prototypes before the final results of early wind-tunnel tests were completely analyzed--a process that sometimes took weeks or months. But am I alone in thinking that in some respects it takes more chutzpah to test-fly one of these modern fly-by-wire wonders? <shudder>

What do you think they do, drop in a computer and tell the pilot to take it around the pattern a couple of times? No wonder everyone's so goosy about fly-by-wire. We're talking about V&V here--verification and validation.

The very least they will do is hot-bench testing, with all the hardware in place and the best aerodynamic model in a computer. They may well have had an iron bird, although I doubt it. The B-2 maybe, but not the YF-23, in my opinion. The iron bird for the F-8 Digital Fly-by-Wire (DFBW) was an F-8C airframe, with the wing tips removed and the engine gone. The hydraulic system, the actuators, the surfaces, the FCS computers--all the "real" hardware, with the aerodynamics in a computer. I don't think there were iron birds for the F-16 or F-18, since our experience with the F-8 DFBW indicated that it was at best an act of supererogation and at worst a red herring. We spent months trying to take care of a problem that turned out to be unique to the iron bird itself.

The X-29, 30-per-cent statically unstable little beast that it is, didn't have an iron bird and it was a great deal more experimental than the YF-23. Nor did the HiMAT or the Shuttle.

A good FCS is sufficiently robust that it can deal with variations in the stability and control derivatives. In general, the initial FCS will be tuned when the derivatives are determined during the envelope expansion that is the first part of the flight program. We have a pretty good idea just how good or bad a particular derivative from the tunnel tests is and we can make worst-case assumptions based on the historical error margins. This is called parametric variation. I was involved in just such an assessment for the Space Shuttle back in the mid-70s.

There is an interesting example of FCS robustness from the Shuttle. Rolling moment due to yaw jet is not only twice the predicted magnitude, it has the opposite sign. The FCS was sufficiently robust to deal with this, although hand-flown roll reversals replaced the preprogrammed ones until the FCS was refined after STS-5.

I've asked our pilots about this and they don't think that it takes anything more from the pilots to fly modern FBW aircraft. The F-8 DFBW, the first digital FBW airplane, was, they say, a little more exciting, but that was some time around 1970 and it had no reversion mode. But modern FBW is no big deal. One of them does admit to being a little nervous about the forward-swept wing on the X-29, though.

Mary Shafer shafer@skipper.dfrf.nasa.gov ames!skipper.dfrf.nasa.gov!shafer
NASA Ames Dryden Flight Research Facility, Edwards, CA

Re: Old O/S and Network Security

Rick Smith <smith@SCTC.COM>
Thu, 2 May 91 15:51:24 CDT

The article about securing old OSes presented some interesting ideas, but it leaves the impression that you can easily solve security problems simply by installing systems with high NCSC security ratings. This is not true.

>If you REALLY want security, install a Honeywell SCOMP between the
>internet, and your local host, LAN, or whatever; at less cost, and more
>risk, install any C2 or better O/S host at that connection site.
> {followed by more about using B2 hosts}

Neither the SCOMP nor a C2 rating provide a magic shroud to protect you from network-borne crackers if you depend on the usual Userid and Password for access to your LAN. A password based authentication system meets the requirements even for an A1 rating. You still need security-conscious users who use passwords in a secure manner, or even an A1 system can be penetrated.

The distinguishing security feature of systems rated B or higher is that they keep a computer's data and activities strictly separated by "security levels." In a military environment you would set up the system to prevent "secret" information from intermingling with "unclassified" information. The system then keeps data at higher levels from leaking into lower levels, whether by accident or on purpose. Higher security ratings (B2, B3, A1) indicate stronger assurance that objects at different levels remain properly segregated.

Even MAIL between users at different security levels is generally prevented. Mail from a higher level user to a lower level user is completely forbidden since it would provide a path for "secret" data to leak out. Strictly speaking, a lower level user may send mail to a higher level user, though the system would not tell the sender if the mail was actually received.

Despite such restrictions, there are real benefits for commercial users. For example, a company could use level separation by defining a "public" level similar to the military's "unclassified" level and a "proprietary" level similar to "secret." Users operating at the proprietary level would be prevented from leaking proprietary data into public areas, and users at the public level could access the public internet. This would protect proprietary data from internet access. This would not necessarily protect the multilevel host from crackers entering it at the public level, but it would keep them away from company valuables.

However, this assumes that only A and B rated computers can access both the sensitive data and the public network. If your unsecure computer can access both your sensitive data and your public network, then you have subverted any other protection you might have provided.

> [The Honeywell SCOMP -- still the only A1 evaluated system --
> is now the Bull SCOMP. ... PGN]

The current version of SCOMP, the XTS-200, is currently under evaluation at the B3 level, not A1. I do not know if an A1 SCOMP is still available, though perhaps another netter might.

Rick. smith@sctc.com Arden Hills, Minnesota

Re: Old O/S and Network Security

Mike Muuss <mike@BRL.MIL>
Wed, 1 May 91 21:56:53 EDT

Bob, In your recent message, you wrote:

<> For years now, there has been a reasonable solution to the problem of
<> "an old O/S" and network security: Install a newer, much improved O/S
<> (WRT network security) _between_ the open network, and the "closed"
<> community that uses the old O/S to process valuable information.

In general, I strongly *disagree* with this policy. The consequence of erecting just one fence around your internal network is that, if any one node of your internal network is compromised, then the entire internal network is compromised. Not a pretty thought.

This was clearly spelled out in the old Army Regulation 380-380, which indicated that every host *must* fully defend itself at the host/network interface. Any additional protection at the local_network/WAN interface was "gravy", but did not count towards successful accreditation of the host's defenses.

I find this strategy rather comforting, knowing that every host on the network is prepared to defend itself, rather than being entirely dependent on the services of the "guard force".

[This discussion generalizes to private life, too. Are you personally prepared to deal with natural disasters, civil disobedience, etc. yourself, at least to a limited degree, or do you place 100% faith in the services of the police and other government agencies? There is a term for people who are prepared: "survivors". Same for computers. But, I digress.]

I've had the privilege of providing the Army's most effective "Tiger Team" to help check internal security at other installations. Installations such as you describe are always the easiest to compromise, because when (not if) you find the first "chink in the armor", the entire site is yours to command.

However, there is an even more severe penalty from the type of policy that you propose. I'm a big proponent of network distributed computing. I used a lot of X windows, BRL-CAD LIBFB remote framebuffers, and distributed high-performance computing applications. On one occasion in '85, I used every Gould PN9000 computer on the MILNET on the east coast of the US to run my distributed ray-tracer, to get images ready for a

publication deadline. (Made it, too!).

I also travel a lot to various Universities and National Labs. I'm quite accustomed to being able to simply "reach out" and invoke processing power on my SGI compute server or one of our Crays, and interact with the processing. Regardless of where I am. I've delivered lectures at NASA facilities, where the images were interactively computed by BRL's XMP and provided in real time over the InterNet. I've run calculations in the USA from the back of a British personnel carrier as RSRE (RSRE packet radio to SATNET to ...).

This type of scientific computing environment is completely compromised when you interpose Janus hosts between the internal and external networks. This spoils the fruits of the past 10 years of accomplishments of DARPA and the network research community.

Furthermore, it usually isn't even very secure. Usually, when I'm trapped into working at such a site for more than a few hours, I manage (as an unprivileged user) to create a bypass in the Janus host, so that I can get some work done. Thus defeating your "security" again.

Now, I understand that at some sites, it is not possible to implement good security on some selection of hosts. (Macintosh and PC's are prime examples of this). In those cases, it may well make sense to isolate those fundamentally insecure machines in a "leper colony" sub-network. But all "real" computers (i.e. anything >= a Sun-2/50) with "real" software (i.e. UNIX, TOPS-20, VMS, etc.) should be provided with a full host defense, and given full access to the network.

So, if you need to implement a "leper colony", at least you will be more aware of the risks associated with doing so. It has a potentially large negative impact on legitimate use of your computers, and it has security vulnerabilities of it's own. However, in the final analysis, it may be cheaper and easier to do than actually implementing real security on all your hosts. I'm certain you can see which strategy I prefer.

I'd like to close by quoting my "golden rule" for computer security:

> "Computer security should be strong enough to repel virtually any attack ***from the outside***, yet unobtrusive enough that the average user is unaware that he is being guarded by a strong defense." -Mike Muuss

Mike Muuss, Advanced Computer Systems, Vulnerability/Lethality Division
U. S. Army Ballistic Research Laboratory

PRODIGY: STAGE.DAT

A. Padgett Peterson, 407-356-6384 <padgett%tccslr.dnet@uvs1.orl.mmc.com>
Thu, 2 May 91 15:36:06 -0400

>From: Bill Seurer <seurer@rchland.vnet.ibm.com>
>Subject: A Prodigy experiment

>The results are:
> Prodigy does not appear to be uploading any data.
> The STAGE.DAT file contains bits and pieces of ERASED files.

I first saw mention of this shortly after the "new" PRODIGY software came out and have participated in a number of discussions on the PC Board before deciding that just the same questions were being asked over and over and....

Consequently, a few months ago I did some testing of my own since my PC has some unusual system integrity management tools resident.

Findings:

1. PRODIGY does not seem to have modified any executables on my system following installation that use the normal DOS EXEC call to load. (A warning screen would appear if this happened) Though PRODIGY has stated that it has the power to do so. Of couse PRODIGY could load a file as data and tranfer execution to it without using EXEC.

2. PRODIGY does seem to have captured the contents of memory at time of installation inside STAGE.DAT. (just before installation I did a SCAN of the disks for viruses using the McAfee utility. The data used by McAfee is encoded in the file to prevent alarming on his own utilities and to make it more difficult for virus writers to discover the strings in use. The decypted strings that would have been in memory were found within STAGE.DAT.

   This probably accounts for the report of the ENVIRONMENT strings and the root directory entry in STAGE.DAT since they are stored in memory.

The bottom line is that I do not know what the limits of PRODIGY's control over my PC when connect are and PRODIGY is not willing to disclose that information. The RISK is not in what is being done today, but what COULD be done by a malicious person or entity with sufficient access (legal or otherwise).

Padgett

Do unauthorised users deserve the protection of the law?

<HCART@vax.oxford.ac.uk>
Thu, 2 MAY 91 17:00:38 BST

Herman Woltring has presented an interesting defense of his compatriots in Holland who have obtained unauthorised access to computers in the US. He argues that "[owners who] are often too lazy to accept their civil responsibilities...try to fall back on criminal law ... to protect their private interests."

Let's be clear about this: the law has to take a stance. It can protect the interests of legitimate users, by making unauthorised access illegal. Or it can protect unauthorised users by making it legal.

If the law can work for just one of these two groups, which should it be? Legitimate users, who pay for and maintain their systems, deal with the frustration and expense of break-ins and often need the computer systems as a vital part of work or research?

Or unauthorised users, whose use occupies system resources and may intentionally or otherwise cause file system damage?

Mr. Woltring evidently believes unauthorised users need the protection of the law more than legitimate users. Could he now tell us the moral arguments behind this conclusion?

Hugh Cartwright. Physical Chemistry, Oxford University, UK.

---

rude behavior and the net.police (Knowles, RISKS-11.58)

Edward Vielmetti <emv@ox.com>
Fri, 03 May 91 01:14:19 EDT

Brad Knowles (blknowle@frodo.jdssc.dca.mil) says some reasonable things, and then goes off the edge a little bit.

> .. if someone from the University of Utrecht keeps breaking into
> computers at Lawrence Livermore Labs, or NASA, or where ever, and we
> can't get the local police to prosecute them (assuming that we have
> collected enough information to identify the perpetrators), then our
> only course of action is cut the Univerisity of Utrecht off from the
> Internet in the US.

It's well within the rights of Livermore or NASA (or their contractors) to put in filters that would deny access from Utrecht to the NASA networks; that might cause some inconveniences if NASA folks actually want to talk to Utrecht folks. Most modern routers have packet filters and network routing control which would make it reasonably straighforward to cut off intruders if you knew their point of access. If you want to press home the point, then have NASA (or where ever) selectively cut off access to the resources which they provide to the Internet, e.g. make everyone from Utrecht get a message when they go to ftp the latest Voyager images at ames.arc.nasa.gov that they are not welcome until they clean up things locally.

> If most every University in the Netherlands has
> people trying this, then we must cut them all off. Since the Defense
> Communications Agency (DCA, soon to be changing our name to Defense
> Information Systems Agency (DISA)) has the right, nay the
> RESPONSIBILITY to keep up (and presumably to police) the Internet,
> then I think I can safely say that this might actually get implemented
> if the folks over at the University of Utrecht keep it up.

Who hired you to be the net.cops? I'm going to be rather annoyed if DCA comes trooping into Alternet headquarters, demanding that the Alternet-EUNET link from Virginia to the Netherlands be severed because of lousy network security

inside of Livermore. Consider that the vast majority of the network is well-served by the link to the Netherlands, and that storming in and cutting off the link because of your putative RESPONSIBILITY is going to have negative consequences for quite a few people.

> We must *not* punish the victims for the crimes of others! As
> was stated by another author, some folks simply don't have a choice
> -- they *must* stay with an old version of their OS becuase some
> mission-critical piece of software runs *only* with that version of
> the OS.

Corporate America (e.g. Ford, AT&T, Sun) have learned to live on the Internet with less-than-secure systems internally by putting in appropriate application level and network security instruments around their systems. If that particular fragile old insecure system has mission-critical software on it, what the *hell* is it doing sitting there out exposed on the Internet? The very least responsibility you have is to pay for your own costs of security and not foist the burden upon the entire rest of the Internet population. Don't drag the rest of us down forcing us to pay for your mistakes.

Msen Edward Vielmetti moderator, comp.archives emv@msen.com

"(6) The Plan shall identify how agencies and departments can collaborate to ... expand efforts to improve, document, and evaluate unclassified public-domain software developed by federally-funded researchers and other software, including federally-funded educational and training software; "
High-Performance Computing Act of 1991, S. 218

Software Warranty

Geoffrey H. Cooper <geof@aurora.com>
Thu, 2 May 91 18:05:01 PDT

I recently bought a three licenses of BBN/Slate for $297 on a special offer. The software came with a little booklet describing the licensing agreement. I was impressed that an honest and sincere effort had been made to make it understandable to an educated person who was not a lawyer. Gold star, BBN.

The document included a software warranty. This was covered some time ago by RISKS in the context of the risks of usual software shrink-wrap agreements; some said it was possible and some said it couldn't work. But I don't recall anyone ever bringing up an actual software warranty that is in use.

So I typed in the juicy bits. I haven't had cause to test this warranty, so I still don't know if it works in practise. It did give me a warm, fuzzy feeling to read it after paying my money. By the way, it also appeared that BBN didn't debit my charge card till the 30 day warranty was up.

[There is no copyright on the agreement, although the term BBN/Slate is listed as a registered trademark.]

>From "Licensing Agreement for BBN/Slate(TM) Software":

7. Limited Warranty and Disclaimer of Liability

BBN HAS NO CONTROL OVER LICENSEE'S USE OF THE SOFTWARE, THEREFORE, BBN DOES NOT AND CANNOT WARRANT THE PERFORMANCE OR RESULTS THAT MAY BE OBTAINED BY ITS USE. HOWEVER, BBN PROVIDES THE FOLLOWING LIMITED WARRANTY:

LIMITED WARRANTY COVERING BBN SOFTWARE PRODUCTS
BBN/SLATE SOFTWARE PRODUCTS

What is Covered:

BBN Warrants that the magnetic tape cartridge(s) on which the enclosed computer SOFTWARE is recorded and the DOCUMENTATION provided with it are free from defects in materials and workmanship under normal use. BBN warrants that the SOFTWARE itself will perform substantially in accordance with the specifications set forth in the DOCUMENTATION provided with the SOFTWARE when used on an appropriate computer. It is <

Risk Analysis Seminars

"Cecilia Spears" <NG.CSW@Forsythe.Stanford.EDU>
Thu, 2 May 91 16:38:09 PDT

The next upcoming "Risk Analysis Seminar Series" Coordinated by Prof. M. Elisabeth Pate-Cornell. Location: Terman Building, Room 101, Time: 4:15 to 5:30 PM. This class is offered for credit to Stanford students; one unit per quarter. Open to the public - no charge. Offered by Department of Industrial Engineering and Engineering Management.

The schedule is as follows:

May 9: Dr. Max Henrion, Rockwell International, Palo Alto: "COMPARING DIAGNOSTIC RULES AND PROBABILISTIC INFERENCE FOR KNOWLEDGE-BASED SYSTEMS"

May 23: Prof. Daniel Kahneman, University of California, Berkeley: "TIMID DECISIONS AND BOLD FORECASTS"

WORMSC Call for Abstracts

Andrew Lacher <m18709@mwvm.mitre.org>
Friday, 3 May 1991 13:53:50 EDT

** Call for Abstracts **

The Washington Operations Research & Management Science Council (WORMSC) is looking for presentation abstracts for their 28th annual symposium in Washington, DC on October 28, 1991. Subject matter is flexible but should relate to operations research or management science. If you have questions or

would like to submit an abstract, please contact:

Andrew Lacher, The MITRE Corporation, 7525 Colshire Drive, McLean, Virginia 22102 703-883-7182 m18709@mwvm.mitre.org

[The WORMSC Call in, the WORMSC Call out, ... Do WORM-SCrawl him a line, and you can bite, hook, line, and synch-er. PGN]

Search RISKS using swish-e

Report problems with the web pages to the maintainer

Search RISKS using swish-e

THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

ACM Committee on Computers and Public Policy, Peter G. Neumann, moderator

Volume 11: Issue 62

Monday 6 May 1991

Contents

9th Federal Reserve Bank Drowned

<TMPLee@DOCKMASTER.NCSC.MIL>
Mon, 6 May 91 01:36 EDT

On Monday April 8 the computer center at the Minneapolis Federal Reserve Bank was flooded out of commission by a broken air-conditioning cooling water pipe in the ceiling. [I'll ignore the RISKs of such a design; the point of this note is something else.] The Minneapolis Fed covers 1,700 financial institutions in six states; it moves something like $10 billion daily. Note that in addition to the normal check-clearing functions one associates with it, a Federal Reserve bank handles things like direct-deposit of paychecks in its region, so cessation of its function for any length of time can cripple a regional economy. An article in the April 29th Minneapolis Star Tribune describes in fair detail how effective the contingency plan was -- all functions were transferred to a back-up facility in Culpeper, Virginia, using a not-very-well-described set of "minicomputers" at the U.S. Postal Data Service Center near the Minneapolis Airport as an intermediary. (The article says:

"They would serve as the new intake center for data transmitted by financial institutions by direct computer hookup, phone line and messenger. From there the information would be routed over the postal center's high-speed, secure phone line to the auxiliary center in Culpeper.") The Culpeper center is the back-up for 10 of the 12 federal reserve districts -- and this apparently was the first time it was used. The back-up was in operation within 12 hours, although it appears to have taken almost a week before all services were fully restored, and up to ten days for some transactions to catch up.

The point of my note is the following. The executive director of the Upper Midwest Automated Clearing House Association is quoted as saying, "The Fed was concerned because it was running blind. They really didn't want the marketplace to know that they were in disaster recovery ... and susceptible to fraud." The Federal Reserve Bank's chief financial officer said there's no evidence that anybody tried to rip off any banks electronically ... "Our systems were not compromised; the security was there and valid."

It sounds to me like there definitely was a window of vulnerability and that no-one knows in fact if it was exploited. (The cash management officer for a large Minneapolis bank is quoted as saying "We had ... some large dollar transactions, say $200,000, that were lost for up to 10 days.... When you've got items in the hopper [and] you haven't had time to back it up, they get lost.")

[Maybe that is what is meant by a Grace Hopper? PGN]

Changing class grades in Alaska

"Dean Gottehrer" <FFDMG@ALASKA.BITNET>
Sun, 05 May 91 18:37:23 -0900

As a university professor I wondered about the RISK of some programmer changing a student's grades on the computer. I never hear much about it ever happening until the following story appeared in the local papers:

FAIRBANKS -- The University of Alaska Fairbanks has fired a computer specialist accused of using his access to electronically change a student's grades. Robert Concannon, 38, has pleaded not guilty to the felony tampering charge and is scheduled to go to trial in July. He faces up to five years in jail and a $50,000 fine if convicted of the class-C felony.

University officials say the incident has not affected the integrity of the University of Alaska system. "This was a highly isolated incident that was dealt with very quickly," said David Leone, head of the statewide computer network.

Concannon, a database specialist at the university's statewide computer center was fired after a series of audits confirmed a suspicion in the admission's office that UAF student Colleen Gallagher's grades were changed last fall. University spokeswoman Debra Damron said the audits and an independent consultant discovered that Concannon, one of a staff of five, had access to the information. He is accused of changing Gallagher's grades of two "F's" and a "D" to two "A's" and a "C."

[Have others heard of similar cases around the country? Are the penalties

as stiff as the ones here in Alaska? Are they actually applied?
Dean Gottehrer, Anchorage, Alaska]

[Perhaps Concannon might now use his skills to
upgrade his class-C felony to a class-A felony? PGN]

On Tulips, Hacking, and Tequila

"Herman J. Woltring" <UGDIST@nici.kun.nl>
Sat, 4 May 91 23:59 MET

RE: Hacking, Civil, and Criminal Law -- Reply to
--- J. Giles (USA) <RISKS 11(60)>
--- Hugh Cartwright (UK) <RISKS 11(61)>

Both posters seem to overlook the difference between civil and criminal law: the former only requires a balance of evidence, with the court quite passive, the latter requires clear evidence that highly specific acts, defined in the law books as criminal, have been committed, with the court quite active in asserting whether the law, indeed, has been broken. It is one thing to have private litigation between parties, where the court will take a decision by (freely) interpreting the evidence put to it, it is something quite different if the whole Nation is out to fine, jail, hang, or electrocute you.

In essence, most postings on this list make generalisations and comparisons which are typical of civil law; comparisons abound of physical trespassing or breaking & entering with unauthorised access to insufficiently secure information systems (no passwords, known system passwords, or simplistic passwords). At this time, various countries including mine have not decided yet to what extent computer trespassing should be declared a criminal offence. Therefore, the choice is not, in the words of my UK neighbour,

> The law has to take a stance. It can protect the interests of legitimate
> users, by making unauthorized access illegal. Or it can protect unautho-
> rized users by making it legal.

but to decide whether the latter should be declared a criminal offence since it is currently not -- while it may be unlawful under civil law, depending on the parties' arguments in front of a rather passive judge.

The decision involves policy matters of a wider scope than just the alleged criminality of the behaviour in question: is it `opportune' to widen the scope of so-called criminal acts? To what extent is civil law capable of handling these problems? Is hacking by external intruders really so serious as suggested in the (electronic) press? What about internal `theft' within institutions and organisations -- is this much more serious? Should society as a whole (because of the tax-payer's funding of the public prosecutor's office) bear the burden for some private interests OR public institutions who are too lazy to guard their own doorstep? These are some of the questions posed or implied in the Preliminary Comments from the Standing Committee on the Judiciary in the Dutch House of Representatives with respect to Bill 21551 (26 Nov 1990).

I may have been slightly obscure in my Dagobert Duck example; DD is certainly liable in civil law for solliciting criminal behaviour (in all likelihood, his insurance will not pay his damages), and I should think that too blatantly flaunting one's richness might even be sufficiently antisocial to qualify as `criminal' -- the kind of behaviour that causes revolutions.

Mr Giles' example of the lady who enters a singles' bar is inappropriate: it is a public place for which different rules exists -- unless DD's behaviour should be interpreted as turning his vaults into such a public place ... But even in a public place, you may have to pay for services rendered or products provided.

I submit that criminal law is not the equivalent of John Wayne riding into your village and protecting your peaceful and law-abiding community from the nasty crowd that has been invading you from Mexico or The Netherlands. Don't cry for a Strong Man who will wipe out your troubles with a six-gun, but make sure that you take appropriate measures to guard your own doorstep. However, do so with commensurate means, rather than by solliciting crime through overkill: there are too many guns on the street already. If you succeed in convincing your legislators that computer trespassing is tantamount to highjacking a plane -- fine, but do realise the consequences when somebody quite by mistake lands up in the wrong account or tries to find back his own, accidentally deleted data.

I believe that computer users deserve adequate protection under the law, not that `unauthorised' users deserve more protection than `authorised' users. At present, authorisation exists by default under some countries' criminal law, and the question is simply to what extent this authorisation should be withdrawn.

The problem reminds me of the current struggle on software copyright. A new right is about to be born, namely the exclusion of Fair Dealing under British Copyright Law which has entitled you up to now to study and review a software package in object code by decompiling or disassembling it in order to find out about its functional properties -- whether this information is to be used for publishing a critical review in a journal or for making a competing, and hopefully better, software package. The European Communities are in the process of accepting a Directive on Software Protection in which such activities are declared illegal as regards the central core of a software package. Interface aspects may be analysed confidentially, and software `maintenance' may be performed by or on behalf of `legitimate' users.

While the proposed Directive claims that the `central ideas etc.' will remain free and unprotected, and quite appropriately so under the Copyright Doctrine, you may not obtain those ideas from the package unless you are licensed to do so. The proposed Directive curtails former `Fair Use / Fair Dealing' rights substantially. For example, how could Shakespeare lawfully determine under such a system whether indeed his (way of making) thunder had been stolen ... in other words, can patent infringement be legitimally assessed under this new protection scheme, or do we need Anton Pillar orders for that? If so, how do we collect the evidence to convince the judge that such an order is appropriate?

I am not saying that hacking is fair, but I do claim that the criminalising

responses on this Forum are incompatible with the extent of its (un)fairness. Alas, there are no simple solutions, and that's why my reply has become so lengthy.

Herman J. Woltring, Eindhoven/NL

Fences, bodyguards, and security (of old O/S)

"351M::ESTELL" <estell%351m.decnet@scfb.nwc.navy.mil>
6 May 91 07:51:00 PDT

Mike is right about better security ON THE HOST. No quarrel there. And Rick is right about "no magic bullets." I assume - wrongly? - that those who install systems try to use them right. Rick's cautious approach is safer, perhaps because it's pessimistic.

However, the issue I addressed was an "old O/S" where some of the several operational definitions of "old" include (a) poor security in partucular, and (b) little or no networking in general; e.g., UNIVAC's O/S 1100 c. 1980. (A far cry from the 1991 version, which I understand is B2 now, thanks to some pioneering work by TMP Lee et al.)

Clearly, those who, like UniSys get on the ball and improve, reap multiple benefits. However, for that "crucial application" running on an old host with old O/S, a "guard gate" is better than no protection.

To pursue my physical world analogy, should the next President wear a bullet proof vest, a visored helmet, carry a .357 Magnum, and be a martial arts expert? Or can we still rely on the Secret Service?

Broader and deeper views of the problem suggest NO ONE SOLUTION is adequate; i.e., for "classified work" a network should comprise ONLY "multi-level secure" operating systems (i.e., A1 rated by DoDCSC). Today, that is not possible - unless one uses the "guard gate" idea. Moreover, EVEN IF all modern O/S were A1 by say the year 2000, I doubt that DoD, NSA et al, would grant network access to those hosts that run secret work. No problem, in a way; i.e., some of those secure hosts have no desire whatsoever to "offer resources" to the network; BUT they do need to exchange information with colleagues far away - which today they do via US registered mail, bonded courier, etc. instead of encrypted e-mail, for example. There is no reason why today such secret hosts could not use "encrypted e-mail" by following the "guard gate" scheme, complete with approved encryption devices at appropriate points; e.g., use software encryption for the files, on the host; then use a "KG" device to bulk encrypt that data as it passes from the host to the network server; then use STU-III phones to connect to a remote site; all these devices and processes to reside "in the vault" except of course for the "long lines" connecting the two STU-III phones. Yes that is s-l-o-w but it is also secure, and much faster than the US mail and courier alternatives. The fact that such transmissions cannot be direct (host to host) does not mean that they cannot occur. The guard gate scheme makes a layered, but unbroken connection possible: Users must consciously login to remote e-mail hosts; but that is better than no e-mail, etc.

Bob

crackers: passwords & "holes" vs locks & combinations

Leonard Erickson <70524.2603@compuserve.com>
03 May 91 02:22:03 EDT

I agree with Richard O'Keefe's comments in RISKS 11.58. Several of the "well known" holes are exactly equivalent to "well known" "holes" with locks. For example, a certain major brand of bicycle lock can be picked with a piece of bent wire in approximately 5 seconds (as I once demonstrated to an employer who was going to use one to secure some valuable items!)

Likewise, many OS's have equally bad shortcomings in their security IF YOU ARE KNOWLEDGABLE. The user should only have limited responsibility for OS "holes". Especially since, as many have noted, there may be nothing they can do about it. If (for example) you are running a TRS-80 Model 1, you *cannot* fix the holes in it's OS, it would cost more than the entire system is worth. And if you are using such an old item, you either are broke, or have a *very* compelling reason.

On the other hand, you had better not be counting on it being secure. Ignorance *may* be forgivable the first time. After that, you have no excuse for continuing to keep valuables in an "unsafe" environment.

Default passwords and accounts are a bit different. The user *can* change those. Just as when you buy a briefcase with a combo lock, you either change the combo from the factory default, or you accept responsibility for any unauthorized access.

Note, however, that just because I haven't changed the combination on my briefcase (and thus have some responsibility for any resulting losses), that in no way affects the underlying fact that it is wrong to attempt to open my locked briefcase without permission! Unauthorized use of a password is no different from unauthorized use of a combination. The password may be stupid, but you *still* have no business messing with the lock!

Your curiousity regarding the contents of my briefcase, or even merely as to whether I've changed the combo, does *not* give you the right to try and find out. Likewise, a cracker's curiousity doesn't give him the right to go where he isn't wanted.

Fly-by-Wire Glitch (11.55 - Joseph Nathan Hall)

A. Padgett Peterson 407-356-6384 <padgett%tccslr.dnet@uvs1.orl.mmc.com>
Wed, 1 May 91 08:15:54 -0400

This comment on the Northrop YF-23 "early generation flight-control software" glitch was somewhat humourous since over a decade ago we faced the same problems on the AFTI-F16 program, a multiple-redundant full-authority digital system. As Mr. Hall suggested, we used the simple expedient of a weight-on-

wheels switch to control such things. It will be interesting to see when Northrop starts "pushing the envelope" if they will rediscover some other "interesting" anomalies we ran into in the "earliest generation".

Padgett

EFFector Online 1.04

Chris Davis <ckd@eff.org>
Wed, 1 May 91 21:33:03 -0400

```
**********************************************************
**********************************************************
***       EFFector Online #1.04  (May 1, 1991)       ***
***             (Formerly EFF News)              ***
***      The Electronic Frontier Foundation, Inc.      ***
***           Net address: eff@eff.org           ***
**********************************************************
**********************************************************
```

Editors: Gerard Van der Leun (gerard@eff.org)
Mike Godwin (mnemonic@eff.org)

E-mail subscription requests: eff-request@eff.org
Editorial submissions: eff@eff.org

AND NOW THE NEWS

The following press release was Faxcast to over 1,500 media organizations and interested parties this afternoon:

EXTENDING THE CONSTITUTION TO AMERICAN CYBERSPACE:

TO ESTABLISH CONSTITUTIONAL PROTECTION FOR ELECTRONIC MEDIA AND TO OBTAIN REDRESS FOR AN UNLAWFUL SEARCH, SEIZURE, AND PRIOR RESTRAINT ON PUBLICATION, STEVE JACKSON GAMES AND THE ELECTRONIC FRONTIER FOUNDATION TODAY FILED A CIVIL SUIT AGAINST THE UNITED STATES SECRET SERVICE AND OTHERS.

On March 1, 1990, the United States Secret Service nearly destroyed Steve Jackson Games (SJG), an award-winning publishing business in Austin, Texas.

In an early morning raid with an unlawful and unconstitutional warrant, agents of the Secret Service conducted a search of the SJG office. When they left they took a manuscript being prepared for publication, private electronic mail, and several computers, including the hardware and software of the SJG Computer Bulletin Board System. Yet Jackson and his business were not only innocent of any crime, but never suspects in the first place. The raid had been staged on the unfounded suspicion that somewhere in Jackson's office there

"might be" a document compromising the security of the 911 telephone system.

In the months that followed, Jackson saw the business he had built up over many years dragged to the edge of bankruptcy. SJG was a successful and prestigious publisher of books and other materials used in adventure role-playing games. Jackson also operated a computer bulletin board system (BBS) to communicate with his customers and writers and obtain feedback and suggestions on new gaming ideas. The bulletin board was also the repository of private electronic mail belonging to several of its users. This private mail was seized in the raid. Despite repeated requests for the return of his manuscripts and equipment, the Secret Service has refused to comply fully.

Today, more than a year after that raid, The Electronic Frontier Foundation, acting with SJG owner Steve Jackson, has filed a precedent setting civil suit against the United States Secret Service, Secret Service Agents Timothy Foley and Barbara Golden, Assistant United States Attorney William Cook, and Henry Kluepfel.

"This is the most important case brought to date," said EFF general counsel Mike Godwin, "to vindicate the Constitutional rights of the users of computer-based communications technology. It will establish the Constitutional dimension of electronic expression. It also will be one of the first cases that invokes the Electronic Communications and Privacy Act as a shield and not as a sword -- an act that guarantees users of this digital medium the same privacy protections enjoyed by those who use the telephone and the U.S. Mail."

Commenting on the overall role of the Electronic Frontier Foundation in this case and other matters, EFFs president Mitch Kapor said, "We have been acting as an organization interested in defending the wrongly accused. But the Electronic Frontier Foundation is also going to be active in establishing broader principles. We begin with this case, where the issues are clear. But behind this specific action, the EFF also believes that it is vital that government, private entities, and individuals who have violated the Constitutional rights of individuals be held accountable for their actions. We also hope this case will help demystify the world of computer users to the general public and inform them about the potential of computer communities."

Representing Steve Jackson and The Electronic Frontier Foundation in this suit is James George,Jr. of Graves, Dougherty, Hearon & Moody of Austin, Rabinowitz, Boudin, Standard, Krinsky & Liberman of New York,and Harvey A. Silverglate and Sharon L. Beckman of Silverglate & Good of Boston .

Copies of the complaint, the unlawful search warrant, statements by Steve Jackson and the Electronic Frontier Foundation, a legal fact sheet and other pertinent materials are available by request from the EFF.

@+@+@+@+@+@+@+@+@+@+@+@+@+@+@+@+@+@

Also made available to members of the press and electronic media on request were the following statements by Mitchell Kapor and a legal fact sheet prepared by Sharon Beckman and Harvey Silverglate of Silverglate & Good, the law firm central to the filing of this lawsuit.

WHY THE ELECTRONIC FRONTIER FOUNDATION IS BRINGING SUIT ON BEHALF OF STEVE JACKSON.

With this case, the Electronic Frontier Foundation begins a new phase

of affirmative legal action. We intend to fight for broad Constitutional protection for operators and users of computer bulletin boards.

It is essential to establish the principle that computer bulletin boards and computer conferencing systems are entitled to the same First Amendment rights enjoyed by other media. It is also critical to establish that operators of bulletin boards JQJ whether individuals or businesses JQJ are not subject to unconstitutional, overbroad searches and seizures of any of the contents of their systems, including electronic mail.

The Electronic Frontier Foundation also believes that it is vital to hold government, private entities, and individuals who have violated the Constitutional rights of others accountable for their actions.

Mitchell Kapor,
President, The Electronic Frontier Foundation

@+@+@+@+@+@+@+@+@+@+@+@+@+@+@+@+@+@+@

LEGAL FACT SHEET: STEVE JACKSON GAMES V. UNITED STATES SECRET SERVICE, ET AL.

This lawsuit seeks to vindicate the rights of a small, successful entrepreneur/publisher to conduct its entirely lawful business, free of unjustified governmental interference. It is also the goal of this litigation to firmly establish the principle that lawful activities carried out with the aid of computer technology, including computer communications and publishing, are entitled to the same constitutional protections that have long been accorded to the print medium. Computers and modems, no less than printing presses, typewriters, the mail, and telephones -being the methods selected by Americans to communicate with one another -- are all protected by our constitutional rights.

Factual Background and Parties:

Steve Jackson, of Austin, Texas, is a successful small businessman. His company, Steve Jackson Games, is an award- winning publisher of adventure games and related books and magazines. In addition to its books and magazines, SJG operates an electronic bulletin board system (the Illuminati BBS) for its customers and for others interested in adventure games and related literary genres.

Also named as plaintiffs are various users of the Illuminati BBS. The professional interests of these users range from writing to computer technology.

Although neither Jackson nor his company were suspected of any criminal activity, the company was rendered a near fatal blow on March 1, 1990, when agents of the United States Secret Service, aided by other law enforcement officials, raided its office, seizing computer equipment necessary to the operation of its publishing business. The government seized the Illuminati BBS

and all of the communications stored on it, including private electronic mail, shutting down the BBS for over a month. The Secret Service also seized publications protected by the First Amendment, including drafts of the about-to-be-released role playing game book GURPS Cyberpunk. The publication of the book was substantially delayed while SJG employees rewrote it from older drafts. This fantasy game book, which one agent preposterously called "a handbook for computer crime," has since sold over 16,000 copies and been nominated for a prestigious game industry award. No evidence of criminal activity was found.

The warrant application, which remained sealed at the government's request for seven months, reveals that the agents were investigating an employee of the company whom they believed to be engaged in activity they found questionable at his home and on his own time. The warrant application further reveals not only that the Secret Service had no reason to think any evidence of criminal activity would be found at SJG, but also that the government omitted telling the Magistrate who issued the warrant that SJG was a publisher and that the contemplated raid would cause a prior restraint on constitutionally protected speech, publication, and association.

The defendants in this case are the United States Secret Service and the individuals who, by planning and carrying out this grossly illegal search and seizure, abused the power conferred upon them by the federal government. Those individuals include Assistant United States Attorney William J. Cook, Secret Service Agents Timothy M. Foley and Barbara Golden, as well Henry M. Kluepfel of Bellcore, who actively participated in the unlawful activities as an agent of the federal government.

These defendants are the same individuals and entities responsible for the prosecution last year of electronic publisher Craig Neidorf. The government in that case charged that Neidorf's publication of materials concerning the enhanced 911 system constituted interstate transportation of stolen property. The prosecution was resolved in Neidorf's favor in July of 1990 when Neidorf demonstrated that materials he published were generally available to the public.

Legal Significance:

This case is about the constitutional and statutory rights of publishers who conduct their activities in electronic media rather than in the traditional print and hard copy media, as well as the rights of individuals and companies that use computer technology to communicate as well as to conduct personal and business affairs generally.

The government's wholly unjustified raid on SJG, and seizure of its books, magazines, and BBS, violated clearly established statutory and constitutional law, including:

. The Privacy Protection Act of 1980, which generally prohibits the government from searching the offices of publishers for work product and other documents, including materials that are electronically stored;

. The First Amendment to the U. S. Constitution, which guarantees freedom of speech, of the press and of association, and which prohibits the government from censoring publications, whether in printed or electronic media.

. The Fourth Amendment, which prohibits unreasonable governmental searches and seizures, including both general searches and searches conducted without probable cause to believe that specific evidence of criminal activity will be found at the location searched.

. The Electronic Communications Privacy Act and the Federal Wiretap statute, which together prohibit the government from seizing electronic communications without justification and proper authorization.

####

For more information, contact Gerard Van der Leun at 617-864-1550.

END OF EFFECTOR ONLINE 1.04

Search RISKS using swish-e

Report problems with the web pages to the maintainer

Search RISKS using swish-e

THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

ACM Committee on Computers and Public Policy, Peter G. Neumann, moderator

Volume 11: Issue 63

Wednesday 8 May 1991

Contents

Validation and Verification Issues for KB Systems

Paul Tazzyman <paul@pandc.rta.oz.au>
Wed, 08 May 91 16:13:22 +1000

This article follows on from the more general discussion earlier this year about validation and verification of knowledge. This discussion has tended to discuss the technical aspects of V&V whereas the question we are faced with relates to the legal defendability of decisions reached as a result of applying

an expert system to a problem and the establishment, in legal terms, of the "expertness" of the knowledge base. In cases where the knowledge is used in a system which is subject to public scrutiny, and consequently subject to scrutiny by the courts when the eventual output of KB systems is implemented, the heuristics may be challenged by other "experts".

The issue that this raises is "how is the source of the knowledge used by a KB system given expert status by a court charged with hearing legal challenges to decisions based on the KB system". Under most legal systems the "expert" must satisfy the court that they are in fact suitably qualified in the topic. In the case of a KB system the heuristics may be the result of many "experts" input to the system and therefore there is no single "expert" who can be produced to give expert evidence.

This implies that the knowledge gathering process must first establish, and document, the sources of the knowledge and be able to establish, in sufficient clarity for the courts, the development of the KB system's rulebase.

Presumably the courts have reasonably well established guidelines for the admission of "expert" witnesses and the qualification of such witnesses.

How is a witness given "expert" status and how must the documentation of the knowledge acquisition phase of an expert system be undertaken in order to allow the system to withstand legal challenge to the decisions based on its inferences. Obviously differences between the legal systems in the US and Australia will produce differing opinion, but because of the infant nature of the technology, from the legal aspect, any decision will be cited as a precedent.

A discussion of these issues within this forum will help us, and no doubt other organisations, establish more correct procedures.

Shaun Gray shaung@xwdev.rta.pandc.oz.au paul@xwdev.rta.pandc.oz.au
Roads and Traffic Authority of NSW, Information Services Branch
3rd Floor, 260 Elizabeth Street, SURRY HILLS. NSW. Australia 2010

Disclosure of customer information (AT&T)

Lauren Weinstein <lauren@vortex.com>
Mon, 6 May 91 12:40:56 PDT

[Also sent to TELECOM]

Like others reading the TELECOM digest, I was amazed to see the recent message where an AT&T Communications employee apparently used his access to customer data to conduct a "private" investigation of a "contest/telemarketing" operation, then published the "results" via TELECOM.

Immediately after seeing his original message, I sent the author private email asking for an explanation. Of particular interest to me was whether he was acting in violation of AT&T confidentiality rules, or whether the rules would have permitted such actions.

I received a reply back from him today. In essence, he says that he made a mistake in making the information public, and that AT&T rules do *not* permit such disclosures from customer data. He also says that some of what he said in that message was obtained directly from a conversation with the telemarketer.

In any case, it is obvious from his original message that he did access the customer records of the firm in question, and did obtain information regarding long distance calling patterns and telephone number usage information from those records. However obnoxious some may feel the firm to be, their telecom records are still deserving of the same security and confidentiality we all (should!) expect, and should not be subject to "private" investigations and disclosures outside of official channels.

This is unfortunately symptomatic of the growing range of situations where the data collected on individuals and organizations in the course of their normal business is available to too many persons without authorization or "need to know". The amount of information that can be obtained with essentially no security controls, or often at the best semi-useless, pseudo-controls such as social security number, is vast and growing.

In the telecommunications arena, the problem has grown greatly with the breakup of the Bell System--it seems like customer telephone data is floating around almost freely between the local telcos and the private long distance carriers these days. But the same sorts of problems exist in many other areas of our lives, and only seem to be getting worse, not better.

I believe that the time has come for another look at the Privacy Act in terms of how it does, or does not, protect consumer (both individual and business) information and who (both inside and outside of the firms collecting the data) has access to that information. I believe that meaningful, uniform minimum standards must be established for automated systems that allow consumers to access various account balances or similar data by telephone. The excuses of the firms providing these systems that it would be "too difficult for consumers" to remember a passcode or even know their account number (i.e. the ongoing Sprint account information case) must be treated as the unacceptable responses that they are.

Consumers need protection both from the employees of the firms who maintain the data (whether or not such employees act with malicious intent is not the issue) and from outside persons who can gain access to such data through the often non-existent security of these systems.

Many of the companies involved state that they are providing all of the security required by law. OK then--if they don't feel a need to go beyond the current law to a meaningful level of protection, the time has come to improve the laws to take into account the realities of the information age. And there isn't a moment to lose.

--Lauren--

Quirk in British Computer Privacy Laws

Unix Guru-in-Training <elr%trintex@uunet.UU.NET>
Tue, 7 May 91 15:27:34 EDT

- Quote without comment from The Economist, May 4-10:

"Computers and Privacy -- The eye of the beholder"

...A common feature of privacy law is that governments tend to treat information held on a computer as fundamentally different from that held on paper. ...But technology is making the distinction less and less tenable--with, for example, devices that can scan text from a printed page straight into a computer. ...Because British law lets individuals look at computerised information that others may hold about them, British journalists turn from their computer terminals to typewriter and paper when they write obituaries of elderly (but not yet deceased) public figures. When the subject is no longer in a position to demand his right to freedom of information, the obituary is then put into the computer for publication.

Ed Ravin philabs!trintex!elr

Smart alecks vs. the census computer

Les Earnest <les@dec-lite.stanford.edu>
Tue, 7 May 91 19:53:23 -0700

A news report indicates that an increasing number of Americans are thumbing their noses at the Federal government's mindless insistence on classifying everyone into traditional ethnic categories ["Census menu contained lots of spice," San Jose Mercury News, 5/7/91, p. 1A]. The feds are reportedly fighting back with advanced computer technology.

Several years ago I pointed out in this forum that no one had yet devised a scheme that would reliably and unambiguously assign each individual to a particular racial or ethnic category. Those postings were later developed into an article arguing that all statistical studies of racial or ethnic categories and the governmental programs based on them, especially Affirmative Action, rest upon unstable foundations ["Can computers cope with human races?" CACM, Feb. 1989]. I advocated answering questions about one's ethnicity with "mongrel" and a number of people later told me that they had used that answer or similar ones in the 1990 Federal census.

Today's news story says that the Census Bureau received many answers such as "a little bit Norwegian," "a little bit of everything," "California boy," "Heinz 57," "a fine blend," and "steak sauce." They somehow decided that most of these responses came from people of Hispanic descent, according to Roderick Harrison, chief of the Race Statistics Branch of the Census Bureau. Other answers included "child of God," "none of your business," "NOYB," and "NOYFB."

The article goes on to say:

"This year, for the first time, spiffy new technology enabled the census to decipher each and every write-in answer to the race

question. (In 1980, only a small sample was read.) The census computer was able to sort and assign about 85 percent of those `unique responses' to a racial group."

This is truly a remarkable claim: apparently the computer has somehow figured out not only how to classify individuals into ethnic classes, but how to do it even when they give ambiguous or misleading answers. If this claim holds up under scrutiny, I will nominate it as the first example of true artifical intelligence.

The article goes on to mention that there are limits to its classification abilities:

"But the computer could not match about 200,000 quirky, smart-aleck and just plain weird answers such as `golden child,' `extraterrestial,' `alien,' `exotic hybrid,' `exchange student,' `half and half,' `fat pig,' `father adopted, race unknown,' `all of the above,' `handicapped,' and `exquisite.'"

Despite these limitations, it appears that the Census Bureau is well ahead of the rest of the world in computer science. ;-)

Les Earnest UUCP: . . . decwrl!cs.Stanford.edu!Les
12769 Dianne Dr. Los Altos Hills, CA 94022 Phone: 415 941-3984

UK Interim Defence Standard 00-55

Martyn Thomas <mct@praxis.co.uk>
Wed, 8 May 91 18:11:44 BST

UK Defence Standards 00-55 (Procurement of safety-critical software) and 00-56 (hazard analysis) have been reissued as Interim Standards by the UK MoD. They have been revised, and are no longer *draft* interim standards. They will be used in procurement at the discretion of individual project managers until enough experience of their efficacy has been gained; then they will be revised as necessary and issued as full standards.

I have only skimmed 00-55 as yet, but it seems to have come out of revision improved. The requirement for formality throughout development is still there (strengthened somewhat, it seemed to me), but contentious issues such as the list of proscribed practices (assembler, recursion, floating-point ...) has been revised and removed to a separate "guidance" section, outside the normative part of the standard.

Copies of the standards may be obtained, free of charge, by writing to:

Director of Standardisation, STAN 1, Kentigern House, 65 Brown Street
Glasgow G2 8EX Scotland

..... and *not* to me!

Martyn Thomas, Praxis plc, 20 Manvers Street, Bath BA1 1PX UK.
Tel: +44-225-444700. Email: mct@praxis.co.uk

Patriot vs Scud

<Mark_Jackson.wbst147@xerox.com>
Wed, 8 May 1991 04:34:58 PDT

Can't follow up quickly as they don't carry /Army Times/ in our Technical Information Center. . .

Date: 7 May 91 22:42:35 GMT
From: bcstec!shuksan!major@uunet.UU.NET (Mike Schmitt)
Subject: Patriot vs Scud
Keywords: Software glitch
Organization: The Boeing Co., MMST, Seattle, Wa.
Extracted-from: sci.military Digest V7 #19

According to the latest issue of 'Army Times' the Scud that struck the barracks and killed 28 soldiers was not detected by the Patriot missile battery guarding the area. It was described as "a glitch in the internal working of the system."

The fault was contained in a very complex problem-solving portion of the system's software. The incoming Scud was picked up internally by the battery's computers, but was 'never filtered through the computational process,' and therefore never showed up on the screen.

Once the fault was traced, it was "a simple fix." The Scud was intact on impact, and had not broken up as it descended.

mike schmitt

Some views about the debate sparked by Dutch Hackers story

"Olivier M.J. Crepin-Leblond" <UMEEB37@vaxa.cc.imperial.ac.uk>
Tue, 7 May 91 19:00 BST

I'd like to put forward a few views about the debate concerning the Utrecht Hackers, computer security, etc.: (Note that I have not included any name on purpose: I don't want to flame *anyone* in particular. Indeed, RISKS is not the place for flames - keep that in mind)

1. Someone suggested locking the Utrecht site out of the Internet. vThis is nonsence. Take a similar example: if such a problem had happened using the UK's NSFNet-relay, would you lock it out ? You would be locking out most of the UK's academic users of Internet. And this just because of one hacking incident. (Note here that I am *not* saying that hacking is okay)

2. What level of security: Why is it always a NASA (apologies for mentioning a name - no hard feelings), or military, or US government site which gets hacked ? Why isn't it an undergraduate university computer facility site, or the computer system of an obscure company manufacturing shoes ? (note: I have nothing against shoe-makers)
Possible answers:
either... 1. only break-ins at NASA sites are reported in the press

or... 2. NASA sites seem more attractive to hackers
Hence: isn't it time that one starts setting security standards for "important" sites ? I'm amazed at the fact that logging in a US government computer is following the same procedure as if logging into a local workstation on campus here. Physically speaking, US government computers are protected by perimeter fences, guards, systems of personal I.D., etc. etc. etc. (I've never looked at this any further than I do today). Here, one can come during the day, in broad daylight, and with a bit of luck, be able to switch-off the computer systems by turning the key on the front panel. In the case of the Utrecht hackers, Why is there so much security to reach the computer physically, and so little to reach it virtually ? Follow the open-door policy described later (in 5) and you might as well open your perimeter fences, classified areas, and generally the path leading to your computer room.

3. Someone suggested that some systems could only run their specilaised software on old operating systems. Well, why are they connected to Internet then ? FTP ? Mail ? Wouldn't it be more appropriate to use a more recent machine/Operating System (OS) for FTP and Mail ? There are quantities of machines using an old OS in the world, running specialised software, not connected to any outside network, and hence never hacked !

4. Passwords: assuming there is no bug in the OS, the hacker must use a valid user password. Why not use 2 passwords at "risky" sites ? Indeed, why not use a hard token (to be plugged into a terminal) or make some accounts only reachable from specified terminals ? Why not record any unusual access failure ? Indeed, do Systems managers ever read these log files of failures ?

5. Somneone compared a hack of a computer account with the trespassing of a property which had an opoen door. Well, to answer this idea in the same stupid way:
"If the door is open, if there is no sign showing -NO TRESPASSING- and the doormat says -Welcome-, that I enter, get arrested by the police for trespassing, I can always plead not guilty, because I IGNORED (ie: DID NOT KNOW) that I was not allowed there and was breaking the law."

In short: 1. if there's a convincing warning notice at (or before) login, and an unauthorised user is caught, then YES, PROSECUTE !
2. if NO NOTICE, but just a "welcome" message, then NO, I'm not buying the idea of prosecution.

Olivier M.J. Crepin-Leblond, Communications research student,
Electrical Engineering Dept., Imperial College of Science, UK.

Re: Gary Marx Comments at the Computers, Freedom and Privacy

Sanford Sherizen <0003965782@mcimail.com>
Tue, 7 May 91 20:39 GMT

Conference About Kids Holding Phone up to TV

Since there were so many postings about Gary Marx's comments at the San

Francisco Conference and he is a friend, I faxed him in Belgium and told him that he was on the RISKS wanted list. I asked him about the source for his comments.

He recalls that the example about kids being told to hold up the phone to the tv set was cited in a Congressional hearing and he thinks it was for a candy company. Unfortunately, his documentation is not with him while he is in Belgium.

He's certainly someone who has a lot to contribute to our understanding of technological fallout issues. For those who haven't read his most recent book, it is worth reading UNDERCOVER: POLICE SURVEILLANCE IN AMERICA (U. of California Press, 1988). It is an objective analysis of policing dilemmas and, even though not its major focus, a primer on how to frame some of the central arguments about cyberspace and law abiding policing.

Sanford Sherizen, Data Security Systems, Inc., Natick, MA 01760 USA
MCI MAIL: SSHERIZEN (396-5782) PHONE: (508) 655-9888

Update on S.618

<gnu@toad.com>
Mon, 06 May 91 12:27:19 -0700

I phoned the Senate about S.618, the "Violent Crime Control Act of 1991". Guess who sponsored it? Our dear friend Senator Biden again. You can call his Judiciary Committee staff at +1 202 224 5225 to receive copies of the bill.

The esteemed Senator seems a lot more interested in controlling privacy than in controlling violent crime or terrorism -- since he seems to be seizing on any excuse he thinks the public will swallow to do it.

John Gilmore

Re: Fences, bodyguards, and security (of old O/S) (Estell, RISKS-11.62)

Rick Smith <smith@SCTC.COM>
Tue, 7 May 91 12:09:04 CDT

Bob Estell writes:

>To pursue my physical world analogy, should the next President wear a
>bullet proof vest, a visored helmet, carry a .357 Magnum, and be a
>martial arts expert? Or can we still rely on the Secret Service?

>From what I understand, the President wears a bulletproof vest for public appearances. At least, Reagan did after his earlier experience.

Anyway, physical world analogies don't always work when thinking about computer security. The Vault and platoon of guards represent classic physical security. The Trojan Horse is the classic threat in computer security, and you don't have a serious threat of that kind in most

physical security situations.

Maybe the Trojan Horse program is a computer virus, or maybe it's just some sneaky code that the author hid in your text editor. What it does is make secret copies of your most secret files, putting them where a spy can reach them. This easily bypasses "classical" OS security, since *you* run the text editor, giving it access to *your* files. The implications in a network environment are staggering.

>From what I understand, our technology for producing physical "bugs" just doesn't compare; we still trail James Bond (and even the Man from UNCLE) by decades. On the other hand, hardly any routine computer users would be able to tell the difference between "bugged" or even virus infested software and trustworthy software. Software is too opaque, and does things that you can't really observe.

Rick Smith, SCTC, Arden Hills, Minnesota.

... old O/S

<TMPLee@DOCKMASTER.NCSC.MIL>
Tue, 7 May 91 12:38 EDT

In RISKS-11.62 Bob Estell wrote "UNIVAC's O/S 1100 ... which I understand is B2 now ... thanks to ... TMP Lee et al."

Although I will take some small credit for security enhancements to the Univac/Sperry/Unisys OS 1100, but only a very small credit, I must point out that the system has only a B1 rating, alas. Although it was only superficially looked at, I think it is fair to say that doing what needed to be done to reach B2 was not in the cards. I've not kept close touch recently, but even if I had it would be improper for me to comment on or speculate on what might be happening now.

Ted

Re: The new California Drivers License

Alan Nishioka <atn@cory.Berkeley.EDU>
Tue, 7 May 91 13:41:10 -0700

I thought I would send this in since I first heard about the new California license on comp.risks and I also just looked up the back issues there.

I just got my new California driver's license. No, I'm not 17, but I take the bus a lot.

It has a holographic plastic laminate of "DMV" and the California Seal.

My color picture was digitized into and IBM computer as was my thumb print and my signature. The mag stripe on the back has three tracks.

Just for fun, I thought I'd try to read it. I had previously been able to read bank cards (with help from sci.electronics). I found that the information encoded is basically just what is printed on the card. Kinda uninteresting. Of course I couldn't figure out what little extra information was encoded.... (marked unidentified below)

It took me a little while to figure out the format, and I suppose it is documented somewhere (anyone know where?) but it was fun.

Bank Cards -- conform to ANSI/ISO 7810-1985 ($10)
Track 1: 6 bit word with 1 bit parity. LSB first.
code offset 32 below ASCII code.
Track 2: 4 bit word with 1 bit parity. LSB first. Numbers only.

Driver's License --
Track 1: 6 bit word with no parity. Otherwise same as Bank Card.
Track 2: Same as Bank Card.
Track 3: ?

California Driver's License:

Track 2: (low density)
8 unidentified digits
License Number
Separator
Expiration Date (YYMM)
Separator
Date of Birth (YYYYMMDD)

Track 1: (High density)
DALAN TAKEO NISHIOKA $
974 TULARE AVE ALBANY
Name
Address
City

Track 3: (High density. Can't reposition read head.)

It looks like there is space for a 58 character name (since someone was worried earlier), a 29 character address and a 13 character city.

I suspect the third track contains the rest of the information from the front of the license.

Alan Nishioka KC6KHV atn@cory.berkeley.edu ...!ucbvax!cory!atn
974 Tulare Avenue, Albany CA 94707-2540 37'52N/122'15W +1 415 526 1818

Search RISKS using swish-e

THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

ACM Committee on Computers and Public Policy, Peter G. Neumann, moderator

Volume 11: Issue 64

Wednesday 8 May 1991

Contents

Cable Zapping

<sullivan@poincare.geom.umn.edu>
Wed, 8 May 91 13:08:50 CDT

An earlier RISKS had excerpts from an April 25 NYTimes article about American Cablevision 'zapping' chips inside illegal cable hookups. Not included were quotes at the end of the article from some customers who claimed they had only regular cable service, but had been zapped anyway. I don't know the laws

governing cable service, but it would disturb me if, say, the phone company started sending destructive signals down the phone lines. Perhaps, though, you're allowed only to connect the cable company's own equipment to your cable. Otherwise, the cable company sounds just as bad as Prodigy.

I basically feel I have a right to sense my environment.
Though the common disregard for speeding laws is disgraceful, I believe radar detectors must be legal. I am bothered by claims that decoding satellite TV signals is illegal: though of course I could not resell copyrighted programming, if someone broadcasts radiation at me, and I'm clever enough to decode it, that should be allowed. Cable TV is different, though, since I have signed an agreement with the cable company to get a hookup.

John Sullivan, Geometry Center sullivan@geom.umn.edu

Fences, trojan horses, and security

"351M::ESTELL" <estell%351m.decnet@scfb.nwc.navy.mil>
8 May 91 14:28:00 PDT

Just yesterday, I saw a video tape "movie" (docudrama?) offered by the NIS (Naval Investigative Service) on "human intelligence." (It is "security and safety awareness week here.)

The points I'd like to pass on, in reply to Rick Smith's posting about "trojan horses" are: (1) NIS still believes that "trojan horses" are a SERIOUS threat to government RDT&E labs; i.e., "moles" as well as employees who are angry, frustrated, broke, greedy, or stupid. The FBI, et al agree with this opinion. (2) One reason that the threat is NOT more serious (i.e., that the damage is usually limited) is that we've made serious efforts to reduce the risks.

Yes, it is hard to spot a trojan horse (or virus, etc.) in a software package. It is also hard to spot a spy in a crowd. For the last several years, they have abandoned wearing trench coats, carrying daggers and magnifying glass, and speaking in obvious accents. True, the physical analogy is limited; every analogy is. (That's true by definition of "analogy.") But the typical computer security person still has things to learn from it.

Bob

More on Almost Humorous Fly-by-Wire Glitch (RISKS-11.61)

Mary Shafer <shafer@skipper.dfrf.nasa.gov>
Mon, 29 Apr 91 20:10:10 PDT

Joseph Nathan Hall (jnh@eceugs.ece.ncsu.edu) writes:

> From the pages of Popular Science, April 1991:
>
> "...Spectators at the first flight of Northrop's [YF-23] prototype noticed its huge all-moving tails--each larger than a small

> fighter's wing--quivering like butterfly wings as the airplane
> taxied out to the runway. Test pilot [Paul] Metz says this
> occurred because the early generation flight-control software
> didn't include instructions to ignore motions in the airframe
> caused by pavement bumps. The answer, he adds, is inserting lines
> of computer code that tell the system not to try to correct for
> conditions sensed when the fighter's full weight is on its nose gear."

Talk about a pack of slow learners. I remember sitting in the control room watching the AFTI/F-16 waving its canards and tail at every expansion joint in the taxiway. They finally stopped it with a squat switch. But I shouldn't criticize the YF-23 team too much, because the X-29 didn't have one originally, either.

> I'll grant that in the 1990s we can analyze wind-tunnel tests in a
> few hours (or less) and can even simulate untested airframes with
> some success. In the 1950s pilots frequently flew prototypes
> before the final results of early wind-tunnel tests were completely
> analyzed--a process that sometimes took weeks or months. But am I
> alone in thinking that in some respects it takes more chutzpah to
> test-fly one of these modern fly-by-wire wonders?

Old cases of Telco tieup and grade hacking

George Malits <malits@apache.sw.stratus.com>
Mon, 6 May 91 18:19:25 EDT

1) on the topic of a computer failure at the fed reserve, RISKS-11.62.
Consider this. In the mid 70's sometime, a disgruntled x-employee of the phone company started a number of wastepaper basket fires in various telco facilities. He got lucky at Irving place and destroyed a switching facility. A goodly chunk of Manhattan was without phone service for several MONTHS. What would the effect have been if he had chosen a different facility? Like one that serviced Wall St?

Let me tell you what I remember. The year would be in the 74-76 range and the facility attacked was the telco building on Irving place in Manhattan (around 15th and second). In any case, it was quite the fire and the switch was rendered scrap. What we (the telephone dialing public) found out was that these switches are normally custom built and ordered years in advance. The solution was to ship whatever switch was under construction to Manhattan and "make it fit". This also involved shipping the people building the switch to Manhattan so that they could continue to build the second half while other tech's were installing the first half. Meanwhile, no phones. Small business men were using CB to communicate with friends/family outside of the affected area who would then relay the call. Telco set up banks of microwave link phone booths at certain street corners but....In any case, the key limiting factor turned out to be the space available in the cable lockers in the basement. They were so cramped that only one or two techs could work at a time. Also, it was so hot down there that they worked REAL SHORT shifts. Their progress was of course a hot topic in the news. I remember that there was some key piece of diagnostic equipment (?) and that something like 3 of the 5 units in the US were in use in Manhattan. I don't have any good references for further

details (I read about it in the Daily News at the time) but it was quite a big tadoo so I suspect that it would have been covered in some journal or other.

2) Computer hacking of grades, RISKS-11.62. Back at Columbia, in the mid 70's, several prof's kept a list of the various test grades on line. This was a completely "unofficial" set of grades for their own use. We discovered it and, from looking around the directory a little, figured out that they were computing "the curve" from this file and thus assigning final grades for the class. After MUCH discussion, we decided that the way to turn this to our advantage was to either add non-existent students who did very poorly on all of the tests or to lower the grades of real students that we didn't know/like. The idea was to lower the curve but leave our own grades unaltered (no smoking gun). In the end, we whimped out but I did add one line to the file that said "do you know how tempted I was to change this file". I figured I'd give the prof something to think about.

Re: Changing class grades (RISKS-11.62)

Adam Engst <ace@tidbits.UUCP>
Mon, May 6, 1991 7:24:42 PM

> Concannon, a database specialist at the university's statewide computer

Does anyone have any more information about this case? It strikes me as a little odd that this guy would have changed a random student's grades so radically. It seems more likely that there was some collusion present between Concannon and the student, at which point the management sorts might want to think about the why and how such collusion, if indeed present, became possible. No mention is made of what happened to the student, if anything, which would clear up my question slightly. Somehow I doubt that database people are recompensed handsomely enough in general to prevent the occasional incident of bribery in whatever form.

Just curious ... Adam Engst, TidBITS Editor

TMPLee: 9th Federal Reserve Bank Drowned

Brinton Cooper <abc@BRL.MIL>
Wed, 8 May 91 17:52:12 EDT

TMPLee@DOCKMASTER.NCSC.MIL reports

"On Monday April 8 the computer center at the Minneapolis Federal Reserve Bank was flooded out of commission by a broken air-conditioning cooling water pipe in the ceiling. [I'll ignore the RISKs of such a design; the point of this note is something else.]"

Let's not ignore this and similar risks. In an effort to minimize the risks to the environment, we are strongly urged not to use Halon to extinguish computer room fires. This puts us back to sprinkler (water) systems. The advantage to Halon was that it was unlikely to do secondary damage to the installation;

water has no such feature.

Now what? _Brint

[To stave off discussion on halon itself, let me point out to new RISKSers that we have had numerous discussions in RISKS in the past:
RISKS-5.28
Halon (Dave Platt, Steve Conklin, Jack Ostroff, LT Scott Norton, Scott Preece)
RISKS-6.79
Risks of Halon to the environment vs. risks of other fire protection (Dave Cornutt)
RISKS-6.87
Halon environmental impact citation (Anita Gould)
RISKS-6.89
Halon environmental impact citation (Jeffrey R Kell)
RISKS-7.03
Halon (Romain Kang)
RISKS-7.04
Halon agreement and the ozone models (Rob Horn)

Just in case you really want to get gassed on this subject. PGN.]

Denise Caruso reports on new anti-encryption bill: S.618

John Gilmore <gnu@toad.com>
Mon, 6 May 91 11:54:15 PDT

Denise Caruso wrote a great piece for her "Inside Technology" column of the Sunday, 5 May 1991, SF Examiner, on page E-14. It concerns the attempts to outlaw encryption and why that is a bad idea. She claims that there is a second bill that has had anti-encryption stuff quietly slipped into it last week by the FBI: S.618, "The Violent Crime Control Act of 1991".

I'll quote her closing paragraph to encourage you to get and read it all:

"I want crime to stop. I want terrorism to stop. But do we want to secure the networks or not? I have *never* seen evidence that power in the hands of government authority didn't corrupt. I have never heard of a compromise-able network that didn't get compromised. With increasing reliance on computer-based networks, back doors for law enforcement (or whoever else figures it out) make me afraid. I don't think they're a good idea."

S.618 via FTP & mail server, instead of flooding Washington

Brendan Kehoe <brendan@cs.widener.edu>
Wed, 8 May 91 14:39:26 -0400

Senate bill S.618 is available via anonymous FTP from:
ftp.cs.widener.edu [192.55.239.132]

in the file
pub/cud/law/bill.s.618
as part of the Computer Underground Digest archives.
It's about 227k, so please try to do it after 5pm EDT.

Hopefully this will save the taxpayers a few dollars.

Brendan Kehoe - Widener Sun Network Manager - brendan@cs.widener.edu
Widener University in Chester, PA A Bloody Sun-Dec War Zone

NYTimes article on E.F.F and John Barlow

<*sullivan@poincare.geom.umn.edu*>
Wed, 8 May 91 13:20:49 CDT

The New York Times Magazine, April 21, 1991, had an article "In Defense of Hackers" by Craig Bromberg. The article is based substantially on discussions with John Barlow (founder of EFF), pictured as an "electronic cowboy". The cases discussed (including rtm, Craig Neidorf's 911 memo, and Steve Jackson Games) are familiar to risks readers, but it is nice to see a well-reasoned discussion in the mainstream press.

John Sullivan, Geometry Center sullivan@geom.umn.edu

Re: Disclosure of customer information (AT&T)

<*smb@ulysses.att.com*>
Wed, 08 May 91 15:28:13 EDT

Lauren relates a story of someone posting confidential information based on internal AT&T data. So what?

As noted, misuse of such data is already against the rules. It is quite likely that the individual will be disciplined, possibly even fired. I don't see that there would have been any greater protection if a Federal law were involved. If someone chooses to act unethically, rules, at whatever level, won't stop them.

Talking about inadequate technical protection of data doesn't wash in this case. I haven't seen any evidence that the employee in question wasn't authorized to retrieve that data -- maybe that person did have legitimate access to that database. This is not a situation where an outsider called up, and was able to bluff or hack a way in.

Ultimately, security rests on people. The most sophisticated technical means in the world provide no protection against a suitably-placed, suitably-skilled, dishonest person. Organizations that care about security know this, of course; critical objects (large sums of money, missile launch systems, etc.) are protected by at least two individuals. But for routine access, it would be crippling to the organization to do that, and I don't think that that's fixable.

--Steve Bellovin

Customer Info Disclosure (AT&T)

Lauren Weinstein <lauren@vortex.com>
Wed, 8 May 91 13:31:33 PDT

I think Steve may have partially misinterpreted the thrust of my recent message. In no way did I mean to imply that a "technical" problem was at the heart of the recent AT&T customer information disclosure. In this particular case, it is clear that a "people" (and possibly a policy) failure occurred. Whether or not the employee in question had a legitimate "need to know" the information in question, and so whether or not he *should* have had access to the data, are important questions, however.

The reason I brought up the related issues of automated account interrogation systems and the like is that information privacy is based on the triad of policies, people, and technology. No one element stands alone. The current lack of adquate standards relating to all of these areas is resulting in far too much information being passed around, both within and between organizations, without adequate controls. Failure or inadequacy of elements in any leg of the triad can have significant negative results as far as the end effects are concerned.

A key point that technologists need to be concerned about is that the available technology may result in policy and people failures that are much more far-reaching than might have occurred without the speed and finality that these systems allow. One obvious example among the multitude: A single "people" error in a credit entry, propagated through credit bureau databases through lack of adequate policy controls and checks, can cause an individual incredible hassles--or much worse.

More and more, the transactions of our lives are being viewed as the raw data of targeted marketing. The telcos and long distance carriers would like to market calling pattern data to businesses who would use that information to "target" customers of interest. The credit card companies use customer buying information to cross-promote other merchandise through outside firms. Even if you view these particular cases as relatively "innocuous" (though I would disagree with you!) these are but the tip of the iceberg.

The issues related to customer information collection and the subsequent access to, marketing of, and use of that data for purposes that the customers might not even imagine, need to be addressed as broadly as possible. Attempting to deal with them purely from the standpoint of one or two legs of the triad won't work. The policies, the people, and the technology must all be considered, and where appropriate, minimum standards for the handling and control of this information must be mandated by law.

As others have pointed out, it starts to look more and more like the proverbial Big Brother won't necessarily be a government entity (at least in this country). Rather, it might be Big Brother, Inc.

--Lauren--

The means justify the ends? (piracy probe)

<henry@zoo.toronto.edu>
Sun, 5 May 91 00:45:37 EDT

> The evidence was obtained by a consultant employed by DEC at attend
> a Syntellect training course in February. He copied it's system
> software which was later examined by DEC. [...]
>
>... Surely the consultant ... didn't ask for permission to copy their
>system? In which case, is the evidence not inadmissable by virtue of
>being gained by illegal means?

What law has been broken? That wasn't *their* software. You don't own the licensed software running on your system; if you inspect the license agreements carefully, you will find that the authors retain ownership, and you have bought only the right to use it. You are usually required to protect it from unauthorized copying, but copying done by the owner's representative, with or without your knowledge, hardly qualifies.

Henry Spencer at U of Toronto Zoology utzoo!henry

Search RISKS using swish-e

THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

ACM Committee on Computers and Public Policy, Peter G. Neumann, moderator

Volume 11: Issue 65

Friday 10 May 1991

Contents

RISKS Backlog

"Peter G. Neumann" <neumann@csl.sri.com>
Fri, 10 May 91 10:34:38 PDT

Well, I don't know what combination of circumstances caused it, but recently there have been hundreds of messages pending in the queueueueueueueue that I had either flagged for consideration or in a few cases not even read, on ATMs, cashless gas pumps, red and green clocks, electronic cash, automated highways, droids, self-parking cars, SSNs, Dutch crackers, one-time passwords, credit cards, etc., all of which appear to be further iterations on previous iterations on iterations ... . I trust you will bear with me for arbitrarily cutting them off. The RISKS mailbox had become enormous (hovering around 500 undeleted messages), and because MM apparently REWRITES the whole file on the drop of a hat, that consumes ghastly amounts of waiting time and makes reading mail somewhat unpleasant. Sometimes mail comes in faster than MM can handle it and prevents me from even reading for minutes on end -- even with a SPARCstation! So, it was time. Thanks to all of you who responded so

diligently on those subjects and went for so long without hearing about might have happened to your contributions. If you feel your contribution would still be valuable and timely, please revise and resubmit. And thanks to all of you who have expressed appreciation for my being such an effective filter so that YOU don't have to filter through all of the third- and fourth-order interstitiations! But the no-pass filter is too antisocial, so I hope we can return to a more even flow. PGN

Draft International Standard on the safety of industrial machines

Martyn Thomas <mct@praxis.co.uk>
Fri, 10 May 91 11:33:12 BST

IEC TC4 WG3 has developed a draft international standard on electrical equipment of industrial machines [sic]. This is being extended to cover professional, leisure and domestic use of machines - so it could have very wide significance. I quote some comments on the use of software, from the latest draft (April 1991).[henceforth, my comments are in [], all else is text from the draft standard]

12.3.4 software verification

Equipment using reprogrammable logic shall have means for verifying that the software is in accordance with the relevant program documentation.

12.3.5 Use in safety-related functions

Programmable electronic equipment shall not be used for category 0 emergency stop functions ... [this is where stopping is achieved by immediate removal of power to the machine actuators - each machine *must* be so equipped].

For category 1 emergency stop functions [where power is available to the actuators to achieve the stop, and is then removed] and all other safety-related stopping functions, the use of hardwired electromechanical components is preferred .....

These requirements shall not preclude the use of programmable electronic equipment for monitoring, testing, or backing-up such functions but this equipment shall not prevent the correct operation of these functions.

NOTE: It is believed at present that it is difficult, if not impossible, to determine with any degree of certainty in situations when a significant hazard can occur due to the maloperation of the control system, that reliance on correct operation of a single channel of programmable electronic equipment can be assured. Until such time that this situation can be resolved, [!!] it is inadvisable to rely on the correct operation of such a single channel device.

[So that is the perceived state of the art in standards: the problem is the software, (no mention of complexity being the root issue), and multiple channels are seen to solve the problem (although the sections on redundancy and diversity make no reference to software, so no guidance is given on

their relative benefits). 12.3.1 says that the IEC 65A standards shall be followed, which may help, but I find it very depressing that our technology should be so apparently immature that new standards cannot find a way to define where and how it may be used.]

[Exercise for the reader: compare and contrast the approach of this standard with UK Def Stans 00-55 and 00-56.]

Martyn Thomas, Praxis plc, 20 Manvers Street, Bath BA1 1PX UK.
Tel: +44-225-444700. Email: mct@praxis.co.uk]

Netware 286 Trojan Problem

John Graham-Cumming <John.Graham-Cumming@prg.oxford.ac.uk>
8 Mar 91 20:49:08 GMT

I'm managing (at least for the moment) a Novell network running Netware 286.

I've recently realised that it is possible to pipe a file into the LOGIN command. This has the rather unfortunate affect that it is possible to write a Trojan horse which simulates login (it was quite easy in GW-BASIC plus a batch file on my system) which does not need to print the almost standard "Access denied." type message when pretending that a user has incorrectly typed his password; it doesn't need to pretend at all as it is possible to write a program that steals the password and performs a successful login. This makes the Trojan horse very hard to detect.

Has anyone else had a similar problem with piping and LOGIN? Any simple solutions?

John Graham-Cumming, Oxford University Computing Laboratory,
Programming Research Group, 8 - 11 Keble Road, Oxford UK

Big Brother in the air

Andrew Koenig <ark@europa.att.com>
Wed, 8 May 91 23:54:21 EDT

The May 1, 1991 issue of The Aviation Consumer (a newsletter for pilots and airplane owners published by Belvoir Publications in Greenwich, Connecticut) has a remarkable article about transponders in general aviation aircraft.

Airplanes, especially little ones, are mediocre radar reflectors because they're so far away from the radar transmitter and have lots of smooth curves. To make them easy to track, people install transponders. A transponder contains a receiver that picks up a radar pulse from the ground and a transmitter that blasts out a much stronger pulse in response. It also sends out twelve bits of data that the pilot can set by twiddling four knobs to select octal digits. This is called a "squawk code" and is a way of ensuring positive identification by ATC. When a pilot first calls a controller on the radio, the controller usually responds with something like "squawk 1776," which is a request for the pilot to set 1776 into the transponder dials. Presumably

no other aircraft in the area is squawking 1776 (you're supposed to squawk 1200 if not talking to ATC), so the ATC radar can unambiguously track that particular airplane. Indeed, transponders are required in high- volume airspace.

What the Aviation Consumer article says is that some pilots have found that their transponders have been modified so that they continue to operate even when turned off. Moreover, when in that state, they squawk a particular code unrelated to what's in their dials. Further research revealed that the modifications were made by US Customs agents as part of the "war on drugs." The idea is that they the Customs agents find airplanes that they think are likely to be used for drug smuggling and then modify those airplanes' transponders to make the airplanes easier to track. In particular, if the pilot flies the airplane with the transponder switched off, the magic squawk code sets off all kinds of alarm bells in the ATC office.

They were unable to find out whether these clandestine transponder modifications were pursuant to court orders, or whether Customs was just targeting, say, a randomly selected population of Cessna 210 aircraft in southern Florida.

[One interest to RISKS that might not be obvious is its close philosophical connection to the current debate about trapdoors in encryption systems.]

"Bugs" (was Re: Fences, bodyguards, and security)

William Ricker <wdr@wang.com>
Thu, 9 May 91 13:26:58 EDT

"We" /qua/ NATO may trail Fleming's Q's department. However, the erstwhile DDR had a very high-tech bug factor, which is one of the few eastern German factors successfully converting to the world market, I hear. The secret police's bug factory looked at its capabilities (so the radio reports (BBC? Christian Science Monitor? NPR? I forget) say) when unification came and decided to go into the hearing aid business, since their miniaturization technology, previously classified, beat anything the West's hearing-aid businesses had -- so they had some chance of maintaining their salaries & volume. Given some of the really small things already on the US market in hearing aids, if they really had *those* beat, their bugs *would* have been comparable to Bond.

I haven't heard if they made a go of it.

/s/ Bill Ricker wdr@wang.wang.com

Now which train am I part of?

Mark Brader <msb@sq.com>
Thu, 9 May 1991 23:43:00 -0400

[I am forwarding this exchange to Risks; I don't have permission to identify the original writers. The second writer drives trains for a major North

American railway -- Mark Brader]

> The coal unit trains that operate around here (Cleveland OH) use
> radio controlled mid-train helpers. When it's working right, the
> radio control keeps everything in synch. When it's not, it makes
> quite an interesting mess, viz. Rockport yard a year or two ago -
> something went askew, and the helpers kept on doing their thing when
> they shouldn'ta! Ground through the ball of the rail, among other things...

When Locotrol I was first introduced to [railway], the system required a code number on the head-end to match the receiver on the slaves. The code number was any number chosen by the shop staff (that was the theory anyway). One day, a coal train was in the siding somewhere near [place in mountains]. He was sitting there, luckily, with a full train brake set. As it happened, someone had picked the same code number on two sets of remote equipment, and the guy approaching the siding was in Throttle 8 climbing a hill. The slaves on the guy in the siding picked up the Throttle 8 signal and tried to push the train out of the siding! They eventually (after grinding a few moons in the rail) got an overspeed and shut down... long day for the crew on that one...

Where justice is done ...

"Herman J. Woltring" <UGDIST@nici.kun.nl>
Fri, 10 May 91 18:14 MET

The recent commotion on the Dutch crackers/hackers might have been placed in a better context at the outset if the following News Analysis in the Dutch daily "NRC Handelsblad" of 23 April 1991 would have been quoted. It was written by Frank Kuitenbrouwer, standing legal commentator with that journal and (former) visiting professor of Law at Utrecht University, The Netherlands [and included here with his knowledge].

Under the heading "Computer Crime Bill gives the Justice Department too much elbow room", Mr Kuitenbrouwer wrote as follows [in Dutch -- the translation is my responsibility -- HJW]:

Amsterdam, 23 April. Are The Netherlands lagging behind in the fight against computer crime? This suggestion was made in an article in the New York Times daily of last weekend where the alarm-bell chimed about Dutch "hackers" (i.e., crackers of computer systems) who allegedly had burglarized American Defense systems by remote entry from the university system SURFnet ["Samenwerkende Universitaire Reken Faciliteiten" -- Cooperating University Computation Facilities, a private foundation with central offices in Utrecht, albeit not at Utrecht University -- HJW]. This contemporary student exercise featured on Dutch TV a few months ago without causing too much commotion. "You see?", the Americans must think, "computer crime in The Netherlands is handled in the same way as drugs", but that is -- like the situation with drugs -- too simple a form of reasoning.

Indeed, Dutch Law is silent on the item of "computer peace disturbance", while Germany, France, and recently also the U.K. have introduced new provisions in their penal codes. However, these were rather incidental adjustments of the Penal Code, while The Netherlands are working on a Total

Program to guide the Dutch Penal Code into the digital era by one move, including new authorizations for the police and for the Department of Justice. The relevant Bill is already under consideration in Parliament, including a proposal to declare Computer Cracking a criminal offence.

Whether such a special rule will have much effect is another matter. Many years ago a student at the former Twente University of Technology [now a full University in the North-East of The Netherlands -- HJW] explained man's irrepressible tendency to browse around in each other's computer homework in terms of "the instinct that leads man to play Mastermind". In 1987, an American criminologist, Erdwin H. Pfuhl from Arizona State University, qualified the 46 computer crime laws effectuated between 1975 and 1985 in the U.S.A. as "symbolic legislation". This was no exaggeration: by 1987, not a single prosecution had been initiated on the basis of the new provisions. However, Pfuhl found 58 criminal cases on computer misuse based on existing rules such as forgery. Also in The Netherlands, this has proven possible.

Pfuhl mentioned some interesting reasons for this lack of impact of the Penal Code:

-- Incidentalness: Computer misuse continues to be a rather rare event; curiosity battles with disapproval for priority.

-- Positive image of the perpetrators. The term "Rust effect" is sometimes used (after the young German sports aviator who outwitted Russian Air Defense); the serious nature of the reproach is tempered by appreciation for the stunt. Actually, many a serious informatician started out as a hacker: "Experience as a hacker is a valuable asset on a CV", according to the Dutch computer journal Computable.

-- The victims are usually institutions and thus don't strongly appeal to one's imagination. Besides, although most publicity is directed to the hackers, it would appear that most computer misuse originates from within by far, from one's own organisation or enterprise. In this way, all computer misuse is brought within the gray zone of white-collar crime and of the concomitant company cultures.

-- The element of play. Already the Dutch author Johan Huizinga taught in his "Homo Ludens" [the Playing Man (1938); Huizinga was a historian and professor, first in Groningen and later in Leyden -- HJW] that playing has no moral function: it resides *outside* the conventional antitheses: wise or stupid, true or false, good or bad. (Government) automatization a game? Indeed, one representative spoke about "young branches of sports" during the parliamentary deliberations of 15 February 1986. Progress in automatization is often said to depend on unconventional solutions, on prospecting border lines, including normative ones.

-- Own fault. Lack of elementary precautions in the systems under attack. Last year, the German Accounting Office investigated an army computer facility. On the roof, an antenna was found that led to the basement, but nobody could explain the thing's purpose. Even though unauthorised access was duly logged by the system, those signals were swamped in more than 1000 reports per 24 hours, according to system personnel.

The Netherlands wish to make penalization of computer peace disturbance dependent on the requirement of a "clear threshold"; this offense can only lead to a conviction if the attacked system is secure [cf. "Computers at Risk -- Safe Computing in the Information Age", US National Research Council, National Academy Press, Washington DC 1991, ISBN 0-309-04388-3 -- HJW]. Thus, the ball is bounced back in the case of the attacked American computers. Is this not again one of those typical Dutch idiosyncracies? Not at all: back in 1985, the Federal Republic of Germany included the requirement of "special security" in

its penalization of computer peace disturbance. In that country, the relativity of the computer crime provisions became most obvious in the case of the three hackers who "by order of the KGB" [the quotes are mine -- HJW] had burglarized into American networks. Early 1990 they were convicted to conditional punishments only [cf. Clifford Stoll's "Stalking the Wily Hacker", Comm. of the ACM 31(5), 484-497, May 1988, reprinted in Dunlop & Kling, "Computerization and Controversy -- Value Conflicts and Social Choices, AP 1991 -- HJW]. The judge did not even consider computer peace disturbance and confined himself to third-rate espionage only. Even in the U.S.A., Robert Morris -- who virtually brought a large research network to a stand-still in November 1988 because of of a virus prank that went out of control -- got off with a conditional punishment.

Precisely because of the symbolic nature of many computer crime laws, there is rather much reason to fear that the ambitious way the matter is tackled in The Netherlands may be worse than the problem. Certainly, the investigatory authorizations for the authorities go much further than, e.g., the recommendations of the Council of Europe. There is a real danger that these authorizations will be used by the Justice Department for some extensive fishing in the electronic data processing pond [this alarm was already rung on 20 May 1988 in the same journal by Richard de Mulder, professor of criminal law at Erasmus University in Rotterdam, chairperson of the task force on computer crime of the Netherlands Society for Computers and Law -- HJW]. Such fishing does not have to be confined to direct misuse of information technology but could concern anything that the Justice Department finds interesting. Even the most spectacular computer hack threatens to pale before the fishing expeditions made possible under the Dutch Computer Crime Bill.

I might add that the latter point becomes particularly striking with the recent RISKS posting on allegedly illegitimate house searches and impoundings by the USA's Secret Service, even more so as the Dutch Bill provides the gouvernment with extensive rights to protect its own secrets. At a previous occasion, I intimated that those provisions remind more of the U.K.'s Official Secrets Acts (where everything is secret unless officially released, with official `D-notices' sent to editors etc. if something has leaked out) than of the USA's Freedom of Information Act pursuant to its First Amendment under the Bill of Rights,

> Congress shall make no law respecting an establishment of religion, or prohibiting the free exercise thereof; or abridging the freedom of speech or of the press; or the right of the people peaceably to assemble and to petition the Government for a redress of grievances (Art. 1).

In my mind, `freedom of speech and of the press' presupposes equitable access to relevant information: without such access, this freedom becomes an empty shell.

While I am not an admirer of some ways that things are run in North America (where I used to live for two years, with one daughter born there who now has dual citizenship), I find this provision particularly appealing. Fortunately, the constitutions of both countries provide sufficient leeway to partake in the legislative debate before the gouvernment goes fully out of control. However,

denouncing the authorities as `the bad guys' should not diminish concern for other, less public invaders of our electronic privacy!

Going back to the networking situation, there are a few datasets on (im)proper rules of conduct; those who are interested in scanning those, may wish to send the following line to NETSERV@BITNIC.BITNET in New York:

GET CONDUCT CODE

For more commercially oriented rules, you might send the following three lines to LISTSERV@BITNIC.BITNET:

GET LEGAL COMMERCE
GET LEGAL GTDA
GET LEGAL COUNSEL

In particular, the LEGAL COMMERCE file from the US Department of Commerce states that remote computer access in BITNET is possible for file transfer only (using commands like the above GET filename filetype), but not for remote login. Thus, hacking on BITNET seems possible only for those files that have not been protected against remote retrieval, similar to ftp on the Internet. I am not certain about the EARN situation, but SURFnet certainly provides the possibility for remote login via telnet etc., both nationally and internationally, leaving it to the individual nodes' discretion to inhibit this feature locally, either in general or from specific sources. This, in my mind, is the proper approach; however, some care my be necessary in the long run to prevent hackers from outsmarting the protection schemes. Otherwise, one may become exposed to similar tricks as have been succesful for free long-distance calls on the telephone system.

Herman J. Woltring, Eindhoven/NL

Search RISKS using swish-e

THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

ACM Committee on Computers and Public Policy, Peter G. Neumann, moderator

Volume 11: Issue 66

Monday 13 May 1991

Contents

"Children of the Computer" To Teach Our Children

"Jay Elinsky" <ELINSKY@YKTVMZ.BITNET>
Mon, 13 May 91 00:21:53 EDT

The Sunday, May 12 edition of the New York Daily News has the front-page headline "The Brain Drain -- City faces flood of novice teachers". One of the hopeful new teachers, who will replace old-timers lured out by a retirement incentive, is a 23-year-old student teacher in English, whose name and alma mater I will omit even though they're given in the article.

His cooperating teacher gives him high marks for energy and creativity. "[He] concedes, however, that spelling and grammar are not his strong suits, and that he is working hard not to repeat spelling mistakes such

as `hatrid', `envolved', or `increduluous' when he writes on the blackboard or in homework assignments. `I'm a child of the computer. I'm used to pushing 'spellcheck' and that corrects the words'". As I said above, he's a student teacher in English.

Jay Elinsky, IBM T.J. Watson Research Center, Yorktown Heights, NY

[Good speling and gramar arent everything but it shure helps. I include this item here to remind us that discipline can easily stifle creativity, but that creativity without discipline may be of very limited value. It clearly helps to have some discipline, energy, creativity, and perhaps even some intelligence! PGN]

Case of the Replicated Errors: An Internet Postmaster's Horror Story

"Erik E. Fair" (Your Friendly Postmaster) <fair@APPLE.COM>
Thu, 09 May 91 23:26:50 -0700

[Forwarded to RISKS by Jerry Leichter <leichter@lrw.com> and Jim Horning]

This Is The Network: The Apple Engineering Network.

The Apple Engineering Network has about 100 IP subnets, 224 AppleTalk zones, and over 600 AppleTalk networks. It stretches from Tokyo, Japan, to Paris, France, with half a dozen locations in the U.S., and 40 buildings in the Silicon Valley. It is interconnected with the Internet in three places: two in the Silicon Valley, and one in Boston. It supports almost 10,000 users every day.

When things go wrong with E-mail on this network, it's my problem.
My name is Fair. I carry a badge.

[insert theme from "Dragnet"]

The story you are about to read is true. The names have not been changed so as to finger the guilty.

It was early evening, on a Monday. I was working the swing shift out of Engineering Computer Operations under the command of Richard Herndon. I don't have a partner.

While I was reading my E-mail that evening, I noticed that the load average on apple.com, our VAX-8650, had climbed way out of its normal range to just over 72.

Upon investigation, I found that thousands of Internet hosts were trying to send us an error message. I also found 2,000+ copies of this error message already in our queue.

I immediately shut down the sendmail daemon which was offering SMTP service on our VAX.

I examined the error message, and reconstructed the following sequence of events:

We have a large community of users who use QuickMail, a popular macintosh based E-mail system from CE Software. In order to make it possible for these users to communicate with other users who have chosen to use other E-mail systems, ECO supports a QuickMail to Internet E-mail gateway. We use RFC822 Internet mail format, and RFC821 SMTP as our common intermediate E-mail standard, and we gateway everything that we can to that standard, to promote interoperability.

The gateway that we installed for this purpose is MAIL*LINK SMTP from Starnine Systems. This product is also known as GatorMail-Q from Cayman Systems. It does gateway duty for all of the 3,500 QuickMail users on the Apple Engineering Network.

Many of our users subscribe, from QuickMail, to Internet mailing lists which are delivered to them through this gateway. One such user, Mark E. Davis, is on the unicode@sun.com mailing list, to discuss some alternatives to ASCII with the other members of that list.

Sometime on Monday, he replied to a message that he recieved from the mailing list. He composed a one paragraph comment on the original message, and hit the "send" button.

Somewhere in the process of that reply, either QuickMail or MAIL*LINK SMTP mangled the "To:" field of the message.

The important part is that the "To:" field contained exactly one "<" character, without a matching ">" character. This minor point caused the massive devastation, because it interacted with a bug in sendmail.

Note that this syntax error in the "To:" field has nothing whatsoever to do with the actual recipient list, which is handled separately, and which, in this case, was perfectly correct.

The message made it out of the Apple Engineering Network, and over to Sun Microsystems, where it was exploded out to all the recipients of the unicode@sun.com mailing list.

Sendmail, arguably the standard SMTP daemon and mailer for UNIX, doesn't like "To:" fields which are constructed as described. What it does about this is the real problem: it sends an error message back to the sender of the message, AND delivers the original message onward to whatever specified destinations are listed in the recipient list.

This is deadly.

The effect was that every sendmail daemon on every host which touched the bad message sent an error message back to us about it. I have often dreaded the possibility that one day, every host on the Internet (all 400,000 of them) would try to send us a message, all at once.

On monday, we got a taste of what that must be like.

I don't know how many people are on the unicode@sun.com mailing list, but I've heard from Postmasters in Sweden, Japan, Korea, Australia, Britain, France, and all over the U.S. I speculate that the list has at least 200 recipients, and about 25% of them are actually UUCP sites that are MX'd on the Internet.

I destroyed about 4,000 copies of the error message in our queues here at Apple Computer.

After I turned off our SMTP daemon, our secondary MX sites got whacked. We have a secondary MX site so that when we're down, someone else will collect our mail in one place, and deliver it to us in an orderly fashion, rather than have every host which has a message for us jump on us the very second that we come back up.

Our secondary MX is the CSNET Relay (relay.cs.net and relay2.cs.net). They eventually destroyed over 11,000 copies of the error message in the queues on the two relay machines. Their postmistress was at wit's end when I spoke to her. She wanted to know what had hit her machines.

It seems that for every one machine that had successfully contacted apple.com and delivered a copy of that error message, there were three hosts which couldn't get ahold of apple.com because we were overloaded from all the mail, and so they contacted the CSNET Relay instead.

I also heard from CSNET that UUNET, a major MX site for many other hosts, had destroyed 2,000 copies of the error message. I presume that their modems were very busy delivering copies of the error message from outlying UUCP sites back to us at Apple Computer.

This instantiation of this problem has abated for the moment, but I'm still spending a lot of time answering E-mail queries from postmasters all over the world.

The next day, I replaced the current release of MAIL*LINK SMTP with a beta test version of their next release. It has not shown the header mangling bug, yet.

The final chapter of this horror story has yet to be written.

The versions of sendmail with this behavior are still out there on hundreds of thousands of computers, waiting for another chance to bury some unlucky site in error messages.

Are you next?

[insert theme from "The Twilight Zone"]

just the vax, ma'am,

Erik E. Fair apple!fair fair@apple.com

trojan pipe to login on 4.x bsd (Re: Graham-Cumming, RISKS-11.65)

Mark Seecof <marks@latimes.com>
Fri, 10 May 91 16:56:14 -0700

> >From: John Graham-Cumming <John.Graham-Cumming@prg.oxford.ac.uk>
> Has anyone else had a similar problem with piping and LOGIN?

On many Unix's with BSD features you can fool, not login, but 'su -' (simulate a login) which might "do the job" of of fooling the user (his utmp entry will be wrong). To accomplish this you must use the TIOCSTI ioctl in a clever way (I am reluctant to say more). I think that the getpass(3) routine could probably be modified to limit this attack by messing with the terminal's distinguished process group (TIOCSPGRP).

Mark Seecof, Publishing Systems Department, Los Angeles Times, Times-Mirror Square, Los Angeles, California 90053 213-237-5000

Emergency off switch - IBM 1620

Martin Ewing <ewing-martin@CS.YALE.EDU>
Sat, 11 May 1991 03:22:15 GMT

Remember all the risks we unknowingly took in our youth? Driving without seatbelts, using lawnmowers without automatic shutoffs, etc.? Well, there were computing risks like those, too. Recently wandering through the library stacks, I came across "Programming the IBM 1620" by Clarence B. Germain (Prentice-Hall, 1962). (The 1620 was a scientific machine with variable word length and 1-5 KIPS -- don't ask about SPECmarks.)

I was going over the control panel description when I came upon the following:

> Finally, we should mention the EMERGENCY OFF SWITCH... It removes all power from the machine instantly. Damage to the machine results from its use, and a customer engineer is required to turn the machine back on. Unless the computer is struck by lightning while you are using it, do NOT touch this switch; it is for emergency use only.

Men were men in those days, and giants strode the earth.

Martin Ewing, Yale University

Rude Behavior (Where justice is done, Woltring, RISKS-11.65)

<WHMurray@DOCKMASTER.NCSC.MIL>
Fri, 10 May 91 22:28 EDT

Not all rude behavior should be criminal. The Dutch have always tolerated behavior that other people have criminalized. Who are we to tell the Dutch

what level of rude behavior they should be prepared to tolerate?

>Thus, the ball is bounced back in the case of the attacked American
>computers.

Ah, there is the rub. The behavior of the Dutch students is not confined to their country. Are we prohibited from telling the Dutch what level of rude behavior we are prepared to tolerate?

Not only are the Dutch not prepared to call that behavior criminal, they do not appear to be inclined to label it rude. Not only are they not prepared to invoke criminal sanctions, so far they have refused to invoke social sanctions. While they contend that criminal sanctions are not warranted, they continue to fund the little rowdies. While they seem to object to being labelled a rogue nation, otherwise responsible citizens of that nation insist upon defending and justifying this behavior and trying to blame the victims. While they clearly have the option to confine this behavior within their own borders, they do not do so. What are the rest of us to do? Have we no choice but to provide the playpen for brats?

HJW's assertions to the contrary notwithstanding, this is not an issue of the security of American systems. While our systems may not be more secure than those in the Netherlands, they are no less so. Neither are they less secure than those in the rest of the internet. While our systems are the targets of these attacks, it is the systems in Europe, specifically including those in the Netherlands, that are paying the cost of attack. Our systems are the targets, but we are no more the victims than the rest of the internet.

Given the number of systems in the internet, the level of security is a given; it cannot change much in a short time. Given the law of large numbers, given a normal distribution of security in systems within the net, the net will always be vulnerable to this kind of attack.

"Computers at Risk," the report cited by HJW, would have you believe that the problem is one of the systems shipped by vendors. If vendors did a better job of design and chose safer defaults, the problem would be solved. Would God that that were so. It would be lovely to have to deal with only thousands of vendors instead of millions of users.

While good design and safe defaults may be necessary to security, they are not sufficient. Do any of you seriously believe that there is any security that a vendor can put into a system that users cannot compromise away? Do you believe that if a vendor could do so, that all of us his competitors would follow his lead? That no vendor could be successful selling performance and function at the expense of security, or that none of the systems that he sold on that basis could find their way into the net?

This is not simply an issue of the security of the systems within the net. The security of the net is, only in part, a function of the security of the systems in it, it is also influenced by other properties and behavior of those nodes. If you can believe the report, the Wily Hacker used the system of the Mitre Corporation as it was intended to be used. However, that intention so reduced the Wily Hacker's normal and expected cost of attack that it put the rest of net at risk. In taking his scientific/law-enforcement response to the attack,

Cliff Stoll put his neighbors at risk. Now, he was at least watching to be sure that the Wily Hacker was not too successful, but wouldn't you expect your neighbor to pull the plug on him?

Note that the security of a given system does not protect it. My system may be sufficiently resistant to outsiders to keep the Dutch students out. However, it does not keep them from using the adjacent system to attack me. The attack is a problem without regard to its success. It consumes some cycles, but it consumes an inordinate amount of communication capacity.

So, what are we to do? Assume that the Dutch students continue their rude behavior. Assume that their elders continue to fund them and smile tolerantly on the little hoodlums. Must we simply tolerate it? Have we no other open options? How long will we tolerate this abuse before we break the connection?

Now, I was not surprised at the response when I suggested this remedy last month. I expected that a community dependent upon connectivity would be reluctant to use that connectivity as a control mechanism. I was a little amused at the over-statement that was used to attack the idea.

I did not suggest that we ostracize Holland (Go back and read it if you must) though I did say that we should be prepared to do so. I did not even suggest that we permanently bar any systems from the net. It did not occur to me that anyone would think that the disconnections would need to be permanent or even of long duration. One of these days I will learn that if you leave room to be misconstrued, you can expect to be.

I only said that if you get rude traffic, break the connection to the system that it is coming from. Tell them why you have done so. If they are not the origin, invite them to follow your example. (Of course you can restore the connection as soon as the rude traffic stops.)

That is all I said to do. If everybody does that, the rude traffic will be isolated at its source. Now, the originators may continue to send the rude traffic, but I doubt it. If no system will listen, who will they send it to? Their elders may continue to fund "their experiments," but I doubt it. If we stop playing victim, the fun will go out of their playing bully.

I have to confess that I was surprised that some readers concluded that I advocated having data police and that I was nominating myself for the job. Let me make it clear. What I want is an orderly network that needs no policing. What I want is the kind of orderly well-behaved network that we have enjoyed for almost two decades. To the extent that there is any requirement for policing, what I am proposing is self-policing. What I am resisting is the idea that between what is illegal and what we can prevent, we must expect and tolerate everything else. What I am resisting is the idea that our only hope for order is to appeal to the authority of the law.

Finally, let me conclude with a regret. I regret that this has become a national issue. I particularly regret that the nation involved is the Netherlands. I hope they take no more offense at my rhetoric than is intended. If all the world were as civilized as the Netherlands, it would be a better place.

Nonetheless I am convinced that the rhetoric is indicated and I hope that it gets their attention. I am concerned that these otherwise most orderly of people appear not to understand that they are fostering mischief. I am concerned that they seem not to realize that they are setting in motion forces which they cannot control and inflicting damage on public order which may not be reversible.

William Hugh Murray, Executive Consultant, Information System Security
21 Locust Avenue, Suite 2D, New Canaan, Connecticut 06840 203 966 4769

Re: Where justice is done ... (Woltring, RISKS-11.65)

Richard A. O'Keefe <ok@goanna.cs.rmit.OZ.AU>
13 May 91 09:08:39 GMT

I'm sorry to keep this topic going, but I am rather distressed by this. People keep writing as if "unauthorised entry" were only a threat to big universities and Government sites, as if the only reason for a site to be vulnerable is negligence or incompetence. "It's easy, just put a B2 layer in between your net and the rest of the world!" "It's *just*, you only have to convince the court that your system was secure."

That's not my perspective. I'm worried about small organisations (as I said before, I have a particular charity in mind) for whom an 80386 running UNIX V.3 is a *large* expenditure, for whom buying an extra PC would be a financial hardship. These people could benefit a lot from being on the net. E-mail could save them a lot of money. Remote access could cut down on consultants' fees (no need to make a physical trip). There must be many thousands of small businesses in the same situation.

These people are vulnerable to "unauthorised entry" too. Why would anyone break into a system with no juicy data sets &c? Well, why do people spray graffiti all over the trains? Why do people try to burn down schools? Would anyone really break into a charity's computer and destroy files if they thought they could get away with it? YES!

Whatever "security" requirement is demanded of a victim before the courts will protect them should not be more than the victim could
(a) reasonably be expected to know about, not being a computer expert
(b) reasonably be expected to afford, bearing in mind the cost of the data and computer system.

Re: Quirk in British Computer Privacy Laws

paj <paj@gec-mrc.co.uk>
13 May 1991 10:16:03-BST

Ed Ravin <elr%trintex@uunet.UU.NET> quotes The Economist on the UK Data Protection Act, saying that in order to evade the right to personal information about you held on computer, reporters write anticipated obituaries on paper.

A far worse example was (possibly is) the university I attended. In those days it was University College Cardiff. It did not allow students to see their records, and held them on paper in order avoid having to do this. Processing was done by computer under a DPA clause which permits temporary storage for a limited time without having to have the data registered. Then the data was printed out and the magnetic media erased. The next time it was needed it was re-keyed. I found this to be a truly stunning way of doing things.

I also glanced through the report which preceded to the DPA. There was mention made of this issue. Many of the experts who gave evidence stressed that the distinction between computerised data and manually held data is an arbitrary one. The report noted that this was probably true but that the protection of paper files was outside their brief, so they could not consider it.

Hanlon's Razor: Never attribute to malice that which can be adequately explained by stupidity.

Paul Johnson +44 245 73331 paj@gec-mrc.co.uk

British Privacy Law (Ravin, RISKS-11.63)

<chaz_heritage.wgc1@rx.xerox.com>
Mon, 13 May 1991 04:28:00 PDT

> When the subject is no longer in a position to demand his right to freedom of information, the obituary is then put into the computer for publication.

This was not the reason why manually held records were excluded from the provisions of the Data Protection Act, 1984. British law does *not* 'let individuals look at computerised information that others may hold about them'. Perhaps Mr. Ravin should read the Act. His faith in British law is touching, but is quite misplaced.

Chaz

Re Quirk in British Privacy Laws

<jpff@maths.bath.ac.uk>
Mon, 13 May 91 15:28:07 BST

When we at the university were looking at the implications of the so-called Data Protection Act I was led to asking the questions about the use of scanners. We were concerned with the procesing of examination marks, and as we include second year results in out final examination we wondered if printing them and deleting the files, and then scanning would be OK. The opinion we got was that if you intend to re-enter the information then it still comes under the DPA. (The court case inquiring what I intended to do could have been interesting. :-))

However in the case of obituaries the situation is different. The DPA does not apply to information about dead people, as that is not personal.

An amusing sideline to this is we considered the holding of bibliographies, which were then searched, which would be personal data, and so we would have to register under the law. However if we sent the university hit squad round we could save the serious offence of holding unauthorised personal data, if at the expense of a murder or two.

==John ffitch

Re: Dagobert (NL) or Scrooge McDuck (UK/US) [RISKS-11.58]

"Herman J. Woltring" <UGDIST@nici.kun.nl>
Fri, 10 May 91 23:00 MET

When I referred to "Dagobert Duck" in my RISKS-11.58 posting, I did not realise that this personality is called Scrooge McDuck in Anglosaxon (and, I believe) American parlance. I trust that the identification was unambiguous by context!

Search RISKS using swish-e

THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

ACM Committee on Computers and Public Policy, Peter G. Neumann, moderator

Volume 11: Issue 67

Tuesday 14 May 1991

Contents

The UK Data Protection Act and email/net and university users

<reynolds@syd.dit.CSIRO.AU>
Tue, 14 May 1991 09:37:14 +1000

One of the problems of the UK Data Protection Act is that it is only concerned with the use of the data and not the contents. An author writing a biography is not covered by the Act because he is word-processing - but if he seachs the text ONCE for the occurrence of a personal name, or creates a name index, the Act immediately applies.

This applies to all UK users of email and usenet. If they just read their mail and discard it the Act does not apply. If they keep a copy of the text for later reference by name (or scan their mailbox to select mail) the Act applies. (If you have a personal name in a usenet kill file this could well be processing under the Act!)

The matter gets worse. If you have ANY data under the Act you have to register

(or be covered by an employers registration) with only a few exceptions. In addition the usenet postmaster acts as a bureau under the Act so that if any of his users process personal information from usenet he should register as a bureau....

Registration is a complex, time consuming and expensive process in which you have to detail the kinds of personal information you hold, where you get it from, and what you use it for. There are NO minimum levels. I produced some schools software, including a dozen teaching examples. One of these used a list of the English monarchs, and included the personal information that Queen Elizabeth II came to the throne in 1952. Technically speaking, whenever I sold a copy of the software to Hong Kong (or the Isle of Man!) I would need to be registered as an overseas dealer in personal information, and any UK school using the package should be careful not to reveal the information about the Queen to a passing adult on an open day display unless their registration included disclosure to members of the general public.

As far as examination marks are concerned, the Act contains specific provisions which most UK Universities have chosen to ignore. They escape by using the 40 day maximum period allowed to execute disclosure, by saying they will always take 40 days to disclose, and because exam marks are never in the computer for more than 39 days they will never be disclosed. The Data Protection Registrar (effectively the relevant ombudsman) has commented that this is probably legal but violates the spirit of the Act. If universities keep exam data (including continuing assessment results) on the computer, or print out/OCR techniques to "cheat", they are definitely in breach of the Act. If they manually re-input a previous years data, they have deliberately chosen a risky route, with obviously increased possibility of error, they may end up violating the principles that "Personal data shall be accurate ..." and "Appropriate security measures shall be taken ... against accidental loss or destruction of personal data".

Needless to say these aspect of the Act is totally unworkable, and only serve to encourage people to ignore it, even when it matters, which has a serious "risks" component. An Act which failed to distinguish between automated and manual methods, and which avoided the need for registration by allowing anyone to ask anyone for data (if they have any) would be far less risky.

For further information see my paper "Computer Conferencing and Data Protection" in The Computer Law and Security Report, March/April 1990, or the more popular "Letter of the Law" in the (UK) Personal Computer World for May 1990. (If anyone knows of any relevant UK court case developments in the last year, please let me know.)

Chris Reynolds CSIRO, Division of Information Technology, PO Box 1599, NORTH RYDE, NSW 2113, AUSTRALIA +61-2-887-9480

DEC copies system software, charges pirates [Digital Forgery]

<bremner@cs.sfu.ca>
13 May 91 12:16 -0700

RISKS readers will recall the story of a DEC UK employee who attended a seminar and copied the system software off the machine the seminar was taught on. The firm that gave the seminar was subsequently charged with pirating the software.

My concern is not with the cloak and dagger aspect or the actual copying, but with the admissability of digital media as evidence. Audio recordings are not admissable as evidence in any jurisdiction that I am familiar with; compared with the tricky job of splicing together an audio tape, forging a copy of a mag tape with system software on it is trivial.

My conclusion (as a legal layman) would be that the presentation of a tape with and incriminating serial number on it would have exactly the same weight as the presentation of a piece of paper with the same serial number scribbled on it: none (actually, I guess it might convince me that the witness was not misremembering). What counts here is the word of the DEC employee who says: yes, I copied this (to tape or paper) off of the system in question.

bremner@cs.sfu.ca ubc-cs!fornax!bremner

Re: Free speech & government control of information (RISKS-11.60)

Larry Hunter <owner-cpsr-dc@nlm.nih.gov>
Mon, 13 May 91 11:41:45 EDT

I feel compelled to continue the debate that Jerry Leichter and I have been having on goverment control of information, particularly as it applies to the current attempts to regulate effective encryption. In RISKS-11.60 Leichter says:

> There are two basic areas in which we differ. First, Hunter believes I'm attempting to prescribe appropriate actions. If I gave this impression, let me correct it: I'm trying to PREDICT. My claim is not that stricter controls are a good idea. Rather, I suggest that they are an inevitable result of the direction in which our technologies are headed.

If Liechter thought stricter controls on the flow of information were a bad idea, he certainly fooled me. And the way I read the rest of his message, doesn't seem to object that strongly.

> (There's certainly room for a good deal of debate about "technological determinism" here. It's not that I don't believe that alternative paths are POSSIBLE; I'm just projecting what I think is by far the most likely path.)

I agree that the government is very likely to attempt to dramatically extend its already quite intrusive control over the flow of information. Major corporations and other socially powerful entities will also attempt to control the flow of information that effects them. I further agree that alternative paths are possible. Does it not seem to follow from those stipulations and implication above that this control is not good, that we, as a sophisticated and priviledged (i.e. well educated, financially secure) computer scientists,

OUGHT to be working to PREVENT new controls on of the flow of information, especially something as nasty and unnecessary as the prohibition of effective encryption??!!

> The second issue grows from the first, and Hunter's view of how the fundamental laws of our society are determined. To state it starkly: If "society" comes to believe that government controls on information are necessary, will constitutional limitations still prevent them from coming into being? Hunter believes so; I think he's being naive.

I believe that I (and others) OUGHT to work hard to keep the government from imposing the controls that it has proposed, and others like them. The constitution is a very powerful tool that can be used in this battle to preserve rights that lawmakers (and even political majorities) may wish to curtail. I think it is one of our best tools in this battle. It may be naive, but it seems to me that you have a very cynical view of the role of the consitution in this society. (To my mind, it is America's most positive contribution to political history.)

> The Constitution protects "speech", "religion", "the press". It never defines any of these terms; case law does. We think we know what they mean, and that the "clear meaning" will not change, but history makes it clear that these terms are quite malleable. .... Note that we don't need a constitutional amendment to effectively change the definitions of crucial terms in the Constitution - all we need is a majority of the Supreme Court. ... I see little reason to suppose that the courts will blindly accept that all computerized information is "speech", if society decides that some limitations on it are necessary.

True, and somewhat cynical, but recall that I am not arguing for reliance on the supreme court to protect the ability of Americans to use effective encryption. I think that we ought to be education, lobbying, FIGHTING to preserve this aspect of the right to free speech, and that the constitution is an important tool in this fight. "Society" is not an entity that believes and decides; people do. People who, these days, are being called upon to have opinions about many issues that were recently obscure technical minutia. I suggest that we as responsible computer scientists have an obligation to communicate, educate and act as concerned experts in the political process.

> In the past, we've generally been able to draw the line between things or acts and information - "mere speech".... In the information age, this line becomes fuzzy. For export, a description of DES is OK, a chip implementing it is not. How about a good software implementation? Should a computer virus - simultaneously speech (pure information) and a potentially dangerous "thing" - be freely publishable?

These are important questions that can (and will) be settled by in the political process, as is the question of whether the government should be able to break all encryption schemes sold to American citizens. Some of these questions are easier than others. For example, letting loose a virus or any other kind destructive program seems clearly action. E.g. Robert Morris, Jr.

didn't even try a free speech defense at his trial. Free speech is not an international guarantee (there are many people who are denied visas to visit the US because of their opinions or comments), so the export issue seems moot, although someone from DEC ought to know that export restrictions can include software...

> Let me give a non-computer example of the kind of problem we will face: Mr. M is a numerologist and conspiracy theorist. He believes that he can track down conspiracies in the world by examining various numerical data related to people. He starts a magazine, OutNumber, in which he regularly publishes any numbers he can find concerning (mainly) the rich and powerful. Mr. M has a following, and he has money to pay for tips, so he has no problem finding all sorts of interesting numbers concerning people. Soon he is publishing people's charge account numbers, checking account numbers, PIN's, private telephone numbers, cellular phone numbers, and so on. At no time is there any question of Mr. M's involvement in any attempt to use this data for fraudulent purposes - he is sincerely interested only in his numerological research.
>
> OutNumber, and Mr. M, are probably protected under the Constitution as we currently construe it. My question is, should they be? Do you think there's really a social concensus that it's essential to protect the ravings of a Mr. M, even in the face of (let us imagine) clear evidence of massive fraud by OutNumber readers against those "profiled" in the magazine? How long do you think the courts will stand up in the face of a new concensus that says, hey, get rid of this guy?

I leave this intact because I think it is a good example. I would say that Mr. M should indeed be allowed to publish his magazine. I for one would suspect that anything that shut him down would also be used to close down David Burnham's Transactional Records Analysis Center (TRAC) which has made some remarkable inferences about the IRS and other government activities on the basis of analysis of public records. I'm sure there are lots of people in the government who would like to shut him down, and that such a law would be applied to TRAC long before it would be applied to Mr. M's hypothetical gossip rag. And I suspect that existing law would adequately protect the celebrities defrauded by readers - that's what fraud laws are for. As for social consensus, I recognize that the content of the Bill of Rights is consistantly supported by less than half of the population in polls, but that does not mean it ought to be overturned or ignored. It means that we have to act to preserve it.

> Finally, Hunter responds to my suggestion of some fiction stories with readings on political theory. I have no problem with this. The reason I suggest fiction is that social concensus, and ultimately law, grow as much out of the gut as out of the head. Good fiction lets you explore your own gut feelings.

Emerson's book is not political theory, it is a history and explication of free

speech rights. Read whatever you like. After all, that is the whole point of this argument, isn't it?

Lawrence Hunter, National Library of Medicine. Please note that I am not speaking as a representative of the government.

Re: Case of the Replicated Errors: An Internet Postmaster's Horror Story

Neil Rickert <rickert@cs.niu.edu>
Mon, 13 May 91 13:36:50 -0500

In RISKS DIGEST 11.66, Erik Fair <fair@APPLE.COM> reports on a mail problem encountered at Apple.COM, at relay.cs.net, and at uunet.uu.net

Erik's report made interesting reading, and does raise some issues of concern.

However, in pointing the finger at the culprit, I believe he has pointed it fairly and squarely in the wrong place.

>The important part is that the "To:" field contained exactly one "<" character,
>without a matching ">" character. This minor point caused the massive
>devastation, because it interacted with a bug in sendmail.

This "minor point", as Erik calls it, is a violation of the standard for Internet addresses (RFC822). Many would say that this is a MAJOR point.

>Sendmail, arguably the standard SMTP daemon and mailer for UNIX, doesn't like
>"To:" fields which are constructed as described. What it does about this is the
>real problem: it sends an error message back to the sender of the message, AND
>delivers the original message onward to whatever specified destinations are
>listed in the recipient list.
>This is deadly.

Excuse me, but this by itself is not deadly.

Let's look at the exact set of conditions which were involved:

1. Mail was sent with an invalid "To:" header.

2. The mail was completely deliverable, in spite of the syntax error, so sendmail proceeded to deliver it.

3. Sendmail reported the error to the message originator.

4. Sendmail did not "repair" the syntax error.

5. The message was destined for a mailing list with many recipients, implying that the error would be rediscovered at each of a large number of relay points.

The combination of all of these was involved in the error.

Erik points his finger only at items 2 and 3. This, I believe, is incorrect.

In spite of the syntax error, it is correct to attempt to deliver the mail if this is still possible. Robustness requires this.

Once a serious error has been discovered, it is correct to report this. Reliability of systems depends on reporting of errors.

Items 2 and 3, then are just plain good programming practice. They cannot be blamed for this problem.

Look now at item 4. There is no question that had 'sendmail' repaired the problem header this would have avoided the problem. Unfortunately there are no standards as to how this should be done. The RFCs recommend against modifying headers. Perhaps some provision should be included that where a an invalid header causes an error to be reported, that header must be "repaired" in some way before the message is sent on. Perhaps the best way to repair the header would have been to relabel it as say "Invalid-To:" or something equivalent, which hopefully would prevent a further syntax analysis at future sites. But, to implement something like this requires a standard.

Certainly sendmail can be indicted for item 4. But it's guilt is secondary to that of the originating mailer which emitted the erroneous header in the first place. Thus the finger here should be pointed back fairly and squarely to Apple.COM, with only contributory negligence on the part of sendmail.

The primary problem, however, is in item 5. For a normal mail message with a handful of recipients, each relayed through a modest number of hosts, the number of messages would have been quite small. It is because this message is to a mailing list that so many problems arose.

The conclusion is clear. Administrators of mailing lists have a special responsibility. It is not enough to use an aliases entry to replicate the original message. The mailing list must be considered to be creating a new message based on the contents of the original message. As such it must take care to meet the various standards for mail (such as RFC822). This should involve validation and repair, if necessary, of any required headers.

Neil W. Rickert, Computer Science, Northern Illinois Univ., DeKalb, IL 60115
+1-815-753-6940

Re: Case of the Replicated Errors: An Internet Postmaster's Horror Story

"Erik E. Fair" (Your Friendly Postmaster) <fair@apple.com>
Mon, 13 May 91 17:16:06 -0700

I disagree [with Neil]. I would have no problem with sendmail logging that a syntax error was found. What I object to is that it BOTH reported the error back in a separate message to the sender, AND forwarded the message onward to other waiting sendmail which would do the same thing. This is a recipie for disaster, as I saw.

Sendmail should either bounce the letter, or deliver it with no further comment than a log entry. It should NEVER report an error in a return message when it is not the MTA doing final delivery, unless it is actually bouncing the letter, and will not forward it further.

And this has nothing to do with mailing lists - it can (and will) happen if a user just sends out to a list of 100 people, with no formally set up mailing list involved.

Erik E. Fair apple!fair fair@apple.com

Re: Case of the Replicated Errors: An Internet Postmaster's Horror Story

Dan Boyd <consp04@bingsunp.bingsuns.cc.binghamton.edu>
13 May 91 14:43:39

Just goes to show you how hairy sendmail is -- a single misplaced open-bracket, and suddenly your site switches into Craig-Shergold mode...

-- Dan

Daniel F. Boyd

Re: Netware LOGIN problems (John Graham-Cumming, RISKS-11.65)

Leonard Erickson <70524.2603@compuserve.com>
14 May 91 01:39:24 EDT

>I'm managing (at least for the moment) a Novell network running Netware
>286. I've recently realised that it is possible to pipe a file into the LOGIN
>command. This has the rather unfortunate affect that it is possible to
>write a Trojan horse which simulates login

Well, under Netware 2.11 (the oldest version that I've worked with), piping does *not* work. The password must be entered from the keyboard (or stuffed into the keyboard buffer)

So the first solution would be to update your software. Stuffing the keyboard buffer is still a loophole, but vulnerability is very limited if proper security is used. For instance, not allowing users to write files in the LOGIN directory on the network. This requires the trojan to be installed on a particular machine. And requires the "owner" of the program to visit that machine to get the info.

For statistical purposes, we wrote a program that is run as part of the system login script that saves whatever strings are passed to it to a globally *writable* file. We save the Physcal-ID, the login name, the date, time and a few other things.

This turned out to be *very* useful the one time someone submitted a "fake" request for a user account. Once the fake user was called to our attention (he wrote some objectionable email). It was a matter of a few minutes to grep thrhu

the log and find which stations he'd used and when... from there, it was easy to find him.

We also limit most users to *one* connection at a time. This makes it very obvious if anybody tries to use someone else's account at the same time as they are on line.

As others have noted, it is users ignoring good security practices that is the biggest problem. I've come in early on a monday morning and discovered that users in an open area (office cubicles), had not only left their machine logged in all weekend, but that they had left them inside the mail program. I wandered over and sent them a letter "from themselves" warning them that I could have sent *anything* to *anyone*. Didn't faze them. <sigh>

Emergency off switch - IBM 1620

<cook@csel4.eng.ohio-state.edu>
Mon, 13 May 91 15:57:53 EDT

There was real concern in the days of the IBM-1620 and early 360's that the need to destroy the link to power would arise. In some versions, pulling the switch caused a sort of knife blade to sever the cables.

These precautions were seldom needed. Most centers, including the one in which I operated the 1620 and 360, had an elaborate power control system which shut off power to the computer, the lights, the terminals, and the air conditioning.
R.I.Cook, M.D.

Search RISKS using swish-e

THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

ACM Committee on Computers and Public Policy, Peter G. Neumann, moderator

Volume 11: Issue 68

Thursday 16 May 1991

Contents

Is fuzzy control more suitable for nuclear reactors?

Paul Eggert <eggert@twinsun.com>
Tue, 14 May 91 18:25:27 PDT

Japan's Power Reactor and Nuclear Fuel Development Corporation, an R&D organization supervised by the Science and Technology Agency, is now using fuzzy logic to control the water temperature of a tank in the Fugen prototype heavy water reactor operating in the Fukui prefecture. The fuzzy device, an Omron FZ-1000, is not used in normal, stable operation, but only when the reactor starts or shuts down, under the

argument that in these conditions fuzzy logic is more suitable for the large amounts of information generated and is less prone to phenomena like overshooting. The fuzzy control is monitored by a human operator and is not yet used in critical places. Further details can be found in Thomas Hagemann's report ``Visit to Omron's Fuzzy Business Promotion Center, Kyoto'', comp.research.japan <4702@gmdzi.gmd.de>, 14 May 1991.

The fuzzy device is not yet being used for critical operations here. But the implication is that fuzzy logic is better than conventional logic precisely when safety is most at risk, i.e. when the reactor is not in normal, stable operation. I'm skeptical. But if true, there may soon be a pressing need for formal verification of fuzzy systems, whatever that may mean.

Paul Eggert

[It better be better, or else someone will be guilty of Zadehmy. PGN]

Of Two Minds about Privacy???

David States <states@ncbi.nlm.nih.gov>
Wed, 15 May 91 00:42:58 EDT

An article in this month's Scientific American states that "privacy legislation has been nickeled and dimed to death" ... but "Maybe that is the way most Americans want it. According to a survey commissioned by Equifax, one of the three major credit reporting bureaus ..." The article then goes on to cite a Harris survey that lists credit reports and loan approvals as examples where most Americans accept invasion of their privacy. Beyond being an obviously self-serving conclusion, it misses the point. A loan request is initiated by the individual and most people would distinguish between a credit check that you have authorized and one done without your knowledge.

Is this an isolated incident or the opening salvo in a PR blitz designed to systematically undermine our privacy rights?

David States

Re: Horible Speling (RISKS-11.66)

Adam Engst <ace@tidbits.UUCP>
Tue, May 14, 1991 9:24:57 AM

I must argue slightly with the story of the teacher who can't spell because he's used to having his computer do it for him. The spell check is a crutch for some, but for many of us it is merely an aid to prevent irritating and subtle errors from finding their way into our texts. Almost no words flagged by my spell checker are words I don't know how to spell, and if they happen to be, I usually figure it out after a while. For some strange reason my fingers wanted to type "propoganda" instead of the correct "propaganda" for a while, but thanks to the continued vigilance of Nisus's excellent spell checker, I've gotten over that unfortunate problem. My point is that the spell checker does not have to be crutch. It can be a learning tool as well, but only if the companies producing word processors design it as such. Complain to them if the

teachers of today cannot spell without that electronic crutch.

Adam C. Engst Editor of TidBITS, the weekly electronic Macintosh journal

---

Re: Changing class grades in Alaska (Gottehrer, RISKS-11.62)

Scott Barman <scott@nbc1.ge.com>
Tue, 14 May 91 20:15:16 EDT

There were things that happened a long time ago (10 years??) when I was a student at the University of Georgia. They ran what was called the University System Computer Network which basically was leased lines and terminal controllers to connect the state universities to a CDC Cyber (70/74 then a 170) running NOS sitting in the computer center at UGA. I don't have to tell RISKS followers about the security problems under NOS!

The unfortunate thing about is that this machine was used by University System schools for more than just student computing. There was one "rumor" that allegedly someone at (I think) Georgia Southern changed grades for students at schools other than GSC. I remember assisting a friend who was working for the campus newspaper (the Red and Black) and getting hung up on by several computer center and university officials when we called for information. We were later lectured by the director of the computer center at that time about minding our own business.

The other "rumor" could not be confirmed by print and electronic media since it was a case settled out of court and the records sealed (allegedly because it contained a record of exactly what happened and they determined it to be a risk to the USCN). Allegedly, someone at West Georgia College broke into thier payroll system and had some checks printed in his name--not an alias.

Both of these happened sometime around 1980-82, before computer-related laws made it to the books. I hope there's someone in Georgia who remembers these and can give better details! [...]

scott barman scott@nbc1.ge.com

Re: Emergency off switch - IBM 1620 (RISKS-11.66)

Doug Hardie <doug@NISD.CAM.UNISYS.COM>
Tue, 14 May 91 14:27:49 PDT

I ran a large college computer center many years ago with an IBM 1620. Because the machine was easily accessible by students, we had numerous instances of someone pulling the emergency off switch. The IBM maintenance man got tired of coming out to put it back in. There was a small pin that fell down to the bottom of the cabinet that prevented you from pushing it back in. He showed us how to reset it so he wouldn't be bothered by that anymore. We never encountered any equipment damage from these incidents.

We did encounter another "feature" of the 1620 that was destructive of hardware. Two of us developed a 3 or 4 instruction program that generated some number series. The object was to find the millionth number in the series, or something like that. The program consisted of several instructions that executed quickly (for a 1620) and one divide instruction that was about 100 times longer. We started it running on a Friday evening expecting it would run most of the weekend. After checking some of the early values, we decided to go out to a fast food joint for dinner. We returned about 2300 to find smoke pouring out of the computer room windows. We pulled the emergency power off switch and opened the windows. Didn't want to call the fire department - too much paperwork and embarrassing questions. After the room cleared so we could see, we opened the swinging racks in the back of the control unit. On the end of the innermost one was a Bud box bolted on with a power transistor heat sinked to the outside. That transistor was bubbling some kind of ooze and lots of smoke. We called our maintenance man who came right away. The transistor was part of the divide logic (a late add-on in the design). He first asked what program we were running. Then he asked why we were violating the divide instruction duty cycle. We had never heard of any such restriction, but he was insistent and spent hours searching through the volumes of schematics looking for it. Finally, he grabbed a marker and wrote a divide instruction duty cycle on the cover of one and said something to the effect of there it is, I told you so...

> Men were men in those days, and giants strode the earth.

and students caused them all to crash regularly.

-- Doug

The big red switch on old IBM systems

Bob Wilson <wilson@math.wisc.edu>
Tue, 14 May 91 15:16:48 cdt

The big red power-off switch which used to appear on the panel of the 1620 and earlier machines (650, 70x) came with lots of warnings to the users NEVER to use it, as has been mentioned here recently. As so often happens, it was a device which started out serving a real need and lived beyond it. On machines like the 650, where ALL storage was on a magnetic drum enclosed in the main cabinet (mag core was added later), slow warming up and cooling off was critical. The drum heads were fixed over the magnetic surface, not floating like current disk heads, and of course had to be close to the surface. They were mounted to rigid metal bars to keep the distance fixed, but of course all the various materials had different coefficients of thermal expansion. If you used the "correct" power down procedure, all the cooling air would keep flowing and the system could come down without turning new grooves in the drum. If there were to be a fire, however, of course you wouldn't want to keep pumping in air! Hence the emergency switch. Since it was (we were told) sure to damage the machine if you turned it off with the emergency switch, the switch could not be turned back on without a call from your friendly customer service engineer. The switch had a little pin inside which had to be retracted before you could flip the switch back to the on position. All of that made pretty good sense for the 650 and similar machines. By the 1620, though: The logic

was solid state rather than tubes, and hence generated much less heat. The main memory was core. The interior air driving was reduced to biscuit fans similar to present practice. BUT the same old switch was installed, so that in theory if it got flipped you had to call for service. Most of us found out how to reset it, because some novice was sure to use it sooner or later.

Bob Wilson
Math. Dept., Univ. of Wisconsin wilson@math.wisc.edu

Re: Emergency off switch... (RISKS-11.66)

Robert E. Van Cleef <vancleef@garg.nas.nasa.gov>
Wed, 15 May 91 08:24:54 -0700

On the console of our Amdahl mainframe system, there is a large button labled "Emergency Pull", which had an equivalent function to the one described by Martin Ewing in RISKS-11.66.

One weekend we had a problem with the system that the assigned Customer Engineer did not consider serious enough to justify leaving home, inspite of the arguments from the local Site Manager that the primary subsystem could not run.

The Site Manager then called him from the phone adjacent to the console. He mentioned this switch to the CE, casually asking what would happen if it was pulled. Upon confirmation that is a priority service call would be required to reset the switch, the Site Manager calmly pulled the switch and said "Gee; the system seems to be dead!"

The CE sighed, and came in...

Bob Van Cleef vancleef@nas.nasa.gov
NASA Ames Research Center (415) 604-4366

Re: Emergency off switches

Al Donaldson <al@escom.com>
Wed, 15 May 91 01:00:41 EDT

R. I. Cook mentions the elaborate power control systems for old-time computer centers. This reminds me of the time I worked as a transmitter engineer for a UHF TV station (~1 megawatt). The transmitter was housed in a Butler building out in the boonies, with the transmitter enclosure in the middle of the floor. The enclosure was perhaps 15 by 20 feet, water-cooled, and you could enter the enclosure through a door to perform maintenance. Other amenities were real primitive, with the toilet facilities sort of hidden in a back corner behind the transmitter enclosure.

This was a family operation and one day the owners were in town to do some work on the antenna (nosir, I don't climb 1100 feet in the air for $3/hour...) The wife of one of the owners came along, and after a while, she excused herself to go to the "ladies room."

I guess no one must have told her where the toilet was located, because the next thing we heard was this incredibly loud BANG as she tripped the interlocks to the transmitter door and shut down the transmitter.

Al

Re: Emergency off switch - IBM 1620

S. H. Schwartz <schwartz@nynexst.com>
Wed, 15 May 91 17:03:40 GMT

We had an IBM 1130 in high school (late 70s). One day a student noticed smoke coming out of the rear of the console. He naturally pulled the EMERGENCY STOP switch. We later discovered that someone had dropped a smoldering cigarette behind the console.

Moral: When that big, red button is staring you in the face, day after day, it's easy to find an excuse to use it.

S. H. Schwartz Expert Systems Laboratory NYNEX Science and Technology Center White Plains NY 10604 914-683-2960

Real men and the IBM 1620

Dick Hamlet <hamlet@eecs.ee.pdx.edu>
Wed, 15 May 91 11:36:47 -0700

Recalling the IBM 1620 destructive power switch and the days of "real men" is too good an opening to resist. That machine had a console table on which was mounted a printer for the operator, the only i/o device that a human could read directly. It was used to print error messages, or for low-volume output from programs. (For REAL output, one punched cards and listed them off line on tab equipment.) Later versions of the 1620 used an IBM Selectric typewriter for console i/o, but in 1965 I used an older machine at Argonne National Labs that was fitted with a standard IBM model C electric typewriter. The unit was mounted near the right edge of the table, in such a way that when the carriage returned (under program control!), it was capable of dealing a passing human a nasty blow in the groin. (Not so many real men among the long-term users!) But not to worry, IBM soon recognized the risk, and made available for lease a sort of bent wire guard that delimited the area in which it was unsafe to pass. I wish I knew how much this guard leased for, and what it was called in the 1620 parts list.

RISKS of redistributing SF-LOVERS Digest

"Roger H. Goun 13-May-1991 2100" <goun@ddif.enet.dec.com>
Wed, 15 May 91 16:20:51 PDT

I maintain a distribution list with which I redistribute SF-LOVERS Digest to a

large number of DECcies. While less convenient than direct mailing from the moderator, this arrangement avoids clogging Digital's Internet gateway with nonessential messages. Today I accidentally forwarded another, completely unrelated message to the distribution list. The circumstances may be of interest to RISKS readers.

I have a VMS command procedure that does most of the work of archiving and mailing an issue of the digest. When I'm using DECwindows Mail, as I normally do, I fire the command procedure off from FileView, a GUI for manipulating programs and other files. When I'm logged in from home, I can do it by pressing a couple of keypad keys in character-cell Mail. I haven't done it from character-cell Mail in quite some time, but I was working at home this afternoon, and there was a backlog of digests since I'd been out of town for a few days, so I thought I'd clear out the digests awaiting redistribution. Unfortunately, I fumble-fingered the keypad and dispatched the wrong message.

Now I'm not entirely stupid, so I built some sanity-checking into this command procedure. The first thing it does is search for the "Volume m : Issue n" string in the digest, and it dies with a warning if the string can't be found. Unfortunately, my command procedure had no trouble finding the magic string in this particular message. Next, the command procedure searches the archive for a file called m.SFL, where m is the issue number extracted from the message in hand, and dies if it finds such a file, assuming that this message must be a duplicate. (The archive gets purged every month, so volume/issue rollover isn't a problem.) No such archive file was found, so the unrelated message was sent out. What WAS this bogus message? Why, an issue of RISKS, of course!

RISKS and SF-LOVERS share a common digest format, which defeated the first check. SF-LOVERS publishes more frequently than does RISKS, so the corresponding issue of SF-LOVERS had already been purged from the archive. So much for the sanity checks.

Lessons learned:

- use of a less familiar user interface (in this case, a different mail program) can be error prone.

- sanity-checking doesn't, perhaps because the world isn't sane.

- God is an iron (how else to explain the irony?).

Roger H. Goun, Digital Equipment Corporation, Nashua, NH 03062, +1 603 881 0022, goun%ddif.enet@decwrl.dec.com, {uunet,sun,pyramid}!decwrl!ddif.enet!goun

---

re: case of the replicated errors

Joe Buck <jbuck@ohm.berkeley.edu>
Tue, 14 May 91 13:12:59 PDT

Erik Fair reports on an e-mail disaster that generated tens of thousands of mail messages reporting errors, all directed at his site. Neil Rickert summarizes the conditions that produced the error roughly as follows

1) The To: line had a syntax error (a missing ">" character)
2) The mail was deliverable, so sendmail delivered it.
3) Sendmail reported the error to the originator by mail.
4) Sendmail did not "repair" the error.
5) The message went to a mailing list with many recipients.

Erik Fair's diagnosis: the combination of #2 and #3 caused the disaster (by causing every sendmail program on the net that saw the message to produce an additional error report). Neil Rickert wants to focus on #1 and #5, putting blame on either the sender, the originating mailer, or the mailing list maintainer, and admonishing people not to ever generate bogus mail messages and, if that fails, have mailing list maintainers make sure that it never happens.

Sorry, Neil. Robust software does not cause disasters when presented with bad input, and many mailing list maintainers are not experts in network protocols.

This kind of disaster has happened before, on Usenet. Someone, somewhere, managed to inject a tab into the Message-ID header field, and the offending message (called an "article" in Usenet-speak) got transmitted all over the net.

When this message was received by a site running the standard Usenet news software (version 2.11 of B news at whatever patch level was current at the time), its Message-ID was inserted into the history file, which uses tabs to delimit fields. This had two results:

1) The "duplicate article" check broke: the software "believed" that it had no copy of the article, and pairs of sites that used the "ihave/sendme" protocol generated thousands of duplicate copies.

2) The "expire" program also could not parse the history file entry (this program is responsible for deleting old news), so it was incapable of removing the offending articles, and it generated verbose error messages on the log file.

The combination caused an explosion of Usenet traffic, limited only when major sites' disk partitions filled up completely, preventing them from accepting any more. Thousands of hours were spent all over the net cleaning up after this disaster.

Rick Adams (head maintainer of 2.11 news) then issued an emergency patch that, on receipt of an article with whitespace in the Message-ID, would change the whitespace to "?" characters (or some other character). Notice that this solution violates the "Thou shalt not rewrite a header" holy writ, but I'm for it.

Neil, do you think that exhorting people to make sure that their software never put a tab in their message-ID, and assigning moderators special responsibility, is a satisfactory solution to problems like this? Of course not. Once in a while we'll find that our software systems permit disasters to happen. It's not good enough to try to prevent bad input from ever reaching a system; it must be able to deal with any input. The problem with making software

idiot-proof is that the idiots are so damn clever.

Re: Case of the Replicated Errors

John R MacMillan <john@scocan.sco.com>
Wed, 15 May 91 16:56:20 -0400

| In spite of the syntax error, it is correct to attempt to deliver the mail
|if this is still possible. Robustness requires this.

I disagree. As you pointed out, the message violated the message
standard, and so should NOT be passed on.

| Once a serious error has been discovered, it is correct to report this.
|Reliability of systems depends on reporting of errors.
|
| Items 2 and 3, then are just plain good programming practice. They cannot
|be blamed for this problem.

Individually, in the correct circumstances, this is true. But to do
both in this situation was not. As you pointed out, sendmail could
not correct the header, so the MTA should have either passed the mail
(perhap annotating it with some sort of error header, as MMDF would do
in this same case), or bounced it with a complaint.

Search RISKS using swish-e

THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

ACM Committee on Computers and Public Policy, Peter G. Neumann, moderator

Volume 11: Issue 69

Saturday 18 May 1991

Contents

---

42 die in Japanese train crash under manual standby operation

"Peter G. Neumann" <neumann@csl.sri.com>
Sat, 18 May 91 14:05:47 PDT

Investigations of the head-on collision on 14 May 91 were apparently focusing on the railroad crews, who were supposedly using hand signals because of the malfunction of an automatic signalling system at a 100-foot long siding that had recently been installed especially for running trains from Kyoto to a world

ceramic arts festival at Shigaraki, 215 miles south of Tokyo. 42 died, 415 were injured, 1.5 miles from the siding at which the trains were supposed to have passed. The train was carrying 2.5 times its normal capacity, "but packing trains is not illegal in Japan and is so common that big-city commuter lines assign workers to push the last few passengers through the doors at the daily rush hours."

Source: John E. Woodruff, Baltimore Sun, datelined Tokyo, in the San Francisco Chronicle, 15 May 91. p.A7.

Electronic Ballot Voted Out in World's Largest Democracy

Les Earnest <LES@SAIL.Stanford.EDU>
16 May 91 1424 PDT

By SRINIVASA PRASAD, Associated Press Writer

BANGALORE, India (AP) - India has had the electronic voting machine for 10 years. But when parliamentary elections are held next week, vote counters will again be tallying more than 300 million slips of paper - one by one. Use of the machine previously was snagged by legal barriers, opposition by politicians, doubts about the ability of rural Indian voters to use it and fears it could be rigged. Those hurdles were finally cleared, but the national Election Commission decided the nine-week run-up to the surprise elections was not sufficient to teach the 3 million polling officers how to use the gadget. About 150,000 voting machines will remain stashed in government stores. ``We have faith in the machines, but we can't take risks by using it before properly training the officers first,'' Chief Election Commissioner T.N. Seshan told reporters.

There are no professional polling officials in India. School and college teachers and government clerks are hired as part-time election supervisors. The three days of voting spread over next week were called hastily after the minority government of Prime Minister Chandra Shekhar resigned abruptly on March 6 because of difficulties in governing. He will remain in office until replaced.

Indian voters elect their candidates by using rubber stamps to mark ballots, which are printed with election symbols of political parties or independent candidates. Emblems instead of names are used because 75 percent of India's 515 million voters cannot read. The emblem of former Prime Minister Rajiv Gandhi's Congress Party is an open palm. The Janata Dal party of his successor, V.P. Singh, uses a wheel. Chandra Shekhar's Janata Dal-Socialist party has a farmer with a plough inside a wheel. The Bharatiya Janata, or Indian People's Party, is identified with a lotus. Among the hundreds of symbols used by other parties and independent candidates are a bicycle, rising sun, two leaves, string cot and tree.

The electronic voting machine displays the symbols on a screen with a button next to each picture. The button is pressed to register a vote and it can be used only once until the polling officer releases the mechanism. ``It is precisely to minimize rigging that the Indian machines have several features that are not there in the ones used in developing countries,'' said L.S. Anant of the state-owned Bharat Electronics Ltd., which makes the machine.

Many observers say voting machines would cut costs and get faster results. They say the threat of election rigging is no worse than the current system,

which brings frequent charges of ballot-box stuffing.

National elections are time consuming and costly in India, the world's second most populous nation and the world's largest democracy with 844 million people. The number of voters is more than twice the United States' population, although only 310 million to 370 million people usually cast votes. Because of the vastness of the country polling is normally spread over three days to allow security forces to be shifted to protect the 600,000 polling stations.

The votes will be counted continuously after the first day of elections Monday and final results will be announced three days after the last day of polling, May 26.

Central postal/banking computer failure in Japan

<[anonymous]>
Thu, 16 May 91 09:12:39 xxx

Computer failure hits post office banking in 6 prefectures

Sendai, May 16 (Kyodo) - A large postal banking computer went down Thursday at a computer center in Sendai, putting banking machines out of action for more than three hours throughout Hokkaido and five prefectures in northern Honshu. Computer technicians had the main computer, one of three at the ministry of posts and telecommunications East Japan no. 2 computing center, back on line shortly before noon but postal authorities could not say what had caused the computer to fail. A total of 1,200 post offices throughout Hokkaido and the northern prefectures were affected, with 1,300 automatic teller machines and cash dispensers out of action. Another 3,000 transaction machines used by counter clerks at 2,900 post offices were also inoperable.

According to postal bureau officials, the automatic teller operations can be shifted to an auxiliary computer if one of the three main computers goes down but this failed after thursday's breakdown. Counter clerks in the post offices processed transactions by hand during the failure, the authorities said. Until last week, postal banking services in the four northern regional bureaus were handled by three computer centers in Sendai, Nagano, and Otaru in Hokkaido. To improve efficiency, however, operations were concentrated at the center in Sendai from May 6.

Of Two Minds About Privacy ??? (RISKS 11.68)

"Mary Culnan" <mculnan@guvax.georgetown.edu>
16 May 91 21:49:00 EDT

Unfortunately, I think our privacy rights have already BEEN undermined-- at least when it comes to credit information. There are three ways in which the privacy of credit reports is/can be violated:

1) Because credit reports are online, it is relatively easy for unauthorized people to pull your report (recall Jeff Rothfeder, the Business Week reporter, who got access to Dan Quayle's credit report thru a Super Bureau).

2) The big 3 credit bureaus will prescreen your credit report for unsolicited (by you) offers of credit and/or sell mailing lists against a different database consisting of summarized data from your credit report.

3) TRW and Equifax will also do list enhancement with the marketing database, that is, match their database against a tape another firm sends in and add information about you from their marketing databse to the tape that was sent in (assuming you are on the tape that was sent in). For example, a bank wants to learn more about its customers--it could have its customer file enhanced with summarized credit data. At least one firm has the Equifax marketing database running on its own mainframe.

The credit bureaus will let you opt out of the marketing applications by writing to them. However, in the case where the database itself has gone to a third party, it's hard to see how an individual can exert any control over this information.

Much of this sadly reminds me of problems raised by the Lotus MarketPlace. Further, this is all legal due to giant loopholes in the FCRA.

Mary Culnan

The Death of Privacy?

Jerry Leichter <leichter@lrw.com>
Fri, 17 May 91 00:17:42 EDT

In a recent RISKS, David States quotes a Scientific American article stating that "privacy legislation has been nickeled and dimed to death" - but that most Americans, according to an Equifax survey, don't seem to mind. He wonders whether this is an opening salvo in further attempts to limit privacy.

I think there's something much deeper going on. The more I look around me, the more I come to the conclusion that we, as a society, have almost lost the very idea of privacy. Consider what would, 30 years ago, have been considered "private" by most people. A list might include such things as financial matters - particularly how much money they make/have, health records, family relationships, sexual matters, personal opinions about other people. Today, huge numbers of people have access to our financial and health information, we're encouraged to be "open" about our feelings, sex is widely discussed (note that 30 years ago, "privacy" about sex INCLUDED not having OTHER people's sex live discussed in public), etc.

We can blame some of the changes, particularly about things like financial and health records, on business or government. It's hard to see how we could have medical insurance on today's scale without such records and their relatively wide availability, and in trade for much wider availability of information on our financial affairs we got credit cards and such things; so even here, the story is complex. But much of the "baggage" of privacy we threw away with great enthusiasm during the sexual revolution and the general "opening up" of society in the late '60's. "Let it all hang loose" doesn't mesh well with keeping things private. "Privacy" is closely connected to "shame," but most

of the things traditionally associated with "shame" no longer are either. About the only things we are "supposed" to be ashamed of now are legal or ethical violations.

These are deep-seated and profound changes in our social outlook. They happen to coincide with the emergence of a technology that is able to pierce the anonymity of "mass living". Residents of small communities have never had very much privacy - everyone knew what everyone else was doing. (There was often a tacit social agreement to look the other way, of course.) But large cities were anonymous, and people could get lost in them. Increasingly, they no longer can.

Computerized record-keeping systems have a long history of allowing access to "unauthorized" personnel. When this happens, it should be brought to light and repaired. However, it's important to realize how much of our loss of privacy is intimately connected with the DESIRED operation of our systems. Of cases I can think of from my own personal experience where I felt my own sense of privacy to be violated, one of the most vivid involved having to discuss details of medical treatment with a clerk for some insurance company. By the very nature of the insurance, this clerk was authorized to determine whether I was making a proper claim; but my gut reaction was "this is none of your damn business, I talk to my doctor about that".

-- Jerry

Horible Speling (RISKS-11.66)

Les Earnest <les@dec-lite.stanford.edu>
Thu, 16 May 91 21:55:45 -0700

Unfortunately, I can't blame computers for my spelling lapses, having grown up before they were invented. In fact I invented the spelling checker in 1967 as a cover-up.

I had created a list of the 10,000 most common English words on paper tape when I was at MIT for use by my program that read cursive writing. A year or so after I came to the Stanford Artificial Intelligence Lab, I got a graduate student to write a spelling checker using this word list. He did it in Lisp, which clanked a bit on the DEC PDP-6 that we were using. A few years later I got another student, Ralph Gorin, to write a faster and better machine language version for the SAIL computer, which by that time was a dual processor DEC-10/PDP-6 system.

Freeware was the norm then -- no one even _thought_ of patenting software. From SAIL, the spelling checker spread via Arpanet throughout the DEC-10/20 world, then on to other timesharing systems. When personal computers appeared later, these meddlesome programs became ubiquitous. (I note, however, that the one running here under emacs doesn't recognize "meddlesome.") Unfortunately, spelling checkers don't deal with another composition problem of mine -- fingers that often spell phonetically when I go fast -- because homophones pass the spelling test.

Incidentally, though the venerable SAIL computer now appears to be the oldest

living timesharing system in the world, it hasn't been maintained for a long time and is beginning to show Alzheimer symptoms. On the afternoon of June 7 we plan to have a party celebrating its 25th birthday, last rites, and wake. Anyone who would like to receive SAIL's last words, which are likely to include a boastful summary of its accomplishments, should send a message (content unimportant) to Farewell@SAIL.Stanford.edu.

Les Earnest, 12769 Dianne Drive, Los Altos Hills, CA 94022 415 941-3984
Internet: Les@cs.Stanford.edu UUCP: . . . decwrl!cs.Stanford.edu!Les

---

Re: Horible Speling (Engst, RISKS-11.66)

Brinton Cooper <abc@BRL.MIL>
Thu, 16 May 91 15:05:19 EDT

My wife's pupils (grade 4) use a spell checker in connection with a word processor that's only a little more than an electronic typewriter. Targeted for children, the spell checker will flag homophones (homonyms?) and ask the user if he/she knows which one he/she really wants. This feature seems to be in the spirit of Adam's point.

However, if the teachers of today cannot spell without that electronic crutch, I'd be more likely to complain to (1) them, (2) the school district who hired them, (3) the "university" which trained them, and (4) the public schools where they didn't learn to spell.

_Brint

(bogus) IBM red switch

Mark Seecof <marks@capnet.latimes.com>
Thu, 16 May 91 13:44:21 -0700

Okay, I can't resist adding to the red-switch discussion. I used an IBM 1401 in high school. It had an "emergency" power-off switch--which no one ever pulled. It also had a 1403 600-LPM line printer. If you placed an invalid character in the carriage-control column of a FORTRAN output record, the line printer would spazz out and feed paper continuously at high speed. The printer would emit a loud and distinctive scream as paper shot dramatically from the back.

Of course, inexperienced student programmers who provoked this behaviour would try to stop the printer by punching the large red STOP button on its console. Ha! That button, like its twins on the read/punch unit and CPU cabinet, would halt the processor but have no effect on the printer. There was a transparent button with some innocuous label (I don't remember the exact wording and my manual is at home) which would actually stop the printer. Because panicky students weren't likely to find the proper button before hundreds of feet of paper were propelled through the printer, the official technique for dealing with the situation was to step on the paper in the paper box (which stood open beneath the front of the printer). The printer would tear the paper off neatly at a page-perf and then sit there whining until someone punched the proper

button.

Moral? The large red STOP button on the front of a machine should stop THAT MACHINE, not some other machine on the other side of the room. This is even more important when the machine in question is a mechanical device which could injure someone (suppose your regulation IBM computer-programmer's tie got caught in the tractor feed mechanism as you were peering at some output...).

(Also on the subject of red switches, I have been informed that the reason the newer IBM PS/2's and RS/6000's have white power switches is because of a German government regulation which demands that the ONLY red switch in an entire computer room be one which turns off all power to all equipment in the room, and it was easier for IBM to fit all small computers with white power switches than to fit some with red and some--for sale in Germany--with white. Note also that the Germans have proposed that their (sometimes silly) rules be adopted by the whole EEC.)

Mark Seecof, Publishing Systems Department, Los Angeles Times, Times-Mirror Square, Los Angeles, California 90053 Voice: 213-237-7605 Fax: 213-327-3119

Emergency off switch - IBM 1620 (RISKS-11.67)

Stuart I Feldman <sif@lachesis.bellcore.com>
Fri May 17 21:40:58 1991

If we are reminiscing about ancient unsafe designs, consider the IBM 650, which had both `AC power off' and `DC power off' buttons. The DC power off turned off the active logic (vacuum tubes!). AC power off didn't actually do that, but initiated the power down sequence, which included putting on the braking rotors for the magnetic drum (cylinder rotating at 12,500 rpm). The corresponding `AC power on' button started the spin-up motors. For lack of a relay, there was no interlock between these functions, and it was possible (or so I was warned as a tyke) to warm up the drum by having the two motors fight each other.

So what's so strange about a guillotine for the power cord?

IBM Emergency pull switches

Gene Spafford <spaf@cs.purdue.edu>
17 May 91 02:26:32 GMT

Back in the 1981-1983 timeframe (the exact year escape me), IBM donated some equipment to the School of Information and Computer Science (now the College of Computing) at Georgia Tech.

Included in this donation were 3 IBM Series 1 machines. Each of these was equipped, in the upper right-hand corner, with a bright red "Emergency Pull" switch.

Those of us using the Primes, Vaxen, and AT&T gear made jokes about the switch

(and about the IBM gear in general). Little did we know at first....

In the 7 years I was at Tech, I saw lots of equipment pass through the lab. We had, other than the IBM gear, AT&T 3bX's, Primes, HP systems, Data General, Xerox, Symbolics, and various other bits & pieces, including lots of telecommunications gear. In all that time, with over 100 machines, we had 4 fires in the lab.

One was caused when a CDC disk drive on one of our Prime 400 machines had its bearings seize (the disk had been on-line for something like 6 years with no maintenance, and the machine had been up for over a year without a reboot, as I remember -- the most reliable collection of hardware I've ever seen). The fire was well-behaved and put itself out; the Prime continued to run, but the first command typed at the console that caused a page fault caused a panic halt.

The other 3 fires were all IBM Series 1 machines. These weren't just little blow-a-capacitor-and-create-smoke fires, either. They were burn-up-the-power-supply type fires that took controller boards with them. One was so complete, we had to dispose of the machine as there was too little to salvage, as I remember.

We concluded that the pulls were not there out of tradition, but were installed because experience or choice with the design indicated that they were necessary to deal with the tendency towards self-immolation.

Ever since then, I have believed that any machine that has an emergency pull probably needs one. Computers that are likely to catch fire or electrocute me (see the old Risks posting about the jealous computer electrocuting the scientist) are not high on my list of preferred computing platforms. I also tend to flinch when a sales-critter tells me his cpu really smokes; it took me a while to even tolerate the idea of using a SPARC. :-)

Gene Spafford, NSF/Purdue/U of Florida Software Engineering Research Center, Dept. of Computer Sciences, Purdue University, W. Lafayette IN 47907-1398

Re: Four-digit address causes NYC death (Pellett, RISKS-11.60)

Scott Barman <scott@nbc1.ge.com>
Thu, 16 May 91 13:56:27 EDT

The original posting (Nilges, RISKS-11.55) came from a report aired on WNBC in New York. To find out more about this, I spoke with a director I know who is familiar with the story (he did not work on the story and the original reporter/director is out on assignment). I was reminded of something that Mr. Ravin forgets; a large parts of Queens was not fully developed until after World War II. There are a lot of addresses that look like they would cause a conflict when given, such as an 83rd Street vs an 83rd Avenue address as well as cross streets with names (the incident in the report happened off of Queens Blvd.). Over that time, the city assigned different address numbers on some of these and nearby streets to hopefully avoid conflicts and give emergency services a better chance of finding these places. Unfortunatly, over the years the city has never properly adjusted the "official" city specifications for

addresses and this specification is what they used for designing the 911 system.

Bob Frankston <Bob_Frankston%Slate_Corporation@mcimail.com> writes:
>Representation is a nontrivial issue. While it may be "obvious" that one
>should allow for five digit addresses, what about fractional addresses due to
>subdivided lots (how do you say "384 3/8e 1St SW" in ASCII, how does it
>sort?? Apartment addresses? Alternative addresses (6th Ave vs Avenue of the
>Americas)? Why not require full color graphics and then discover you can't
>present it on a belt-mounted radio?

Curious about the 6th Avenue vs. Avenue of the Americas differences (since part of this building is on 6th Ave.), we contacted the NYC Emergency Services Bureau and were told that the system understands the addresses at 6th Avenue and the operators are trained to use 6th Avenue instead of Avenue of the Americas in the computer and when dispatching assistance.

Oh, and there are no "3/8" addresses. There are halves and they are addressed in the system (albeit badly I have been informed). Also, NYC does not use compass directions like SE or SW but does used an address like "40 W. 50th Street" and these are addressed as well.

Another problem the report didn't cover, and nobody did either, is that there is a problem (again in Queens) with Harry Van Arsdale Drive. This street name was changed a few years ago from Jewel Avenue and is entered in the Emergency Services Bureau computer as two different addresses because there is no way to properly link these addresses in that system. So a person can call and report a fire at (for example) 80-15 Jewel Avenue and another person can call and report one at 80-15 Harry Van Arsdale Drive and two dispatches will be sent. We were told the one time something like this happened, the local fire house understood it to be the same address eventhough the 911 operators didn't. ESB uses the same procedure as the 6th Ave vs. Ave. of the Americas problem but since this is a newer change and since some of the ESB operators are not from NYC (20% are New Jersey residents) they leave it up to area fire and police not to dupicate the calls. This is something ESB is looking to fix.

scott barman

Transactional Records Acess Clearinghouse

Larry Hunter <hunter@nlm.nih.gov>
Fri, 17 May 91 10:07:41 EDT

I have been inundated with messages asking me for more information about David Burnham's Transactional Records Access Clearinghouse (note the correction of the name from my posting in RISKS-11.60). Here is contact information for those of you who would like to know more about the organization:

Transactional Records Access Clearinghouse, 999 Pennsylvania Ave., SE, Suite 303, Washington, DC 20003 (202) 544-8722

Search RISKS using swish-e

THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

ACM Committee on Computers and Public Policy, Peter G. Neumann, moderator

Volume 11: Issue 70

Wednesday 22 May 1991

Contents

Shuttle Columbia delayed

"Peter G. Neumann" <neumann@chiron.csl.sri.com>
Wed, 22 May 91 19:16:30 PDT

NASA halted the space shuttle Columbia's launch countdown on 21 May 91 because of ``bad computer parts and fuel sensors''. ``The parts to be replaced include nine fuel temperature sensors, one of the five main computers and one of the 23 units that link the main computers with shuttle components.'' Retry is scheduled for 28 May. [San Francisco Chronicle, 22 May 91, p.A8]

Patriot Lapse and Software Failure

<cdp!mrotenberg@labrea.Stanford.EDU>
Tue, 21 May 91 17:59:03 PDT

The New York Times reported that computer failure was responsible for the failure of a Patriot missle to stop a scud missle that hit an American military barracks in Dhahran. According to the Times story, the Patriot's radar system was rendered inoperable by the computer failure.

According to army officials, "an unforseen combination of `dozens' of variables -- including the Scud's speed, altitude and trajectory -- had caused the radar system's failure. . . . [this case was] an anomaly that never showed up in thousands of hours of testing."

The Times article states that "During the war, American military officers were reluctant to discuss any weapon failings. But even after the cease-fire, many officers were averse to say anything that might tarnish the one-sided allied victory over Baghdad's forces."

["Army is Blaming Patriot's Computer For Failure to Stop Dhahran Scud" -- New York Times, May 20, 1991, A6]

Marc Rotenberg, CPSR Washington Office.

[The NY Times front-page story (Eric Schmitt, 20 May 91) cited 28 dead in a U.S. military barracks in Saudi Arabia on 25 Feb 91, the single worst American casualty in the war. Apparently the radar never saw the incoming missile because of a computer failure, permitting the Scud to land intact. (This latest report corrected an earlier report, which suggested that the Scud had broken up into pieces without a Patriot having been launched.) An AP article on 21 May cited 29 killed and 97 wounded. PGN]

AP reports software bug caused Patriot failure

Gene Spafford <spaf@cs.purdue.edu>
21 May 91 14:17:00 GMT

[...] The article concludes with: "The Army source said the glitch arose because the computers had been running continuously for four days."

FOUR DAYS!? I sure hope that the article is wrong or the person being quoted didn't understand. There is no excuse for a system that fails if it isn't rebooted every few days, especially when it is in such a critical application.

And these are the guys who claim they can develop a permanent missile shield for SDI? Just whose side are they on?

Gene Spafford, Dept. of Computer Sciences, Purdue University, W. Lafayette IN 47907-1398 Internet: spaf@cs.purdue.edu phone: (317) 494-7825

Let the Games Begin! [Airline discounting practices]

Jerry Leichter <leichter@lrw.com>
Tue, 21 May 91 08:02:23 EDT

In a recent RISKS, I reported on the airline practice of adjusting the number of discount seats on flights on a continuous basis. This practice, known as yield management (I mistakenly called it load management), allows them to maximize profit. I also noted that some travel agencies were starting to respond to yield management - only possible because of the massive computational resources available to the airlines - with computers of their own, which continuously search for good deals.

Well, for every offense there's a defense, and for every defense an offense. The Wall Street Journal (Monday, 20-May, page B1: "Agents Rankle Airlines With Fare-Checking Programs") reports on the next exchange in this battle: The airlines are changing the fee structure for their reservation systems in an attempt to shut down the scanners. Traditionally, access to the systems has been on a flat fee basis. Now, the airlines are beginning to charge per inquiry beyond a certain monthly quota. The fees are about a penny per inquiry, but that adds up - one agency will reportedly run up fees well in excess of $100,000 a year.

The airlines, of course, claim the fees are being imposed for a different reason - they say the programs are putting excessive load on their systems and adding to their cost of operation.

The developers of the scanners are modifying them to make fewer inquiries, and will also try to pass on the costs to their customers. However, some experts in the business believe the airlines will win this war, and that the scanner programs have no future.

Michael Levine, dean of Yale's School of Organization and Management and a former CAB official, is quoted saying "You have to be concerned about the consumer's perspective. Consumers ought to have the right to shop, and nothing should impeded that." I suspect he may have framed one of the next big computer law and regulation issues.

-- Jerry

Yet another Push The Button story

Jonathan Rice <rice@willow.cray.com>
Mon, 20 May 91 9:54:51 CDT

Control Data CYBER 170 series mainframes, and at least one generation of their descendants, were watched over by a box called the TMPC: Temperature Monitor and Power Control. One pushbutton on this device, usually mounted conveniently close to the operator's console, was labeled "LAMP TEST." Unfortunately, pressing the button not only illuminated each of the failure modes on the diagnostic panel, but actually raised all of the alarm signals -- high temperature, motor/generator failure, etc. The mainframe would shut down to the tune of the world's awfullest buzzer and the curses of the operators.

Every CDC site I ever visited, and that was a fair number, had a "lamp test" story to tell. And many had ordered a blank keycap to replace the original.

To add to the growing collection of morals, then: emergency shutdown switches

should not be labeled with the equivalent of "Push Me."

Jonathan C. Rice | Internet: rice@cray.com | UUCP: uunet!cray!rice

HHS malpractice data bank start-up problems

Richard Guy <guy@PRAM.CS.UCLA.EDU>
Mon, 20 May 91 14:48:46 PDT

"The malpractice data bank is turning into a Frankenstein" by Mark Holoweiko, Senior Editor, _Medical Economics_, May 6, 1991 [a medical trade journal sent unsolicited to members of the American Medical Association]

Despite warnings by the General Accounting Office that it was nowhere near ready to operate, the National Practioner Data Bank was opened last Sept. 1 by the Department of Health and Human Services. By law, medicine's dirty laundry began pouring into a Camarillo, Falif., computer facility run by Unisys Corp., which had contracted with HHS to handle the project.

Malpractice insurers, hospitals, state lcensing boards, and other "health-care entities" started mailing in information about doctors and dentists--mostly reports of payouts on professional-liability claims, and adverse credentialing and licensure decisions. Simultaneously, hospitals began querying the data bank for information on medical staff members and applicants. In addition, licensing boards, medical societies, and other oentities, such as certian HMOs and group practices, became eligible to query the data bank.

Only six weeks later, it appeared that the GAO's fears had already been borne out. The dirty laundry was piling up at the door. The software that Unisys was supposed to develop either wasn't in place or didn't work, so the company was trying to cope manually with the deluge of information and requests.

The backlog of quieries numbered in the tens of thousands, procuding eight- to 10-week delays in response time. In the absence of a data-bank reply, hospitals, licensing boards, and others wondered if they could safely give a doctor the green light to practice.

To complicate matter,s both the GAO and the HHS Office of the Inspector General raised concerns about theconfidentiality of the data; hundreds of physicians lodged disputes over the workding of reports about them; and Unisys exp0erienced major cost overruns and demanded more money. Meanwhile, in light of GAO criticisms, Congress threatened to cut off funds that had already been appropriated for 1991. Finally, Unisys had such big problems of its own that its solvency seemed questionable.

Will the data bank ever work? "Since we opened Sept. 1, the bank has been operating as we had hoped it would," insists Robert G. Harmon, M.D., administrator of HHS' Health Resources and Services Administration, which oversees the bank. But few share Harmon's view.

"They're having a terrible time," says James S. Todd, M.D., executive vice

president of the American Medical Association and a member of the data-bank executive committee, which advises Unisys on the project. "The project is really in jeopardy at this point," declares another committee member.

EGGS WERE LAID AT THE PLANNING STAGE

"The people involved in designing the project didn't know what they were doing," says an executive committee member. "They didn't understand insurance, medical malpractice, computers, the basic components of the whole project. And they got themselves into a real mess."

Back in the psring of 1990, the GAO examined the data bank's development by HRSA and Unisys, the npresented a report to HHS bluntly title, "National health practitioner data bank has not been well-managed." AMong other things, the GAO said:
>"No one person has been accountable. ... [sic] Instead, accountability is shared by at least 14 HRSA officials." And none of the 14 had "the necessary training and experience" to ensure that the system would meet specifications. COnsequently, HRSA was relying on Unisys "to carry out the critical management functions of establishing plans, schedules, and budgets, and ... [sic] testing computer programs before they are implemented."
>The project's total cost might increas from $15.8 million to $25 million.
>"HRSA cannot ensure that appropriate security measures will be installed to prevent unauthorized access and manipulation of data-bank information," becuase it hadn't complied with governement regulations and conducted a risk analysis.

GAO recommended that the September 1990 opening be postponed.

In response, HRSA engaged governement computer experts to evaluate security and test the software. They found several weaknesses. FOr example, the system wasn't equipped to detect aunauthorized changes to the data and trace them back to the culprits.

Nevertheless, through the Office of Inspector General, HHS maintained that "the management processes employed by HRSA are both reasonable and adequate," and the confidentiality concerns have been adequately addressed." It pushed for the Sept. 1 launch. Adding that Unisys' request for another $9 million was "out of line" and had "subsequently been withdrawn by the contractor," HHS asserted that the project was on schedule and within budget.

The House appropriations COmmittee temporarily withheld data-bank funds for fiscal 1991 pending assurances from HHS Secretary Louis W. Sullivan that the deficiencies cited by GAO had been corrected. But government computer experts certified the system as secure, the funds were released, and HHS forged ahead and opened the bank.

THE FINANCIAL SITUATION IS PRECARIOUS
[omitted; operating expense overruns; Unisys losses]

BACKLOGS ARE HOLDING UP CREDENTIALS

The first order of business was to clear the logjam. As of February, there was a backlog of about 500 reports to enter into the system, and 108,000 queries to

answer.

"There's been an eight- to 10-week wait for responses to queries from hospitals," says James Todd. "That's a long time when you're talking about credentialing. Take a new physician coming to a hospital. The hospital has to query the bank before it can grant him privileges. Does the physician have to sit and do nothing for two months? Or, if he starts practicing without a response from the data bank, what is the hospital's liability?"

According to the AMA, some doctos have, indeed, complained that hospitals refused to grant them privileges until hearing from the data bank. But the law creating the data bank seems to contain a loophole: All it stipulates is that a hospital must *query* [emphasis original] the bank before it grants privileges; it doesn't have to wait for a response.

Accordingly, the American Hospital Association's general counsel, Fredric Entin, advised hospitals to proceed with granting or renewing privileges. "I've heard that some hospitals have let the delay paralyze them, but I suspect it's very few," say Entin, who's a member of the executive committee.

The situation is similarly discouragin for state licensing boards, says James R. Winn, M.D., executive vice president of the Federation of State Medical Boards: "Most are querying the data bank before issuing licenses, but getting information has been very slow."

As this issue went to press, however, Fitzhugh Mullan, M.D., HRSA's project director for the data bank, told us that the backlogs and delays had been reduced to "zero."

DOCTORS ARE DISPUTING THE REPORTS

Reports to the data bank are supposed to include a description of the practitioner's alledged wrongdoing. This narrative is limited to a maximum of 600 characters, or about 50 words. [... example and further discussion of wording dispute procedures omitted]

If the data bank ruins a doctor's reputation by disseminating erroneous information, can the physician sue Unisys or HHS for damages? "I don't believe so," says AHA General Counsel Fred Entin. "The governement has sovereign immunity. That means that you have to get the government's permission before you can sue it. And since Unisys is acting as a government contractor, I think this immunity would extend to the company as well."

CONFIDENTIALITY IS HIGHLY QUESTIONABLE

"I feel that the data bank is secure," says HRSA's Robert Harmon. "We have numerous safeguards built into the computer systems. The computers themselves are housed in a secure facility that does work for the Pentagon. Personnel have to be cleared. There are stiff penalties for improper use of the information." (Each violation is punishable, via the IG's office, by a civil montary penalty of up to $10,000.)

But that's not the issue, says Ronald S. Gass, senior counsel for the American

Insurance Association and a data-bank committee member. "The facility in California has ultra-high security, guard dogs, barbed wire, and all that stuff," he agrees. "But is it sending information out the right way?"

As of February, according to government figures, about 12,500 organizations had been authorized to query (or, in the case of malpractice insurers, just report to) the data bank. When we added up all the nation's hospitals, HMOs, malpractice insurers, and physician and nurse licensing boards, the total fell short of 12,500 by roughly 5,000. Surely, hundreds of these are group practices, professional socities, and preferred provider organizations. But exactly who they are is anyone's guess. Furthermore, so many and varying types of organizations are legally entitled to query the bank that leaks seem inevitable.

[more discussion of "self-certification" access loopholes; also discussion of an emerging practice of requiring physicians to produce data-bank reports as a part of credentialing process.]

THERE ARE OTHER HOLES IN THE SYSTEM

[discussion of hospital peer review decisions, confidentiality, liability of peer reviewers ommitted]

MORE DEMANDS MAY OVERTAX THE SYSTEM

As currently programmed, the bank's computers can't distinguish medical doctors from other practitioners, or tell what percentage of reports concern malpractice payouts and disciplinary actions.

A policy analyst with HRSA acknowledges that Unisys "can't even tell us how many hospitals have queried," let alone how many HMOs, insurers, group practices, and others have access. "This is the office that sets the policy," she continues. "Even *we*[emphasis original] don't have access to that information."

Insurers for all licensed health practitioners--not just doctors and dentists--are now supposed to be reporting payouts on malpractice claims. Are they? "At this point, the system is not capable of pulling that out," the analyst admits.

[further discussion of which government agencies have access to the data bank; legislation confusion over the extent of data the bank is to contain]

THE PROGNOSIS IS GUARDED FOR NOW

[complaints about query costs ($3 now, maybe $6 soon), paperwork burden]

One big flaw may be the type of information being gathered. "While the data on disciplinary actions is pretty current," notes Larry Smarr, "the stuff on malpractice claims is old because claims are usually paid six or seven years after the events that precipitated them. So I don't know how this is ever going to be of value in identifying problem physicians."

A concurring view comes from Sara C. Charls, M.D., who represents the Council of Medical Specialty Societies on the executive committee: "The inclusion of malpractice cases--especially those settled for small amounts--waters down the whole purpose. The estimate is that malpractice cases

comprise 80 percent of the reports to the data bank, and they're the least reliable indication of physician competence. I think an enormous amount of money is going into a system that will be paralyzed by its own weight."

Re: SCIENTIFIC AMERICAN SIDEBAR

"Willis H. Ware" <willis@rand.org>
Tue, 21 May 91 10:56:06 PDT

With respect to the sidebar on page 27 of the June Scientific American which discusses privacy and about which there have been a few messages to RISKS FORUM, I'm afraid that in the process of getting from my remarks during a panel session at the CFP Conference into print some distortions unfortunately occurred. Paul Wallich, by-lined for the article, is someone that I talk with from time to time but it wasn't quite as he reported. Clarification is warranted.

I said explicitly that the U.S. had used a piecemeal approach with minimal privacy laws in contrast to the European approach of a comprehensive law that typically creates an all-powerful data protection body of some sort and generally with a data-protection commissioner. I did use the phrase "nickle and dime" as a surrogate for "piecemal and minimal", not as indicative of deliberate actions to stonewall or kill off privacy. The appendage "to death" crept in, is not mine and changed the meaning.

I did not say that the commercial sector is THE enemy but rather that it was time to consider it as an additional opponent to privacy along with government, which was the early focus of concern because of its widespread control over entitlement programs.

I did say "I've watched nothing happen" because nothing has happened for privacy in 17 years. At best the country has resisted erosion of the positive actions of the 1970s. I think I did not admit to depression but on the contrary, I said explicitly that I would not quit the game and would continue to seek solutions.

It is because of the U.S. failure to put in place comprehensive privacy legislation that Simon Davies [Australia] did indeed say [as reported] that the U.S. is an embarrassment to the rest of the world.

I wish that Mr. Wallich would have picked up the much more important point that I hope was made clearly to the Conference audience. The only basis that I can think of for structuring the privacy issue is to regard it as a social equity problem in which the stakeholders include not only every individual but also private sector organizations and government. A forum is needed to identify, compare, discuss and balance off the obviously competing interests of the different parties. Where to find such a forum and how to conduct the dialogue is indeed an awkward problem presently without an answer.

Willis H. Ware

2ND CALL, COMPUTING & VALUES CONFERENCE, AUG 12-16

Walter Maner <maner@bgsuvax.UUCP>
21 May 91 06:47:32 GMT

The National Conference on Computing and Values will convene August 12-16, 1991, in New Haven, CT. N C C V / 91 is a project of the National Science Foundation and the Research Center on Computing and Society. Specific themes (tracks) include

- Computer Privacy & Confidentiality
- Computer Security & Crime
- Ownership of Software & Intellectual Property
- Equity & Access to Computing Resources
- Teaching Computing & Values
- Policy Issues in the Campus Computing Environment

The workshop structure of the conference limits participation to approximately 400 registrants, but space *IS* still available at this time (mid-May).

Confirmed speakers include Ronald E. Anderson, Daniel Appleman, John Perry Barlow, Tora Bikson, Della Bonnette, Leslie Burkholder, Terrell Ward Bynum, David Carey, Jacques N. Catudal, Gary Chapman, Marvin Croy, Charles E. M. Dunlop, Batya Friedman, Donald Gotterbarn, Barbara Heinisch, Deborah Johnson, Mitch Kapor, John Ladd, Marianne LaFrance, Ann-Marie Lancaster, Doris Lidtke, Walter Maner, Diane Martin, Keith Miller, James H. Moor, William Hugh Murray, Peter Neumann, George Nicholson, Helen Nissenbaum, Judith Perolle, Amy Rubin, Sanford Sherizen, John Snapper, Richard Stallman, T. C. Ting, Willis Ware, Terry Winograd, and Richard A. Wright.

The registration fee is low ($175) and deeply discounted air fares are available into New Haven.

To request a registration packet, please send your name, your email AND paper mail addresses to ...
BITNet MANER@BGSUOPIE.BITNET InterNet maner@andy.bgsu.edu (129.1.1.2)

or, by fax (419) 372-8061
or, by phone (419) 372-8719 (answering machine), (419) 372-2337 (secretary)
or, by regular mail, Professor Walter Maner Dept. of Computer Science
Bowling Green State University Bowling Green, OH 43403 USA

Terrell Ward Bynum and Walter Maner, Conference Co-chairs

InterNet maner@andy.bgsu.edu (129.1.1.2) | BGSU, Comp Science Dept
Relays maner%bgsu.edu@relay.cs.net | Bowling Green, OH 43403
maner%bgsu.edu@nsfnet-relay.ac.uk | 419/372-2337 Secretary
BITNet MANER@BGSUOPIE | 419/372-8061 Fax

Report problems with the web pages to the maintainer

Search RISKS using swish-e

THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

ACM Committee on Computers and Public Policy, Peter G. Neumann, moderator

Volume 11: Issue 71

Thursday 23 May 1991

Contents

The RISKS of Posting to the Net

<mmm@cup.portal.com>
Thu, 23 May 91 11:58:07 PDT

I just had an interesting visit from the FBI. It seems that a posting I made to sci.space several months ago had filtered through channels, caused the FBI to open (or re-open) a file on me, and an agent wanted to interview me, which I did voluntarily.

My posting concerned destruct systems for missiles. I had had a chance to look at the manual on the destruct system used on the Poseidon and Polaris A3 missiles, and was shocked at the vulnerability of the system which triggers the system. In my posting, I commented that the system seemed less secure than

many garage-door openers. It uses a set of three tones, in which two tones are presented, then one tone is taken away and the third tone is applied. The only classified parts of the system are the frequencies of the second and third tones.

On the net, I asked whether tone control systems like this are still used for missile destruct systems. By e-mail, I received an answer from a person who was currently designing a destruct system, and he indeed confirmed that not only are tone-control destruct systems still used, they are a requirement of some test ranges. (However, he thought it would be difficult to send a bogus destruct command because of the need to blot out one of the tones which is transmitted continuously from ground control; it would be far easier to insert a bogus flight control command and send the missile toward a city.)

A few months later, I received a message from my sysop asking me to call a person at Patrick Air Force Base who wanted to get in touch with me. This guy was real concerned that I had revealed "sensitive" information. He said he kept his copy of my posting in his safe! I guess he didn't know that it had already been distributed throughout the industrialized world. He didn't want to say anything about the subject over the phone. He asked whether I would be willing to be interviewed by an investigator. I agreed, and he said I would be contacted within 24 hours by someone locally. That was the last I heard of him. I suppose he talked to someone who knew more about destruct systems, and was reassured that it isn't possible because it hasn't happened yet.

Two days ago, more than half a year after my original posting, I got a message that someone from the Palo Alto office of the FBI wanted to talk to me. I called him, and we agreed to meet this morning. He didn't seem too concerned with the technical aspects of my posting -- I guess he also had his own experts to consult. He mostly seemed to be checking me out to see if I was plotting to blow up a missile. He was also very interested in how the net works. I told him all about the net. He wanted to know if there was any sort of censorship or control over what goes on the net, and I explained it was mostly after-the-fact control, for example if you post a commercial advertisement the management of your site will get a ton of e-mail asking that your account be cancelled.

He asked whether someone could post an offer for $10,000 for blueprints of a missile or something, and I said there isn't any sort of censorship that would prevent that sort of thing. But the closest thing to a request for information on performing a crime that I knew of was a couple years ago when someone asked in the chemistry newsgroup about methods for electrically igniting a chemical. I told him about the controversy that caused, though I omitted my role in answering the original poster's question :-)

I also told him about newsgroups like alt.drugs, rec.pyrotech, etc. He took copious notes. He asked about the equipment needed to access the net. I told him about computers and modems and Portal. I should contact Portal management to see if I get a bonus if he signs up as a customer :-)

The only surprise came at the end of the interview. He asked if I had any questions. I said I was curious how my posting ended up in his hands. Before he could answer, I said I suppose you were contacted by that guy at Patrick Air Force Base. This surprised him, and he said he knew of no involvement by

anyone at Patrick Air Force Base. I asked how he _did_ know about my posting, and he said he couldn't answer that. I then went on to tell him about the controversy over Uunet, and their role in supplying archives of Usenet traffic on tape to the FBI, and he seemed surprised by that also.

So what's the RISK here? None to me, because I was a perfectly innocent party. I suppose some people would be really concerned to learn that their postings to the net are being monitored for possible illegal activity. But I would be far more concerned if they weren't. The fact that two independent investigations were started is reassuring to me, because it shows that the government is not totally brain-dead with regard to possible threats to their big projects. Certainly if _I_ were FBI director, I would consider Usenet to be a great resource. I'd learn all about computer crime, recreational drugs that aren't illegal yet, low-tech ways of building bombs, how to contact Earth First!, etc., etc.

If SB266 wants plaintext, give them plaintext...

Peter Wayner <wayner@cs.cornell.edu>
Thu, 23 May 91 16:17:23 -0400

There has been plenty of discussion about SB266 requiring all communication equipment to provide the plaintext to the government on demand. Well, I've decided if they want plaintext, give them plaintext. I've written a program that will convert any file into strings from a context-free grammar. The bits are recovered by parsing. To test it's viability, I created two grammars and a program to do the work.

The first converts any file into the radio commentary of a baseball game between two teams, The Blogs and the Whappers. Could something as American as baseball be hiding something?

The second converts a file into something approximating a speech by Neil Kinnock . I chose Neil Kinnock because SB266's sponsor, Joe Biden, is fond of borrowing liberally from Mr. Kinnock's impressive oratory. Unfortunately, the only really substantive chunks of Mr. Kinnock's speeches I could find were from a NYT article by Maureen Dowd in 1987 about the striking similarities between the speeches of Joe Biden and Neil Kinnock. The limited sample leads to a "broken record" effect. (The libraries in America don't seem to contain collected speeches by Mr. Kinnock. If anyone has a video tape of his impressive 10 minute commercial of Brahms and anti-Bromides, I'd love to see it.)

I managed to encode information using this text by slightly permuting the word choices. I've been wondering if Senator Biden wasn't doing the same thing when he didn't quote verbatim. Perhaps he was sending messages to someone?

My apologies to Mr. Kinnock for mutilating his careful diction and rhythm.

If anyone in the United States would like to experiment with the programs, please drop me a line. I'll send you the source code. It is written Think Pascal 3.0 for the Mac, but it should be a breeze to convert to other Pascal's or even C. The offer only extends to electronic addresses in the United States

because the Commerace department restricts the distribution of cryptographic protocols beyond the borders. The security of the system is a bit hard to assess (breaking it is, in some senses, a PSPACE-complete problem), so I'd rather abide by an annoying rule than spend time in the can. If you would rather receive it by disk, send me one with a properly franked envelope, and I'll mail it out.

If you want a copy of a Tech Report describing the topic, send me a paper address and I'll send it out. This document can cross borders. Thank god for the first amendment.

Finally, here are two examples of the program at work:

Baseball

It's time for another game between the Whappers and the Blogs in scenic downtown Blovonia . I've just got to say that the Blog fans have come to support their team and rant and rave . Let's get going ! Another new inning . Ain't life great, Ted ? Yup. How about those players . The pitcher spits. Prince Albert von Carmicheal comes to the plate . He's trying the curveball . He pops it up to Harrison "Harry" Hanihan . One out against the Whappers. Now, Parry Posteriority swings the baseball bat to stretch and enters the batter's box . Here we go . OOOh, that's almost in the dirt . Definitely a ball . The next pitch is a bouncing knuckleball . Short and away . The umpire calls a ball . It's a change-up . and it's ... La Bomba ! HomeRun ! Yup, got to love this stadium. Now, Mark Cloud swings the baseball bat to stretch and enters the batter's box . Yeah. He's uncorking a toaster . No contact in Mudsville ! It's a fastball with wings . No wood on that one . He's uncorking what looks like a spitball . Whooooosh! Strike ! He's out of there . These are the times that make baseball special . Now, Parry Posteriority swings the baseball bat to stretch and enters the batter's box . Another fastball . No contact on that one . A full windup and it's a split-fingered fastball . He pops it up to Orville Baskethands . Well, that's the end of their chances in this inning, Rich .

Neil Kinnock

Why were the Coal Mines all my ancestors had ? These people who could write poetry ? My people who could make wonderful things with their hands ? Why didn't they get the chance ? Were they too weak? The people who would work underground for 8 hours and come out to play football for the evening ? Do you think that they didn't get what we had because they didn't have the drive ? Never . It was because they never had a platform on which to stand . Why am I the first man in my family to go to University ? Was it because our ancestors were too thick ? Why were my ancestors shut out of life ? My people who could dream dreams and recite poetry and dance and make wonderful things with their hands and dream dreams ? My parents who could make wonderful things with their hands and sing and write epic poems and make beautiful things and see visions ? Why didn't they get the chance ? Were they too weak? Those people who worked underground for 8 hours and come up to play football ? Does anybody really think that they didn't get what we had because they didn't have the stamina ?

No . There was no platform on which they could stand .

Both of these examples are just small portions of the result of encoding the message:

Paul is dead! I am the walrus!
Buy something right now. Don't shoplift. Buy! Buy!
Here are the plans to the Overthruster, Sergei.
Yoyodyne forever.

Voting By Phone

James K. Huggins <huggins@zip.eecs.umich.edu>
Thu, 23 May 91 12:25:35 EDT

This afternoon, during the Senate's debate on the Campaign Finance Reform Act, Senator Robert Dole (R-Kansas) offered an amendment (which was agreed to by the Senate) directing the Federal Election Commission to conduct a study regarding the feasibility of allowing disabled voters to vote by telephone in federal elections. The main motivation behind the amendment was to provide easier ways to vote for disabled Americans who may find it difficult to reach a polling place. The amendment does not require the FEC to immediately implement voting by phone, but only to study it.

Previous issues of RISKS have discussed the risks of voting by phone at length, but one risk stands out in this particular case. If the danger of coerced votes in "normal" phone votes is substantial, I believe it is even higher in this situation, where the threat of physical violence against the physically disabled voter would be greater than normal.

Jim Huggins, Univ. of Michigan (huggins@zip.eecs.umich.edu)

Using commercial databases to augment Government surveillance

<pine_ridge%oak.span@Sdsc.Edu>
Thu, 23 May 91 11:25:34 GMT

Buried in an article in the 23-May-91 Wall Street Journal was a reference to an interesting computer-related risk. The article, entitled "Travelers From Abroad Face Summer of Extra-Long Delays at U.S. Airports," reported that incoming travelers may face delays of up to 5 hours in clearing immigration at some airports.

Previously, "selective screening" and "citizen bypass" plans have been used by customs and immigration officials to expedite inspections of arriving passengers. The Immigration and Naturalization Service (INS) now is taking the position that all persons entering the U.S. must be checked. After interviewing Michael Cronin, assistant INS commissioner for inspection, the WSJ reported, "He notes that the U.S., unlike many other countries where

immigration inspections are looser, doesn't require national identification cards or have a national police force to stop people on the street and enforce immigration laws. Thus, he argues, port of entry must keep tight control."

One of these controls is the new Advanced Passenger Information Program. Under this program, airlines transmit data about arriving passengers to the INS before passengers arrive. The government adds this information to its databases and uses these databases to help determine who gets inspected. This program is currently in place for U.S.-Japan flights and will be implemented soon for U.S.-European flights.

I am unhappy with the idea of the government augmenting its surveillance of me by tapping commercial databases. What other uses will they make of this information? What's next? Should the government get copies of my phone bills to see if I'm talking to the wrong people?

An aside: I find the treatment of foreign travelers by the INS embarrassing when compared to the way I am treated by officials in other countries. The evil hacker-condoning Dutch, for example, seem to process everyone coming in to their country with courtesy, efficiency, and fairness. I've never noticed Dutch police randomly stopping people on the street and examing their identity papers, either.

Brad Dolan pine_ridge%oak.span@sds.sdsc.edu B.DOLAN (GEnie)

UPS & Electronic Signatures

Alex Bangs -- bangsal@ornl.gov <abg@mars.EPM.ORNL.GOV>
Thu, 23 May 91 07:59:32 EDT

For those of you who don't sign for UPS packages, UPS is now switching over to an electronic clipboard for their drivers. This device is called the Delivery Information Acquisition Device (DIAD) [_Network World_, May 6, p. 15]. I had my first experience with one the other day when a package was delivered. The most unique part of this device is a pad which is signed by the customer with a stylus and stores the signature electronically. You can see your signature appear on the DIAD's LCD display.

I visited UPS R&D about a year ago when they were still testing this device. They explained the logic behind this. Not only does it get rid of paper for signatures, but when the information is downloaded into a mainframe, it can be used by a central customer service organization. When a customer calls in claiming a package was not delivered, they can look it up on the computer and check if it was delivered, and who signed for it (not noting, however, that many people's signatures are unreadable!).

So, how many of you like the idea of your signature being stored electronically somewhere in the bowels of someone else's computer?

Alex L. Bangs, Oak Ridge National Laboratory/CESAR,
Autonomous Robotic Systems Group bangsal@ornl.gov

Re: Yet another Push The Button story

Tom Coradeschi <tcora@PICA.ARMY.MIL>
Thu, 23 May 91 12:20:05 EDT

This thread reminds me of a suggestion a co-worker made for our new laboratory (Lots of high energy capacitors, switches, etc). We would install a large red pushbutton, with a lighted label above it reading "Push to Test". When the button was pushed, the label would change to "Release to Detonate".

Well, I liked it... tom coradeschi

Re: (Bogus) IBM red switch

"John A. Pershing Jr." <pershng@watson.ibm.com>
Tue, 21 May 91 10:59:56 EDT

Note that the 1403 printer itself also had a "STOP" button on its control panel (I don't remember if it was red, or some other color). Amazingly enough, if the printer went into the "high speed paper slew" mode due to an -- er, -- unfortunate choice of carriage control character, the printer's "STOP" button would have NO EFFECT WHATSOEVER! (I discovered this when the printer was loaded with continuous-form payroll checks!)

Unfortunately, the function of the "STOP" button was to tell the printer to stop accepting commands from the channel *after* the completion of the current command (e.g., "skip to channel 5"). Sigh...

(There *was* a second button on the panel labelled "Carriage Stop", or something like that, which *would* stop the fountain of paper. Not immediately obvious to a panicked junior programmer...)

John Pershing, IBM Research, Yorktown Heights

Re: Privacy

Richard Johnson <richard@oresoft.com>
Mon, 20 May 91 8:14:46 PDT

Mary Culnan ("Of Two Minds About Privacy" RISKS 11.69) and Jerry Leichter ("The Death of Privacy?" RISKS 11.69) detail some of the problems associated with automated systems that detail specific information about our personal and financial lives. To summarize:

1) Undesired access to data
2) Undesired manipulation of data
3) Undesired offerings of data (Mary) and
4) Undesired large-scale changes of public opinion (Jerry)

{nota bene: That is my reading - you might have meant something else. Also, by "undesired" I mean "undesired by the subject"

(me, specifically).}

It seems this is just the tip of the iceberg, though. Recently released footage from the Persian Gulf conflict show a sophisticated airborne battle-management system capable of spotting movement, location, and identification of literally everything within several hundred miles.

Several states are experimenting with bar codes for vehicle location, speed detection, and identification. While officially not for criminal investigation purposes, I doubt most anyone would object to a search of the records to locate the perpetrator of say, a felony hit-and-run.

Birth, death, marriage, licenses, education, service, and major property occasions are all publicly recorded, and often _required_.

Our employers often know where to find us, even when we are not at work. Our neighbors often know the roads we use to drive to work. Our grocers often know the days we get paid, and the times we like to shop.

The problem is not just technology. The problem is how much an individual is willing to waive control of information about her (him) self. If we don't actively guard our privacy, we shall surely fall prey to those who would profit from that information -- perhaps at our expense.

Richard Johnson

Re: The Death of Privacy?

Email Mujahideen <Robert.Allen@eng.sun.com>
Mon, 20 May 91 09:22:59 PDT

To my mind there is a more serious problem responsible for our loss of privacy (not to mention other rights). It's the attitudes towards convenience.

Every time you use one of the Electronic Fund Transfer (EFT) devices at a Lucky's store, gas station, etc., you are giving up significant portions of your privacy. By buying gas this way someone can closely figure your driving habits: did you go somewhere this weekend? Where did you go (where did you use EFT to buy gas?)? What kind of mileage did you get? Is it possible you took a side trip where you used gas, but didn't buy any until later? What kind of food do you buy (I'm not sure if this is tracked)? How much do you normally spend on food, versus getting cash back? Why do you get so much cash back from a grocery store instead of a bank (trying to hide something?)?

We are well on our way to a cashless society. I predict that it will eventually be illegal to own cash. Certainly whenever a drug dealer is busted today, you hear all about the (gasp!) several thousand dollars in cash found. Heck, *I* know people who keep that much at home, and they are definately not drug dealers.

Once we become cashless, operating on "credits", the only people with any true freedom will be the hackers who are able to crack the systems and pilfer.

You-all and I will be at the mercy of both the hackers, and the gov't. By that time it will be impossible to break the sequence, since literally EVERY purchase you make, from birth-control, to books, to how much you give to your church, will be tracked, and you will be at the mercy of any future laws passed, such as, say, anti-birth control, anti-gun, anti-drug, anti-"pornography", etc. It's already happening today, and it will only get worse.

Search RISKS using swish-e

Report problems with the web pages to the maintainer

Search RISKS using swish-e

THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

ACM Committee on Computers and Public Policy, Peter G. Neumann, moderator

Volume 11: Issue 72

Monday 27 May 1991

Contents

Re: The RISKS of Posting to the Net

Brinton Cooper <abc@BRL.MIL>
Thu, 23 May 91 22:45:57 EDT

mmm@cup.portal.com posted a fascinating note describing how a visit by an FBI agent apparently was triggered by the disclosure of unclassified info about missile destruct systems.

mmm seemed unfamiliar with the notion that he may have revealed "sensitive" information. I guess it's no secret (and may not even be sensitive) that there is a body of information, growing without bound, that is "unclassified but sensitive." Folks not in the employ of the US Government are not likely to be as aware of this as civil servants. The notion is that there are many info

items which, while individually innocuous are collectively sensitive. Also, there is data from the trade secrets or cost figures of industrial organizations, and personal data in individuals (e.g. employment applications). All of this is "sensitive," and we're in deep trouble if we mis-use or publicize it.

I gather that mmm was not a civil servant or member of the military when he read the manual which he described. One wonders, then, how he got it and how he was supposed to know that it was "sensitive."

The risk isn't too subtle: The growing body of "sensitive" information and the rules surrounding its release bring us close to a British-style "official secrets act." Many of us recall how the stamp of secrecy was misused and abused in the Nixon administration. It requires little imagination to the potential for more widespread abuse in the case of "sensitive but unclassified." I believe that we have Reagan and his national in-security advisor, Adm Poindexter, to thank for this kettle of fish.

_Brint

Re: The RISKS of Posting to the Net

<rmoonen@hvlpa.att.com>
Fri, 24 May 91 10:30 MDT

Arghh. That's all we need now. Next thing, someone who says potentially dangerous words on the net, like say, ehh... blue box (Get that guys, BLUE BOX), or ehh... assassination of BUSH, will get a visit from our beloved Big Bro. I just hope they don't become aware of the underground nature of Usenet. If they do, it won't be long before you need a military clearance to even read news, let alone post!

Aside from that, and not really a RISK, but still: Not many people know that all transatlantic phone calls are being monitored by speech recognition equipment of the NSA. If too many keywords like "Bomb", "Assassination", "Ghadaffi", "Terrorist", etc. are recognised within a certain time, a tape recorder automagically switches on. For this reason, I start all my transatlantic phone calls with a list of ten keywords, just to be sure to waste some of their undoubtedly vast amount of audio tape.. :-)

--Ralph Moonen

---

the FBI and computer networks

Phil Agre <phila@cogs.sussex.ac.uk>
Sat, 25 May 91 16:54:28 +0100

Regarding mmm's message in Risks 11.71, I am quite curious whether you had any moral unease about volunteering all of this information to this visiting FBI agent. Of course the information is perfectly public. But this guy obviously had censorship very much on his mind, and I do think it would be just as well if he had never heard of the existence of the Internet. Think how alt.drugs and rec.pyrotech and the like sound to him: rather like how the network sounds

to someone who has just read a histrionic newspaper article about how the government is subsidizing the operation of a little-known computer network that is used for the distribution of pornography (e.g., alt.sex, which surely passes over some US government wires or computers, if only through government funded research projects, on a regular basis, someplace or other). What did you have in mind in volunteering all of this to a representative of a government agency with a long bad record of interference in individual liberty, whose every third sentence included words like censorship? Suppose an aide to Jesse Helms called you up and asked you for the most damaging factoids about government-funded computer networks that you could think of. Would you be sure to tell him or her that it's now possible to send netmail to the Soviet Union, using the .su domain? Do you think that a big, spurious public controversy would be a good thing? How about open FBI files on all regular contributors to rec.pyrotech? Maybe you have reasonable answers to these questions. But I can't think of what they might be.

Phil Agre, University of Sussex

Re: The Death of Privacy

Roger Crew <crew@CS.Stanford.EDU>
Fri, 24 May 1991 03:41:14 GMT

> We are well on our way to a cashless society. I predict that it
> will eventually be illegal to own cash. Certainly whenever a drug
> dealer is busted today, you hear all about the (gasp!) several
> thousand dollars in cash found. Heck, *I* know people who keep that
> much at home, and they are defin[i]tely not drug dealers.

It is already the case, under the RICO laws, that large amounts of cash can simply be confiscated. No warrant is necessary. I'm not sure what the necessary preconditions are, but evidently the standard road-stop to check for license & registration together with some notion of "probable cause" suffices. Police in south Florida are using this against suspected drug-runners with devastating effect.

To get the money back, even if no charges are ever filed, one has to bring a civil suit against the police department in question and demonstrate that the money was not illegally obtained.

The Supreme Court has upheld RICO.

Re: The Death of Privacy? (RISKS DIGEST 11.71)

"Mark W. Eichin" <eichin@ATHENA.MIT.EDU>
Fri, 24 May 91 01:06:04 -0400

<> We are well on our way to a cashless society. I predict that it will
<> eventually be illegal to own cash.

I stumbled across a television show recently (on some cable channel, I don't know what one) about the evils of a cashless society, and how it will

become impossible to survive without being part of the "system" (and thus being tracked by the system...)

It was titled "The Number of the Beast" and alternated between detailed explanations of the data flow in electronic funds systems used now and Biblical quotes regarding being marked with the number of the beast; being marked with the "number" was supposed to be a metaphor for being identified in the electronic funds system.

[I think we've been around on this one before, but I could not find it. PGN]

Re: Death of Privacy (Jerry Leichter, RISKS-11.69)

<WHMurray@DOCKMASTER.NCSC.MIL>
Fri, 24 May 91 07:27 EDT

Jerry, I was around thirty years ago. I remember what privacy meant. I remember how it was compromised and manipulated for the purpose of achieving social conformity. I remember women who lived alone being ostracized from the church because they might be divorced and they certainly were not married. I remember talking about unmarried men, on the assumption that they were homosexual, and therefore fair game for gossip, if not violence. The mechanism was gossip, and the idea was that if one did not conform, that was how they would be talked about.

I remember that it was considered perfectly proper to ask a job applicant what church they belonged to and what political party. It was not that anyone seriously believed that church goers were any more reliable than non-church goers; only that they were subject to social pressure to conform and excommunication if merely accused of nonconformity.

I remember the activities of the FBI, the files collected by "The Director." The political and economic pressure to identify one's associates as Communists. Now we call it McCarthyism, but the idea was ideological conformity.

I remember the gossip about whether such and such a movie star was "queer," whether that one had negro blood, or this one drank. John Garfield never made another film after being associated with Communists, and Ingrid Bergman could not work in this country after her divorce.

Do not hold up to me as an ideal the privacy of thirty years ago. That these things were only talked about over the back fence, and never in the papers, only made it worse. The problem may not have been any worse then, but it was certainly no better. Memory plays funny tricks.

No one cares about divorce, any more. Political ideology is out of favor everywhere except on college campuses. Now its worse to be a racist than to be of mixed race. Today the assumption is that everyone has been in therapy, but just twenty-five years ago it was a disqualifying defect in a vice-presidential candidate. When I was growing up the suspicion of Jewish heritage was enough to keep you out of the country club; now membership in the club is enough to keep you out of office.

Today the issues are communicable diseases, high risk behavior, child abuse, sexism, seduction, abortion, and drug use, but the intent is still conformity. Robert Bork was denied a seat on the Supreme Court for opinions that would have recommended him thirty years ago.

The fact is that there has always and everywhere been a battle between freedom and information. Every society in every age has used what information it had about its members in an attempt to control behavior. In France the police know who sleeps in every bed every night. Now they use computers, but they have always known. In China the Party knows who comes and who goes. They do not use computers, but they certainly know.

We do not gather at the well any more; we go to the mall rather than the general store. We go to MacDonalds rather than the diner. In our age, the communities are so large that it takes computers to keep up with everyone, but the intent and the damage are no different. The content

---

Re: The Death of Privacy? (Leichter, RISKS-11.69)

Geoff Kuenning <desint!geoff@uunet.UU.NET>
Fri, 24 May 91 03:20:38 PDT

> It's hard to see how we could have medical insurance on today's scale
> without such records and their relatively wide availability...

I couldn't disagree more; it's trivially easy to see how we can get along without such records. The whole purpose of the records is to help insurance companies avoid the self-selection problem, where their pocketbooks are emptied by people who get insurance because they know that they have a serious illness. But in a (gasp) national health-care system, this becomes a non-problem, and there is no longer any need for widespread exchanges of medical records -- except, of course, that the patient may find it in his or her best interest to make full information available to the doctor, but that's by choice.

Geoff Kuenning geoff@ITcorp.com uunet!desint!geoff

Re: The Death of Privacy? (Robert Allen, RISKS-11.71)

CNEWS MUST DIE! <mathew@mantis.co.uk>
Fri, 24 May 91 12:34:05 BST

It is not necessary to build electronic funds transfer systems in such a way that all purchases can be tracked. There are acceptable alternatives.

The cash card schemes I have read about in the UK would involve anonymous cards. The cards themselves are 'smart' cards; you would take your card to the bank and transfer money from your account to the card. You would be able to transfer as much or as little as you liked.

You could then use the card as cash, for making small purchases. The card is not marked in any way with your name, and there is no PIN or signature; if the

card were to be stolen, the person stealing it would be able to use the money in the card.

In other words, the proposed cashcard is just like real cash in every respect bar the fact that it's easier to carry around and easier for electronic cash registers to process. Clearly carrying large amounts of money on cashcards would be quite risky from the point of view of possible theft; but then, carrying large amounts of cash around is risky too.

The system is quite similar to the way Phonecards work; I'm not sure whether the US has similar schemes, so I'll explain: You can buy Phonecards in shops, with anywhere between 20 and 200 units of pre-payment for telephone calls encoded into them. This corresponds to 1 to 10 pounds sterling on the card, in units of 5p -- approximately $2 to $20 in units of 10 cents. The Phonecard is completely anonymous. When you have spent all the money on the card on telephone calls, you have to buy another phonecard.

With the cashcard system, you would be able to re-charge the card you already have, which is clearly better from an ecological point of view; and unlike Phonecards, the cashcards should be useful for general purchases.

To summarize, whilst we should be careful to make sure that the electronic funds transfer systems which get implemented are acceptable from a privacy point of view, I don't think the situation is necessarily as bleak as Robert Allen makes it out to be.

mathew

Smart Highways Need Privacy Tutorial

<cdp!mrotenberg@labrea.Stanford.EDU>
Mon, 27 May 91 10:43:15 PDT

As vacationers flocked to the beaches on this Memorial Day, the Washington Post reported that "smart" highways which would relieve traffic congestion may soon be a reality. About $20 million will be spent this year in federal funds to develop Intelligent Vehicle-Highway Systems (IVHS). Last week a Senate committee approved a measure that would devote $150 million a year for the next five years to IVHS. And, according to the Post, proponents call that cheap. Estimates for lost productivity resulting from traffic congestion are pegged at $100 billion annually. The GAO estimates that a full-scale IVHS system could cut commute time by 50% in such places as Los Angeles.

The article describes technologies that range from variable message signs that are tied to networks which monitor traffic flow to roadway-based guidewires with radio-controlled autopilots. The story also describes tollgates that will "read code radioed from a rolling car and automatically bill a credit card."

The article notes that in Europe and Japan trials of such systems have been underway for years.

Privacy aside -- Gary Marx is fond of a song by the Police that begins "every step you take, every move you make . . .I'll be watching you." Maybe it's time

for an update -- "every turn you take, every time you brake . . . I'll be watching you."

It's worth finding out whether the Senate committee has considered the privacy implications of gathering this data on drivers and whether there are any proposals to restrict the secondary use of the information. Likely buyers? Marketing firms and insurance companies.

Marc Rotenberg, CPSR Washington Office

They *are* watching

Jim Sims <sims@starbase.mitre.org>
24 May 91 18:32:40 GMT

In response to poster's lament about the govt getting access to his phone bill to see if he was calling the wrong people:

The government *already* has electronic access to your phone call transactions (numbers & [i think] length of call, not content), without a court order. They just have to show probable cause for a warrant to tap the *contents* of your calls...

jim
DECUS AI SIG Symposium Representative
The MITRE Corporation, 7525 Colshire Drive MS W418 McLean, Va. 22015

Re: SB266

"Willis H. Ware" <willis@rand.org>
Fri, 24 May 91 08:57:55 PDT

SB 266 has been folded in toto into Title V of SB 618 --Violent Crime Control Act of 1991. The old Sect 2201 of 266 is now Sect 545 of 618. Latter is also sponsored by Biden and deConcini. It's very long - 194 pages -- and covers everything but everything.

Here's a list of the major titles:

Title I	Safe streets and neighborhoods
Title II	Death penalty
Title III	Death penalty for murder of law enforcment officer
Title IV	Death penalty for drug criminals
Title V	Prevention and punishment of terrorist acts
Title VI	Drive-by shooting
Title VII	Assault weapons
Title VIII	Police and law enforcement training
Title IX	Federal law enforcement agencies
Title X	Habeas corpus reform
Title XI	Punishment of gun criminals
Title XII	Prison for violent drug offenders
Title XIII	Boot camps
Title XIV	Youth violence

Title XV	Rural crime and drug control
Title XVI	Drug emergencies
Title XVII	Drunk driving child protection
Title XVIII	Commission on crime and violence
Title XIX	Protection of crime victims
Title XX	Crack house eviction
Title XXI	Organized crime and dangerous drugs
Title XXII	Exclusionary rule
Title XXIII	Drug testing

Many of these titles have several sub-titles and most have many sections.

---

computer illiteracy

Ed McGuire <emcguire@cadfx.ccad.uiowa.edu>
Fri, 24 May 91 11:56:44 CST

I received in the mail today a new product announcement. The product is software that tutors new computer users in basic operating system concepts, thereby bringing an end to repetitive questions about logging in, current working directory, and so forth.

The announcement included comments from users of the product, including this direct quote:

> "I am very excited about [the product] and highly recommend its use to finally accomplish the goal of computer illiteracy."

[To badd he didnt spel ilitteracy write. PGN]

Search RISKS using swish-e

THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

ACM Committee on Computers and Public Policy, Peter G. Neumann, moderator

Volume 11: Issue 73

Tuesday 28 May 1991

Contents

Viper

<Brian.Randell@newcastle.ac.uk>
Tue, 28 May 91 17:44:52 BST

From the UK national newspaper, The Independent, 28 May 1991 - reprinted in its entirety. Brian Randell

MOD IN ROW WITH FIRM OVER CHIP DEVELOPMENT

A British company that hoped to market one of the world's most sophisticated computer chips is to be wound up next week amid acrimonious allegations about the Ministry of Defence's role in commercialising a technology developed at taxpayers' expense.

The episode highlights the continuing failure of the Ministry of Defence to foster civilian spin-offs for the products of its military research and development programme, which last year cost the taxpayer some (pounds) 2.2bn. Throughout most of the past decade, the Government has spent more money on defence than on civil research and development.

The chip, known as Viper, was designed by scientists at the Royal Signals Research Establishment in Malvern. It is the most advanced chip, designed for use in "safety critical" applications - such as nuclear reactor shutdown systems, driverless trains or aircraft controls - where lives depend upon faultless operation.

When the Worcester-based company Charter Technologies goes into voluntary liquidation on 4 June, no British company will be left able to provide potential customers with software to program the Viper chip or provide back-up support for its use. The company issued a writ against the Ministry of Defence this year for alleged negligent misrepresentation of the chip's capabilities and of its potential market.

The ministry denies the company's allegations and lodged a defence. The MoD had required the company to post security of (pounds) 75,000 to cover the ministry's legal costs should Charter Technologies have lost its legal action. The company ceased trading on 2 May 1991 and is no longer pursuing its legal action.

Digby Dyke, managing director of Charter Technologies, said yesterday that the company was forced to seek voluntary liquidation after the MoD declined to extend or renew other contracts, unconnected with the dispute over the chip, and because of the losses incurred over the Viper project.

When the chip was developed in the late 1980's, the then director of the Royal Signals Research Establishment, Nigel Hughes, described it as "the first commercially available microprocessor with a proven correct design". Modern microprocessor chips contain such complex circuitry that it is often not possible to demonstrate that the design is completely free of error. As a result, microprocessor developers are increasingly turning to the use of formal mathematics to verify that designs are free of errors.

In 1987, the MoD granted a licence to Charter Technologies to develop software to exploit the chip's capabilities. But this January, the company issued a writ alleging that the chip's design had not been proven, and as a result its money, manpower and time were wasted. The company was alleging, in effect, that the mathematics were not exhaustive.

Although Viper was developed by the MoD and released for commercialisation four years ago, and although a new defence procurement standard for safety-critical equipment, known as 00-55, appears to favour mathematically proven designs, Kenneth Carlisle, the Under-Secretary of Defence Procurement, told the House of Commons last week that "Viper is not currently used in any safety-critical computer systems controlled by the MoD".

The only civilian customer for the technology has been the Australian National Railway Commission, which at the end of 1988 adopted Viper as the core of a new

signalling system. The Australians have now gone so far with developing the system that they would have difficulty switching to another technology.

Computing Laboratory, The University, Newcastle upon Tyne, NE1 7RU, UK
Brian.Randell@newcastle.ac.uk PHONE = +44 91 222 7923 FAX = +44 91 222 8232

Maintenance of constants

Douglas W. Jones <jones@cs.uiowa.edu>
Tue, 28 May 91 12:18:48 CDT

In RISKS-08.19, I described a situation where, due to the cost of modifying a contract, it was less expensive to maintain dead code than to eliminate the dead code. As a result of this story, I have been approached with a similar story from AT&T; the employee who passed on the story asked that I not mention anyone's name. Here is the story:

It seems that the current generation of electronic switching systems coming out of AT&T are controlled by upwards of a million lines of C code. One of the results of this is the need to maintain the constants in the program.

You might think that constants are constants, so this should be simple, but this is not so. There are two problems that make this a headache big enough to require significant manpower.

Problem 1) Not all C constants are inherently constant. Consider string constants. These are just arrays of characters with appropriate initial values. Once such an array is passed to a procedure, the fact that it is constant is no longer known. Of course, on some computers, memory protection mechanisms could be used to make all strings read-only, but this is outside the scope of the C language and would introduce the possibility of errors in constant usage stopping a system that is not allowed to stop. Thus, programmers must be dedicated to auditing every use of every constant that is stored in memory to assure that it is used as a constant.

Problem 2) Because C has a very weak type system, named numeric constants are used instead of enumerated types. As a result, it is quite possible to use the wrong constant and never detect it because the constant has the right value. For example, if one enumeration is (Red, Green, Blue), and another is (Apple, Bananna, Cantalope), your program may run correctly with MyColor = Cantalope, but later, when you add BlueBerry to the second enumeration, the value of Cantalope (which was 2) has changed to 3, and your program will stop working correctly.

Pascal and Ada are both able to enforce the constancy of constants at compile time, and they go a long way towards eliminating problems with constants that coincidentally have the same value. (The latter problem cannot be completely eliminated in any language.)

As I understand the story, there is an actual team of programmers at AT&T who are responsible for auditing constant usage, and nothing else.

Doug Jones

The RISKS of Posting to the Net (RISKS-11.71, -11.72)

<mmm@cup.portal.com>
Tue, 28 May 91 16:56:40 PDT

Brinton Cooper <abc@BRL.MIL> wonders how I got access to the information on the destruct system of the Poseidon and Polaris A3. It was in a book that was published by Lockheed as a training manual. The book had no classification markings, in fact the one place in the book where it referred to classified information was a pointer to a separate, classified document which I did not have. I found it at a sale of used books. It is not too uncommon to find classified material in used bookstores, though I repeat this was _not_ classified.

Phil Agre <phila@cogs.sussex.ac.uk> asks whether I had any moral qualms about talking to the FBI. Judging from his letter and most of the e-mail I've received, it's apparent that many people consider the FBI to be the enemy of the Constitution and the Bill of Rights, rather than one of its defenders. Sure, there have been abuses in the past -- and there will be abuses in the future -- but perhaps you need to be reminded that we live in a world of spies, thieves, cutthroats, skinheads, Mafiosi, and Scientologists, and often our first and only line of defense is the FBI. Sometimes they make mistakes, like in the case of Steve Jackson Games, but do we help the situation by keeping the FBI men ignorant? I think ignorance is part of the reason why these abuses sometimes occur.

In the particular case of censorship, this particular FBI man was interested in how the net works and what relation it might have to criminal activity. He explicitly stated that the FBI was _not_ interested in censoring anyone's speech. When I told him about the recent discussion in alt.forgery, where people were asking how we could discuss forgery without discussing the committing of a crime, the reaction of the FBI man was "Well, you can write a book about forgery." My impression was that he was very sensitive to the distinction between free speech and crime. Just about the last words he said to me were "It's a free country."

If the only thing keeping the net free of censorship is the ignorance of the powers-that-be, that is not much of a defense at all. In fact, I think it would be naive to assume that potential censors aren't already aware of the net's existence. Uunet has revealed that they have sold compiled Usenet traffic on tape to the FBI. FCC men and telco security [people] are known to read the Telecom Digest. God only knows who reads RISKS.

Mark Thorson (mmm@cup.portal.com)

Re: Risks of posting on the NET (Moonen, RISKS-11.72)

"Jim McLeod, ISSM, USAAPGSA" <jmcleod%apg-9@APG-9.APG.ARMY.MIL>
Tue, 28 May 91 9:21:08 EDT

If and when a relative or friend of someone who boasts of such antics is a casuality of an airline bombing or other terrorist act, I hope he remember that his actions probably helped the terrorists and that he might be an accessory to murder of innocent men, women and children. If what he said about NSA is true, then did he ever stop to THINK that the time spent assessing phony "keywords" can prevent the investigation of an actual terrorist plan to commit an atrocity? I am as concerned about privacy and computer risks as the next person, but I get frosted reading such comments. Such an individual would probably be the first to blame "Big Brother" for not preventing the slaughter. [Disclaimer implied]

Re: The RISKS of Posting to the Net (Moonen, RISKS-11.72)

<erspert@ATHENA.MIT.EDU>
Tue, 28 May 91 14:06:48 -0400

> Arghh. That's all we need now. Next thing, someone who says potentially
> dangerous words on the net, like say, ehh... blue box (Get that guys, BLUE
> BOX), or ehh... assassination of BUSH, will get a visit from our beloved Big
> Bro.

Actually, it has already happened. A few years ago, I heard that someone who had posted something to the net about assassinating the president was visited by the FBI.

I suppose that this message will also end up in front of some government worker. :-(

Ellen Spertus

Re: The RISKS of Posting to the Net

Mike Olson <mao@postgres.Berkeley.EDU>
Tue, 28 May 91 11:29:08 PDT

In RISKS-11.72, Phil Agre <phila@cogs.sussex.ac.uk> takes mmm@cup.portal.com to task for disclosing "dangerous" information about the Internet to an FBI agent. While I sympathize with Agre's concerns, I think it's important to maintain some perspective. Censoring one another in our dealings with the government is no different from having the government censor us directly.

Mike Olson, UC Berkeley

Replicated Errors

Robert McClenon <76476.337@compuserve.com>
27 May 91 22:53:40 EDT

I respectfully submit that Neil Rickert is completely and very seriously wrong as to whether sendmail is primarily responsible for the replicated error messages. He would place the burden of preventing malicious software from

taking over networks primarily on network users and only secondarily on network managers. The moral burden of preventing malicious software of course falls primarily on users and only secondarily on network managers. Malicious acts that take over networks by users are immoral. The primary moral responsibility for the Morris worm rests with Morris, and he was convicted of computer abuse. But the primary pragmatic responsibility for preventing network abuse rests with network managers, since there is always a risk of a malicious user. Morris only exploited known vulnerabilities in sendmail and other software.

The message that Mark E. Davis disseminated was, because of the oddities of sendmail, an accidental INTERNET WORM. Anything that can be done accidentally can be done INTENTIONALLY. Network managers have a pragmatic and a moral responsibility to prevent worms and other malicious programs and malicious messages from taking over their networks. To attempt to shift this responsibility entirely to users overlooks the fact that not all users are moral. Someone could have released a message with a malformed header on purpose to flood the Internet with error messages. The primary problem is not with the user (Davis or anyone else). It is with the software. What Rickert says is a robust programming practice is simply not that if networks have finite capacity. Fair is correct. The error should be halted and sent back to the user, or sent forward without comment, or corrected and sent forward. Otherwise a WORM is possible.

Are fuzzy controls risky?

<HORN%HYDRA@sdi.polaroid.com>
Tue, 28 May 91 14:59 EST

Regarding the recently asked question about whether to trust a fuzzy logic based controller for nuclear power plants. I think the correct answer is that they should be trusted as much (or as little) as you would trust any controller. There is no guarentee that a control system is stable or accurate. This applies to both crisp and fuzzy controllers. The mathematical theory for robust control is better developed, but you must do the analysis before you assume stability or accuracy.

Software engineers often make the mistake of skipping this step. Many are unaware that there is a large, well-developed branch of engineering called system control theory. Just because the control laws are precise does not mean they will be accurate or stable. Often the mathematics are inherently unstable and no amount of precision in the software can overcome this. The instability is not a software problem (as assumed by many programmers); it is inherent in the mathematics of the control laws. These must be analyzed and shown to be appropriate.

Fuzzy control stability is not as well developed a theory, but the mathematics of fuzzy control are quite deterministic. Stability and accuracy criteria may be more work to evaluate. The control problem is usually simplified considerably for the fuzzy domain, so the resulting controller may be as easy to analyze as the precise controller or perhaps even easier.

The nuclear power plant is an example of a situation where both may be

appropriate. Consider the sub-problem of measuring the temperature distribution within the core. If you can assume thermal equilibrium, then a scattering of temperature measurements, plus the knowledge of conductivity of the components, plus the knowledge of the shape of the power distribution allows you to compute the temperatures, energy flows, and power generation throughout the entire core. If you cannot assume thermal equilibrium (e.g. startup and shutdown), you must also have the heat constants of the materials, the prior temperature distribution history, and the power generation to compute the temperature. So without equilibrium, you need two previously unnecessary inputs and one previously computed output must now be measured (somehow). These added measurements may drive the control laws beyond the regime where they can be analyzed, and they may also just be unavailable. Power generation distribution can be very tricky to measure directly. It is possible that the fuzzy solution is the alternative that remains mathematically tractable.

Then again, they may just be chasing the fad of the week. I see a lot of ``fuzzy'' systems being invented for marketing and PR reasons.

Rob Horn horn%hydra@polaroid.com

AT&T billing problem: "computer error"

Charles P Pfleeger <pfleeger@TIS.COM>
Tue, 28 May 91 15:58:11 -0400

I recently encountered an AT&T billing error on our phone bill, which the AT&T office acknowledged as a computer error on their part. There was a call from DC to NY which showed no rate code (E for evening, D for day, N for night/weekend), showed 15.5 in the "minutes" column (when all other entries in that column were integers, and [here was the real clue] cost $16.00, when similar (night rate) calls to NY were much less. I have heard from one other person who had similar problem. AT&T cheerfully resolves these matters when called, but I don't know if they are planning to adjust bills for people who don't complain.

Caller ID in commercial applications

<web!roberson@igc.org>
Mon, 27 May 91 19:06:22 -0700

People have been warning that with automatic caller identification, all sorts of strange and possibly undesirable cross-referencing will become common. I have just run across my first reference to a mass-market commercial program which will use caller identification in this manner.

The product is TeleCenter 2.0, developed by Northern Telecom. The advicle [advertisement in the form of an article] in a recent MacWeek [V5 N20, May 21/91, pg 27] said, in part,

> "Features such as caller ID and TeleCenter's address book can be triggered from another application. For example, using caller ID, an

order-entry application could automatically retrieve customers'
addresses and buying preferences when they call to make an order."

Walter Roberson roberson@web.apc.org

Search RISKS using swish-e

THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

ACM Committee on Computers and Public Policy, Peter G. Neumann, moderator

Volume 11: Issue 74

Wednesday 29 May 1991

Contents

Writer steals stories via computer

Rodney Hoffman <Hoffman.El_Segundo@Xerox.com>
Wed, 29 May 1991 13:58:18 PDT

In RISKS-09.75, I summarized a March 1990 `Los Angeles Times' story about a journalist charged with breaking into Fox Television computers. The 29 May 91 `Los Angeles Times' carries the conclusion, a story by John Kendall headlined WRITER GETS PROBATION IN STING AT FOX. Excerpts:

"Free-lance writer Stuart Goldman pleaded no contest Tuesday to three felony charges of illegally entering Fox Television's computer system and stealing story ideas planted by Los Angeles police in a sting operation.... [Goldman]

was placed on five years' probation and ordered to pay $90,000 in restitution, reduced to $12,000 with Fox's approval. The judge ordered Goldman to serve 120 days in County Jail but stayed the sentence....

"Goldman was arrested ... last year by Secret Service agents and Los Angeles police who confiscated a personal computer, floppy disks, Rolodexes and a loaded .38-caliber handgun.

"Prosecutors accused Goldman of using a password apparently gained when the journalist worked briefly for `A Current Affair' to enter the Fox production's computer system. They charged that Goldman stole bogus tips ... and attempted to sell the items to a national tabloid magazine....

"After Tuesday's court session, Goldman vowed to publish his completed book, `Snitch' [about being a gossip-media insider], as soon as possible.

"[The judge] ordered authorities to return Goldman's computer. `I'm sure you know now that computers will get you in trouble,' the judge said. `If you don't, I'll see you back in here again.'"

Consumer Reports report on Privacy

<RMG3@PSUVM.PSU.EDU>
Wed, 29 May 91 16:04 EDT

I've finally read my May issue of Consumer Reports. Of interest to Risks readers is their article `What price privacy?', pp. 356-360.

They mostly cover ground familiar to Risks readers:
*Databases like the files on people who have ever filed malpractice claims or on-the job injury claims.
*The workings of credit bureaus
*The error rate in credit bureau file information

Of greater news are their suggestions on what should be done.
"CU thinks the reforms should go even further. The law should allow information in credit reports to be disclosed only if the consumer authorizes the disclosure. Most people realize that if they apply for a credit card or a mortgage the prospective lender will examine their credit report. What they don't realize is that an application for employment, housing, insurance, even a dating service, may trigger a check. Nor do they realize that their files are routinely prescreened on behalf of direct marketers.
Any new law should also allow the credit bureaus a maximum of 30 days to investigate when a consumer asks that something on his or her credit report be checked for accuracy. Bureaus should be required to disclose to comsumers exactly how they go about investigating possible errors reported to them.
A handful of other laws are supposed to protect consumers against invasions of privacy, but they're riddled with imprecise language, exceptions, and loopholes. For example, a 1978 law supposedly protects against unreasonable searches of bank accounts by government agencies -- but state and local agencies are exempt, as are the FBI and U.S. attorneys.
Ironically, video rental records may enjoy the strongest safeguards against

abuse. Because of a 1988 lay commonly known as the Bork bill (after the Supreme Court nominee whose video-rental tastes were made public in newspaper accounts), a list of the videos you have rented can't be obtained without a court order. No such law protects your medical or insurance records (see box on page 357)."

They also make some suggestions: [List shortened by RG]
"Read the disclosure statements before you sign a credit form. At least you'll know how much privacy you're about to give up.
Check your Social Security records periodically to make certain that no one else is using your number. (Call 800-234-5772 to request a form.)
Likewise, write to any one of the major credic bureaus to opt out of pre-approved credit-card offerings. [The addresses and phone numbers of the big three are included in the article, as is the suggestion to check your record with them periodically. RG]
If a merchant insists on a phone number or address on a credit slip, you can refuse. There is no law that requires this information, and the major credit-card companies actually discourage or even prohibit merchants from asking. In California, Maryland, New York, and Virginia, the practice is illegal."

They also recommend "Privacy in America" by David F. Linowes, published by the University of Illinois Press and available through Consumer Reports Books as a detailed discussion of privacy issues.

I recommend the article to Risks readers (and perhaps the more knowledgeable can make suggestions to CU about policies to pursue).
Robert Grumbine

Re: the FBI and computer networks (Agre, RISKS-11.72)

Andrew R. D'Uva <ard@ctcg.com>
Tue, 28 May 91 22:50:42 EDT

DO YOU THINK THAT YOU ARE DOING ANYTHING WRONG? IS THERE ANYTHING WRONG WITH THE NET?! What the FBI files or does not file is the FBI's business. Why should the U.S. Government have less access than a student at an American university (or a foreign one)? What the FBI investigator "thinks" about censorship is really of no concern. Free speech (well.. free political speech) is a protected right, and the FBI is not capable of truly infringing on it. Just think of the outcry on the net if it tried to do so! :) However, the U.S. Government has a legitimate right to prevent illegal activity from taking place, especially when it occurs over taxpayer-funded networks like some portions of the Internet. In this case, waste is added to the illegal act itself. As for the .SU domain, if the boys at the FBI don't know that there are electronic links to machines in the Soviet Union, you can be certain that the fellows up at the NSA do.. and might even be doing something about it. Wouldn't it be pretty foolish of the Government not to. Would you prefer that a US--> {any other country here} link be kept unmonitored and clandestine in the spirit of free speech. At that point, why not let anyone transmit sensitive, perhaps classified, data to another nation? Sounds pretty silly to me.

The users of the net have nothing to fear
= =
A momentary pause. You could object that my argument stinks.. taken to one conclusion... "Let the police search your home any time.. if you are not breaking the law, you have nothing to worry about" This sort of argument makes sense to me, but I want to point out that you referenced newsgroups in your original message, PUBLIC newsgroups. You could argue that the status of private electronic mail is different, and I might agree with you. As far as transmitting that mail outside the US...well, we would have to argue about that some more. End of pause.
= =
from FBI scrutiny of the newsgroups. And taxpayers do have a right to know that some of their money is being spent relaying alt.sex.pictures to other sites in the US, and abroad. Chalk that one up to goodwill :) The situation with email is, granted, a different one. The way I read your response is that the Internet would be better off without public scrutiny. Why?

Re: Risks of posting on the NET (jmcleod, RISKS-11.73)

<rmoonen@hvlpa.att.com>
Wed, 29 May 91 09:29 MDT

->..., then did he ever stop to THINK that the time spent
->assessing phony "keywords"can prevent the investigation of an actual
->terrorist plan to commit an atrocity?

Oh, this really makes me laugh. If and when a friend or relative becomes a victim of a terrorist act, it is solely the terrorists who are responsible. Furthermore, please explain to me how my actions could "prevent the investigation of an actual terrorist plan", no, even "help the terrorists" ? Gee, next time you get a parking ticket, you'd start feeling guilty about the wasted police time/money that could also have been used to track down real criminals. You'd even have helped them and might be an accessory :-O

I am talking about machines monitoring phone lines, and certainly it would take any tape of my conversations 5 minutes to end up in the garbage can. If this is what they choose to spend tax-payers money on, then I am free to say *anything* I want on my phone calls.

Ralph Moonen, Free citizen of The Netherlands

Re: The RISKS of posting to the net (RISKS-11.73)

arthur rubin <a_rubin@dsg4.dse.beckman.com>
Wed, 29 May 91 08:11:42 PDT

Mark Thorson <mmm@cup.portal.com> refers to the FBI making a mistake in the case of Steve Jackson Games. I believe it was actually the Secret Service, although I still don't understand why they thought they would be interested.

[Also noted by Bill Ricker.]

Re: The RISKS of Posting to the Net

William Ricker <wdr@wang.com>
Wed, 29 May 91 11:58:19 EDT

It does sounds like the FBI Special Agent that Mark spoke with would have seen the difference between the SJG Cyberpunk game and a criminal communication -- if any such exist under our constitution, which I doubt -- which was not understood by the SS agents hunting for allegedly stolen AT&T documents.

Ignorance is definitely a contributor to the abuses; evidentiary seizures of hardware that shut down a legitimate business or FIDO node are not warranted (pun intended) when what is ordered is seizure of evidence stored on disk -- a backup taken by the constables is all that is required, which can be analyzed at their leisure. But typically they wouldn't know (a) how to do a backup, (b) how to analyze it, (c) how to configure a system onto which to restore it. (They also may not have a budget code for renting a PC onto which to restore it, or be forbidden to do so by work-rules and waste-guidelines!) And who in the raiders is going to trust the Obviously Guilty Party to do a backup for them? (S)He might try something tricky to destroy evidence, like in those spy movies...

/s/ Bill Ricker wdr@wang.wang.com

FBI Inquiries

<RSAUNDERS@hssi.dnet.hac.com>
Tue, 28 May 91 16:55:33 -0700

We had a similar inquiry by the FBI a couple of years ago. We were demoing a synthetic TV system using a satellite link between our big computer and the trade show. The demo pictures looked like a very low pass over a nuclear power plant. We had relocated a nearby plant into distant terrain. Some guy say it on his home TV and called the FBI.

People should not expect the FBI to be up to speed on everything. They are just investigating things, they never accused us of anything. They asked where the nuclear plant was (they clearly "saw" one on TV that didn't exist).

We explained everything, and they asked a few questions about synthetic TV. In general they were using their position in the Government to get us to teach them something they didn't know. I am convinced their only interest was to determine if this was a problem they needed to investigate in detail. I presume their approach with real criminals is different. In the previously discussed case, they got a pretty good explanation of Internet mailing lists without having to do a lot of legwork themselves. As long as they don't pester the same people every time, this seems like a pretty cost effective way to get Government business done. I would prefer it to using lots of my tax money to find out something they could have found out just by asking. I think we need more Government that takes simple, direct approaches like this. Give the FBI a

hand for finding an easy solution.

Randy Saunders

Re: Risks of RISKS Networking

<[anonymous]>
Wed, 29 May 91 12:05 xxx

mmm's story about the risks of Risks postings has prompted me to write about my experience concerning the risks of Risks postings. I'm staying anonymous simply because I'd prefer not to have this happen again. Before I start with the story, may I emphasize that this is not happening in U.S.A.

About a year ago, I posted a couple of articles to Risks, concerning the crash of an aircraft in Eastern France. About a week later, my apartment was "kindly visited" in my absence.

Note the following facts:
1. nothing was taken from the apartment
2. old issues of RISKS, printed on line paper and stacked in a corner had been thoroughly examined. The proof was that my quasi-order had been clearly transformed to a full disorder.
3. all my bank papers (account statements, letters from bank manager etc.) had also been inspected - again my quasi-order was transformed to disorder. I mean that it was in some sort of order, but not mine.
4. my passport was obviously examined, since it was put back in a wrong drawer.

The job was very well done. I only noticed that my apartment had been visited because handles on a chest of drawers were sticking up, while I always made sure that they didn't.

Since nothing had been stolen, I decided not to inform the police. However, through some extraordinary coincidence, a man was murdered round the corner, a block away, and the police paid a visit to everybody in the neighborhood to investigate. While I had no information about that crime, I decided to inform them about the break-in in my apartment. Their questions were as follows:
"- do you keep any confidential information in your apartment, whether defence-related or commercial ? "
"- do you work in any governmental institution and have access to classified information ?"
"- do you do any scientifical research which could lead to you keeping important information in your apartment ? "
"- could any friend, girlfriend, or relative have used a spare set of keys to come into your apartment and look through your papers ? "
"- do you deal with drugs ?" (yes, they really asked that !)

Since my answer was NO to all above questions, they decided to send the forensic unit the next day. Deductions of the forensic unit were as follows:

1. the intruder came in via the kitchen window (which was closed but didn't have a lock at the time), stepped into the sink, and left one footmark

on the kitchen floor, due to the moisture collected by the shoe in the sink.
2. the intruder wore gloves since no fingerprints were found, neither on the window nor on anything else (door handles, printouts, drawers, etc.)

The general feeling was that the job had been done by a professional. The forensic unit took a record of the footmark (sneakers) and promised to contact me a few days later.

I got a call from the police two days later. All they said was that it was a professional job but they'd soon identify the intruder(s). Someone was trying to find-out about my sources of income, and it was probably related to "the fact that you deal with computers and store this computer information in your apartment". Well, I had figured that out myself, thanks ! They then told me they would keep me informed on the developments of the investigation.

I have not heard from them since.

Re: The Death of Privacy? (Robert Allen, RISKS-11.71)

Michael Rasmussen <mikeraz@techbook.com>
Mon, 27 May 91 16:24:46 GMT

A point that has always bothered me about this type of `privacy' argument is that `privacy' as we know it is a very recent phenomena. Before we had a high density, easily mobile population the conditions you describe were part of everyday life in the closely knit small communities. There was not privacy as we know it today.

The easy collection of data about a person is applying modern technology to modern population levels to recreate the community knowledge that used to exist.

The significant difference is that then **everybody** who wanted to know your business did, now only the authorities collecting the data can know. The real problem as I see it is to get the information back out of the collecting agencies and into the public gossip trough.

Giving Away Privacy

Sanford Sherizen <0003965782@mcimail.com>
Wed, 29 May 91 13:43 GMT

Many of the recent postings about privacy suggest that privacy is being taken by government and businesses in a one-way transaction. While that certainly occurs, the nature of collecting information is more complex than that.

Consumers and employees often inform on themselves. Some are forced to reveal private information as a "voluntary" tradeoff for obtaining a job or purchasing insurance. The employers often treat this information as available for distribution or whatever use they consider as appropriate. Many corporations routinely report sensitive information about their employees to insurance and

credit organizations, often without letting the employees know that this is their practice. One major hospital's medical records department receives 1500 requests for this type of information each month, to a large part from insurance and third party carriers, which distribute this information to other organizations.

Other people give away their privacy for a variety of inducements. Valuable information is given freely by people in exchange for consumer benefits. Credit card account holders or those tracked through electronic scanning of their store purchases may be willing to make this trade in order to receive discounts or notices of advance sales. One survey company sends a letter to potential interviewees that offers $10 plus the following comment. "...(L)egitimate research is an important part of our world and the accuracy of survey research depends heavily on how many of the people selected into the sample actually end up participating! Often survey results are slanted because too many people are hesitant to cooperate." Who could resist that appeal?

Privacy invasions in the U.S. have become almost a perfected process. The poor were the test population for information scavengers. The poor were checked for their eligibility for welfare, immigration, jobs, and law abiding-ness. They lived with few privacy rights.

The poor tested well and now the technology is being improved to collect information on even more people. Investigating the poor is now the model for intensively examining the lives of the rich and the middle class. These previously protected populations are now checked for their marketability, payment of college loans, correctness of resumes, professional conduct, insurability, and driving records. The list goes on.

Truly, you can run but you can't hide. One day soon, we may start our work by electronically connecting ourselves to a computer that has polygraph and urine analysis options. Our productivity, workhabits, error rates, and deviations can be automatically collected. On a "voluntary" basis, of course.

One recent study found that some companies wre even attempting to restrict intra-company dating by monitoring employees. Pinhole videocameras hidden in smoke alarms, tv sets, and clocks are being sold to companies to monitor employees and customers. Even the privacy of our refuse has been trashed. Some municipalities require that garbage be put in clear bags so that garbage collectors can inspect residents' trash to ensure that they are recycling correctly.

In a strange retribution (justice redux?), businesses have themselves begun to lose some of their own privacy. Industrial espionage is on the increase. Major corporations have formed business intelligence units, many run by ex-intelligence officers. Competitive business intelligence is considered as a corporate necessity today, where anything available about competitors is gathered. Information can be obtained legally through searching government records, speeches by corporate spokespersons, and reviews of want ads seeking specialists (which may indicate new product developments). Other information collection may not be legal.

Consumers have also become interested in piercing the often one-way privacy interests of corporations and government. The Freedom of Information Act and

the various whistleblower laws that provide cash rewards for those who report illegal activities have begun to make corporate secrets more public. Even the electronic tools that businesses use to collect information have become more readily available to those who wish to gather sensitive corporate information, such as corporate contributions to PAC's and stock holdings in South Africa, to cite readily available databases.

Recent information on the East German secret police (Stasi) indicates that they had an estimated 85,000 full time agents and 500,000 part time informants in a population of 17 million citizens. In the U.S., we collect confidential information differently. We don't just gather information on dissidents. In the American way, we believe in equal opportunity collection of information. Our diseases, disorders, deviations, and other details are growing into a national Information Age dossier.

Certainly there are many differences between the East German Communist government and the U.S. government. What is important to recognize, however, is that there are also some startling similarities. We have become a nation of informers and informants. Americans live surrounded by technological vacuum cleaners that such up information. Big Brother has turned out to be the Big Browser.

Sanford Sherizen, Data Security Systems, Inc., 5 Keane Terrace
Natick, MA 01760 USA, MCI MAIL: SSHERIZEN (396-5782), PHONE: (508) 655-9888

Smart Highways Need Privacy Tutorial

Warner Losh <imp@Solbourne.COM>
Mon, 27 May 91 14:29:39 MDT

cdp!mrotenberg@labrea.Stanford.EDU writes:
: It's worth finding out whether the Senate committee has considered the privacy
: implications of gathering this data on drivers and whether there are any
: proposals to restrict the secondary use of the information. Likely buyers?
: Marketing firms and insurance companies.

Thieves? It seems to me if I were able to tap into this system and find out that Fred Smith's car was in grid lock and so was his wife's, then I'd stand a better chance of robbing their house than I would if I was just staking it out. After all, I'd have a nice warning system if I could get periodic updates (or just program my home computer to "beep" me whenever they got withing 3 miles or something like that). Keep in mind that the proposed system doesn't use encryption at all.... (And even if it did, there would be a back door in it, right? After all, isn't that what SB618 (nee SB266) is all about)

Take a look at the book "Mindkiller" by Spider Robinson for an example of a thief that uses the central monitoring computer to rip off people that aren't home.

I wonder if such systems would be mandatory or optional. If they were mandatory, does that mean that I have to pay for LA's terrible traffic problems even though I live in Colorado and face little or no traffic on my way to work?

That doesn't sound fair to me.

Warner

Re: Replicated Errors (McClenon, RISKS-11.73)

Neil Rickert <rickert@cs.niu.edu>
Wed, 29 May 91 11:25:50 -0500

>I respectfully submit that Neil Rickert is completely and very seriously wrong
>as to whether sendmail is primarily responsible for the replicated error
>messages...

On May 24 I observed a period of perhaps 30 minutes in which it was impossible to make an SMTP connection to THINK.COM. This is presumably because it was being besieged with replies to the (apparently forged) sendsys news control message, which asked all news sites to automatically reply to COMPASS.COM (which is gatewayed through THINK.COM).

Approx one year ago a message arrived at our site with a `Return-Receipt-To:' header. It was part of the distribution of a large mailing list, perhaps `unix-wizards-digest', although my memory is uncertain on which list. It took more that 24 hours before an SMTP connection could be made to deliver the return receipt, apparently because the receiving host was saturated with replies.

In neither of these cases was there a "replicated error". Indeed, there was no "error" at all.

I repeat my earlier assertion. The "replicated error" discussion is a bogey man, which has little to do with the problem. The problem was caused by sending into a large mailing list a message which would generate automatic replies. The fact that those automatic replies were error messages is largely incidental. The behavior of sendmail perhaps multiplied the severity of the problem by a factor of three, compared with messages generated only at final destinations. But just generating messages at final destinations can already cause a severe problem.

Clearly the responsibility must be on the distribution system (mailing list software for example) to minimize the likelihood that distributed messages will generate large numbers of automatic replies.

I should note that the original incident was made particularly obvious by the fact that the automatic responses happened to go through an address which was gatewayed by the same host as the mailing list management software. It is likely that many such incidents (particularly with Return-Receipt-To:) have occurred in the past, but since the return address bypassed the list distributor, the problem was only noticed at the site to which the automatic responses were addressed, and they probably decided they had no choice but to live with it.

Neil W. Rickert, Computer Science <rickert@cs.niu.edu>
Northern Illinois Univ.

DeKalb, IL 60115 +1-815-753-6940

Search RISKS using swish-e

THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

ACM Committee on Computers and Public Policy, Peter G. Neumann, moderator

Volume 11: Issue 75

Wednesday 29 May 1991

Contents

Vote-by-Phone - Promises and Pitfalls

<SALTMAN@ECF.NCSL.NIST.GOV>
Wed, 29 May 1991 14:17:27 EDT

> [Moderator's note: Roy is not a regular RISKS Reader, but is one of the world's most honored watch-ers of electronic voting. He asked for some feedback on this, so the RISKS Forum seemed like an ideal place for him to find some knowledgeable and interested sources of feedback. You may respond to him directly. If you think your response would be of general interest to RISKSers, then please CC: RISKS as well. PGN]

Vote-by-Phone - Promises and Pitfalls
Roy G. Saltman, National Institute of Standards and Technology

Many of us have had contact with a voice-response system (VRS). Perhaps you called some organization on the phone, possibly a bank to obtain your account balance, or the Motor Vehicle Bureau with a question about car registration, and you heard, not a real live person, but a recorded voice. The voice was clear and unaccented, pleasant and neutral; it was trying to be a voice with which you couldn't get personal, but it was recorded. The voice told you to push particular buttons on your phone to obtain particular kinds of information.

VRSs have come into wide use in the past few years. The systems are computer-based. The voice you hear when your call is answered is not on an audio tape like an answering machine, but it is a reconstruction from computer memory of the voice of an actual person. That individual and others, if more than one speaker was used, have pre-recorded all the potential messages. The messages were "digitized" (converted into data for a computer) and stored in a

computer memory. When you selected a particular push-button on your phone, that selection activated a corresponding branch of a computer program. The program chose the appropriate response message from the computer memory. The digitized message was then reconverted to a real voice that you heard through your phone.

If you were fortunate, the choices offered you by the voice included exactly the information you were seeking; if not, you stayed on the line even if you didn't have a dial phone, and perhaps you got to talk to a flesh-and-blood human.

Some Questions

Could we vote by phone, using a VRS with the added functions of vote recording and summarization? It's technically feasible, and will be tried in at least one community if some folks in Boulder, Colorado, have their way. However, there are special considerations in addition to the ordinary questions of system design to meet the needs of the particular election situation. Here are some concerns:

* Proof of identity could be a problem.

* Privacy could be an issue, as well, if the voter is in a location where others might be watching or listening or electronically eavesdropping.

* User-friendliness would need to be designed into the system. Voters have different capabilities. There are always special cases when a person with no special training uses an unfamiliar machine.

* The voter without touch-tone phone service must be considered; older ways of voting might have to be retained, in addition to voting-by-phone.

* Accounting and accountability are a concern. It must be absolutely certain that the computer is correctly recording each voter's choices and accurately summarizing the votes for each candidate.

* The system would have to be secure against malicious mischief; extra phone calls from disrupters should not be able to clog the system and prevent its use by participating voters.

* Reliability must be a priority; the system would need to available for use at all times throughout the hours that the polls are open.

Dialing In

The voter with touch-tone phone service would dial a toll-free number. Hopefully, the system will have been designed to be able to accept the maximum number of calls expected at any one time, so that the chance of getting a busy signal will be very small. When the call is answered, the voice would identify its function of providing the voter with election choices and of recording the voter's selections. Perhaps the first selection that the voice will ask the voter to make is the language that the voter would wish to hear. For example, the voter might be asked to push 1 for English, 2 for Spanish, and 3 for another language widely used in the local area. Alternatively, different phone

numbers could be used for speakers of different languages.

Verifying Registration

The next step would be to identify the voter as eligible to vote. For this purpose, the system would have to have the complete file of registered voters resident in the jurisdiction "on-line," that is, instantly accessible. The voter would be asked to enter a multi-digit personal identification number (PIN) and possibly some not-publicly-available personal data. The voter would have been prevously sent his or her PIN by mail.

For assured identification, the possibility must be minimized that a random selection of digits, or even the filching of a PIN, could result in a successful masquerade. A PIN is typically employed with an automatic teller money machine (ATM). In using an ATM, the accountholder enters a PIN and physically inserts a plastic card with a magnetic-stripe containing encoded data. The information available to the system from the stripe on the card enables the PIN to be as short as four digits. With the concept that any touch-tone phone could be used for voting, the absence of ATM-like functionality is assumed. In that case, the PIN would need to be cosiderably longer than four digits, perhaps eight or more, and the inclusion of personal data would serve additionally to prevent fraud.

In addition, it is assumed here that typical State legal requirements for a signature on voting, or personal recognition by a precinct official, or a similar requirement, would have been previously circumvented by legislation.

The Voting Process

Once registration has been verified, and the voter has not been recorded as having voted, a review by the computer of the voter's residence location would determine the contests for which the voter is entitled to vote. The system would then begin to request choices from the voter; for example, "For president, to vote for Washington, Federalist, push 1, for Jefferson, Democrat-Republican, push 2, for Roosevelt, Bull Moose, push 3, for a write-in, push 9, and to go on to the next contest, push 0."

The "go on to the next contest" message provides the voter with the option of not voting for any candidate. An alternative is for the voice to say, "for none of the above, push 0." With either message, if the voter selects any option but write-in, the voice can repeat back the choice ("you voted for .... ") and then proceed immediately to the next contest.

If the voter selected a write-in, the system could then ask the voter to enter the name of the write-in candidate using the letters on the phone buttons, and to push # when finished. Voters planning to write in a candidate's name should be told to prepare beforehand the number-equivalents of the letters in the name (e.g., Smith is 76484), so that the entry process will be as simple as possible. Special assignments for the letters Q and Z would need to be made if those letters were included in a candidate's name, as those letters do not appear on the phone buttons. Usually, Q is assigned to the PRS (7) button and Z to the WXY (9) button. The # button, or * or 1, could be used as an indication that the voter is finished with the write-in, as none of those

buttons is used for letters.

The use of phone buttons to represent a name provides a somewhat ambiguous result, since each button represents three or four letters. There would have to be an understanding and agreement by the election administrators of what name is intended. If this procedure is not acceptable, some other write-in method would need to be invented.

User-Friendly Requirements

System designers would need to keep in mind the following:

Sign-In Problems: If a legitimate voter is not able to get his or her identity and registration verified, for whatever reason, the voter must be able to contact the election administrators to get help or to obtain a different method of voting.

Time Allowance: How long should a voter be allowed to ponder a particular contest, and what should the system do if the voter has failed to vote when that interval is up?

Voter's Error: What does the voter do if he or she has pushed the wrong button, and wants to reverse a choice, (a) while the contest is current or (b) during a choice for a subsequent contest?

Repeating the Choices: How does the voter indicate to the system that he or she wants the choices repeated before casting a vote? Voting by phone would be particularly difficult where the voter has to select a large number of choices from an even larger number of candidates, typically for certain public boards, such as political party central committees. Voice-response is serial; the voter cannot see all the choices at once, and cannot see the selections made. It may be that a ballot should be sent to each voter beforehand, so that the voter could visualize the choices to be made while on the phone.

Overvotes and Undervotes: The system could indicate to the voter that he or she has voted for more or fewer candidates than permitted. Overvotes should be prevented and undervotes allowed. What messages, if any, should be system provide to the voter in these cases?

Failure to Complete the Process: It is possible that a voter could be called away from the phone by an emergency or a higher priority task while in the process of voting. This could happen with a voter at home or at the office. What does the system do?

Voter Disinterest: The voter does not wish to vote on the lower-level offices or referenda, except for one particular contest. How does the voter tell the system to skip to that contest, or cancel the remainder of the process?

Verifying Choices: After the voter has completed voting, does the system repeat back to the voter the choices made?

The only "correct" answers to these questions are those that demonstrate to voters that the system is easy to use and should be widely adopted. If ease of

use cannot be implemented, voters will find the system too complex and may not vote at all.

Voters Without Phone Access

The voter lacking personal access to a touch-tone phone would need to be provided with an alternate method. Touch-tone public phones could be used and the phones could be arranged to require no fee for a voting call. However, these phones are typically in locations where privacy could be a problem. Another method would be to treat those without touch-tone phones as absentee voters, and send them ballots to be returned by mail. If polling stations are to be kept open, each voter would have to declare in advance, like absentee voting, whether he or she planned to vote by phone or vote at the polls. Otherwise, each polling station would need to have on-line access to a voter database that reported which voters had already voted by either method. On-line updating would be needed to prevent an individual from voting by both methods.

Accuracy, Accountability, and Public Confidence

The vote-by-phone system is somewhat more complex than a typical VRS. In addition to the selection of particular messages, the voter's button-pushing actions must cause his or her voting choices to be correctly recorded and accurately assigned to particular candidates. In addition, the system uses no ballots independently filled out by the voter. Consequently, there is no way that a true recount of the results reported by the system could be obtained.

In view of the manner of system operation, it is essential that all the groups involved, that is, the voters, the election administration, the contending parties, and the candidates, have full confidence in the results that the system produces. The only way that confidence can be achieved is for operation of the system be thoroughly tested and checked out before the election. The software used in the system should be totally protected from outside influences, and an identical copy of all of it secured in the hands of the chief State election officer. System testing should use both internal analysis of the computer program, as well as testing and checking system response to a variety and quantity of different potential voter selections and actions. In addition, voter accounting data must be retained. These data include the number of voters signed in and eligible to vote for each contest, and the number of undervotes in each contest. The number of votes plus undervotes in each vote-for-N contest, N = 1, 2, 3, etc., should equal N times the number of voters voting for the contest.

Public understanding that the system does not violate voter privacy is also essential to public acceptance. Voters must be certain that the part of the system that verifies their identities is distinct and separate from the part of the system that records their votes, and that there is no communication of voter identity between the two parts.

Assuring System Security

Total system integrity involves security, in addition to accuracy and accountability. By security is meant the control of access to the system,

where legitimate access is allowed and other access prevented. In an on-line system, such as vote-by-phone, it is crucial that callers only be able to record their voting choices and not be able to, by any combination of pushing buttons, achieve access to the controlling programs of the system.

Based on a history of hacker activity, protection must be implemented against potential disruptions. Other on-line systems have restricted attempts to sign-on to a small number of successive tries on a single call, e.g., not more than three, so that it would not be possible to randomly try many PINs on one call until a correct one is found. Extra calls clogging the system could not be prevented unless automatic number identification (ANI), with which the call recipient knows the caller's phone number, could be used in connection with pre-established voter phone numbers. Voters could be asked to specify a phone number, and one or two alternates, from which they would vote. Then, if ANI were available, the system could ignore those calls not from a voter's phone.

If ANI were not available, calls could be timed-out and ended if the caller remained on the line for more than a maximum number of seconds without successfully completing the initial steps. If a phone from which clogging calls were being made could be identified, it is possible that laws that already exist or could be enacted would allow legal action to be taken. Of course, the election would be long over before a penalty could be imposed.

The Future

The expectation of supporters of vote-by-phone is that its convenience will increase turnout. With a well-designed system, convenience would be improved for persons who are handicapped or home-bound, for frequent travelers away on a moment's notice, and those who always seem to be too busy to go to the polls. Of course, absentee ballots are already available for them.

Some think that failure to vote is simply an administrative problem that new technology or simplified procedures could easily solve, but this article has attempted to show that the application of new technology requires thoughtful and detailed consideration of implementation issues that connect technology to effective human use. Issues have been raised, and some directions for solutions identified, but the real challenges are left to the designers.

Other persons think that failure to vote is a social problem with much deeper causes and solutions than the type of technology being employed. Only several trials of vote-by-phone in different kinds of communities could provide some answers, but the funding of such trials is not a trivial issue. Election administration must compete for funds with all of the other concerns that face State and local governments; advocates of vote-by-phone would need to demonstrate the urgency of their proposals.

Search RISKS using swish-e

THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

ACM Committee on Computers and Public Policy, Peter G. Neumann, moderator

Volume 11: Issue 76

Thursday 30 May 1991

Contents

Privacy, credit reporting, and employment

<ark@research.att.com>
Thu, 30 May 91 09:44:14 EDT

A couple of days ago I saw a news item to the effect that EDS had been requesting credit reports on job applicants without their knowledge and using those reports in their employment decisions. This practice violates the Fair Credit Reporting Act. The gist of the article was that EDS agreed to contact everyone who had been turned down for a job because of a credit report in the past two years and tell them about the report. The unsuccessful applicants could then contact the credit bureaus, request copies of their files, and contest any inaccuracies that might appear.

This story is a beautiful lesson in privacy for several reasons:

1. Things like the Fair Credit Reporting Act are
   less help than they might be because it's so hard
   to find out when people ignore it.

2. The FCRA is almost no help at all against employers
   who request credit reports on employment candidates
   because by the time the appeals procedure has ground
   its way to the end, the candidate is probably not
   going to work for that company anyway.

3. According to the article, it is only recently that
   credit bureaus have started making their information
   available to prospective employers on a large scale.
   This is a nice example of data being used for a purpose
   other than that for which it was originally collected.

The second point is particularly important. If a company turns someone down for a job (partially) because of a credit report and the person then successfully contests that credit report, the applicant is unlikely to be hired anyway, being now a proven troublemaker. Of course the applicant may have found another job in the meantime.

--Andrew Koenig

Job-screening via credit records

Jeff Johnson <jjohnson@hpljaj.hpl.hp.com>
Thu, 30 May 91 13:55:34 PDT

"Electronic Data Systems Corp, a unit of General Motors Corp, agreed to settle charges that it failed to tell job applicants that information in their credit reports influenced the decision not to hire them.

The consent agreement was the first Federal Trade Commission action dealing with a new use of credit data marketed by credit-reporting agencies. The commission said these 'employment reports' which are being used by a growing number of businesses to make hiring decisions, often contain more credit information than the standard credit reports long used by banks and retailers.

Agency officials also said some companies might not be aware that, under law, they are required to inform job applicants when a credit history is being used to evaluate them. They said the FTC is seeking voluntary compliance with the law, and will be publishing an alert to inform companies of their obligations." [...] [Excerpted from The Wall Street Journal, 29 May 91, p.B4]

Re: the FBI and computer networks (D'Uva, RISKS-11.75)

<smb@ulysses.att.com>
Wed, 29 May 91 21:08:05 EDT

I fear that Mr. D'Uva is sadly mistaken, both about what the FBI is permitted to do, and what abuses they have been known to commit. The FBI is *allowed* to gather information about probably criminal activity. They need ``probable cause'', as a matter of public policy and (I think) Federal law. They are manifestly *not* allowed to monitor anything because they don't like it, or because they think it might be evil, or ``un-American'', or ``subversive''. And of course, there are many examples of the FBI not following such rules: COINTELPRO, the myriad files on Dr. Martin Luther King (allegedly sleeping around is not a Federal offense), etc. The same applies to local police departments -- there was a recent uproar about some departments monitoring talk shows on black-oriented radio stations, to find out who the local activists -- ``troublemakers'' -- were, and what they were up to.

Yes, the net is a public forum, and anyone who engages in criminal activity on a mailing list is pretty stupid. But the FBI has no right to engage in systematic monitoring of the net as a whole.

--Steve Bellovin

Re: the FBI and computer networks (Agre, RISKS-11.72)

Andrew R. D'Uva <ard@ctcg.com>
Thu, 30 May 91 0:22:44 EDT

I think that Steve is confusing legal terminology here. Probable cause is invoked when a law enforcement agency needs to make a search or intercept data which is not in the public view. For example, a policeman does not need "probable cause" to stop your car when you are driving in an unsafe manner. The law has been broken, and that is enough to warrant the law enforcement official's intervention. The policeman still needs an actual warrant to search an area in your car which is not under your immediate control (e.g., your trunk). The case here is different: we are talking about the FBI (or any other agency) reading the information carried in a PUBLIC forum, and acting on that information. There is no juridictional issue here, as clearly the traffic is interstate, not intrastate in nature. Surely Mr. Bellovin would not wish to prevent the members of the FBI from reading the newsgroups simply because they are law enforcement officials. That smacks of a different sort of censorship.

> monitor anything because they don't like it, or because they think it
> might be evil, or ``un-American'', or ``subversive''. And of course,
> there are many examples of the FBI not following such rules:

I didn't say anything about "evil" or "un-American" activities. What I did say was that the FBI is entitled to prevent illegal activities, or act when evidence suggests that crimes have been committed. We are talking about crimes, not discussion.

> COINTELPRO, the myriad files on Dr. Martin Luther King (allegedly
> sleeping around is not a Federal offense), etc. The same applies to
> local police departments -- there was a recent uproar about some
> departments monitoring talk shows on black-oriented radio stations, to
> find out who the local activists -- ``troublemakers'' -- were, and what
> they were up to.

Certainly, it would appear that this is a troublesome point..but is it? Much of the "drug war" is fought (here in Washington, D.C.) in areas which are considered "black." Yet there is no such outcry here. If the crimes are being committed, adding a racial element into the equation doesn't help. The appropriate law enforcement agencies need to be able to go to where the crime is... if that's on Usenet... so what? Caveat: I stated before, and state again that the case of e-mail (between 2 parties) is different. Intereption of e-mail is *probably* protected by the "unreasonable search and seizure" clause of the Constitution. Public communication is not (no "search").

> Yes, the net is a public forum, and anyone who engages in criminal
> activity on a mailing list is pretty stupid. But the FBI has no
> right to engage in systematic monitoring of the net as a whole.

PUBLIC forum. Would you have the police/FBI/other agency stop reading the newspapers, listen to radio, or talk to people on the street in order to develop leads on crimes? And why not systematic monitoring? I doubt that the FBI finds my questions on Unix that interesting :-). As for my political views, well, if I choose to make PUBLIC statements on the net, I expect that somebody might hold me to them. Just what are we afraid of anyway? If you find some basis in the LAW, as opposed to your opinion, that monitoring of a public forum by law enforcement agencies is prohibited, I would love to see it. However, I doubt that such a law exists.

-Andrew D'Uva ard@ctcg.COM {backbone}!uupsi!ctcg!ard

Re: the FBI and computer networks (Agre, RISKS-11.72)

Phil Windley <windley@panther.cs.uidaho.edu>
Thu, 30 May 91 13:58:35 PDT

Andrew R. D'Uva (ard@ctcg.com) writes:

> As for the .SU domain, if the boys at the FBI don't know that there are electronic links to machines in the Soviet Union, you can be certain that the fellows up at the NSA do.. and might even be doing something about it.

The Naval Investigative Service (NIS) knows about it. I told them. As a Naval Reserve officer I'm required to report all contact with citizens of certain countries to NIS (so that the NSA doesn't pick it up and the NIS start an investigation of something innocent).

I received mail from someone in the SU. I informed NIS who asked the nature of the contact. That done with, the agent was extremely interested in the fact that the network existed and that I could send mail from my desk all over the world. I taught her about routing and showed her that it had taken 3 hours for the mail to get from the SU to Finland and 30 seconds to get from Finland to Idaho.

As an aside: the mail was routed through kremvax.hq.demos.su. Anyone know

where this computer is? I couldn't get a direct IP address for it.

Phil Windley, Assistant Professor, Department of Computer Science
University of Idaho, Moscow, ID 83843 208-885-6501 Fax: 208.885.6645

> [Sounds like Piet Beertema is at it again!??
> Or another inspired spoofer?
> But not long ago it was April. PGN]

Re: Voting by phone

<AURKEN@VAXC.STEVENS-TECH.EDU>
Thu, 30 May 1991 00:21 EST

Three comments on Roy Saltman's paper. First, voting by phone enables a citizen to verify that his/her vote is actually counted, which is something that is practically impossible to do with existing election technologies. Second, voting transactions can be time-stamped to help guard against fraud and also enable voters to verify the handling of their vote. And third, allowing voters to vote for "none of the above" is an improvement on the normal method of voting, but there are strong scientific arguments for allowing citizens to cast one vote for each choice (a candidate or policy alternative) they approve and zero votes for those choices they reject. The indifference of "none of the above" can be expressed by casting 0's or 1's for all of the choices. This method is much more likely to identify the strongest choice in voter preference orderings.

Imagine what would happen if voters could access online statements about candidates or issues provided by parties or interest groups!

Arnie Urken

Re: Vote by Phone

Doug Hardie <doug@NISD.CAM.UNISYS.COM>
Thu, 30 May 91 8:20:42 PDT

I am concerned about several aspects of such a proposal. There is no question that such functionality can be created. The question is can it fit acceptably into our society. For example, there has always been an opportunity for poll watchers to challenge the registration of specific voters and their right to vote. With this technology, that is not easily possible. The only real way to permit such challanges is to record each person's vote such that a successful challange could cause the vote to be backed out. With this system there is no confidentiality of vote. Everyone's vote is available to someone.

The security aspect I didn't see addressed was how do you protect the computer collecting the votes from tampering by its users? If I am interested enough in influincing the outcome of a election, I will position myself such that I am an operator of such a system. At that point, I think you have lost control of the outcome. Case in point: When I was in college there was a highly contested election for homecomming queen. Two organizations were highly organized and

dominated the scene for many years: the marching band, and ROTC. As a member of both organizations, I found the process quite interesting. Voting was accomplished with mark-sense cards that were run through a fancy machine to convert the pencil markings to BCD. Then the cards were run through a simple counting program on the school computer. I was the acting director of the computer center and therefore had the ability to stay in the computer center during the counting and watch.

The outcome of this "election" was so important that one of the ROTC participants who was a journalism major arranged for one of the San Francisco TV stations to have a live report from the computer room. The operator of the computer was a relatively unknown band member. Sometime during the middle of the count, the computer suddenly crashed. But no panic, no need to rerun the count, the operator knew what the counts were at that time, reset them by hand from the front panel and continued the count. All of this took place during the live feed. The ROTC reporter was suitably impressed by this show of technical competance to make a comment on the air about the benefits of electronic voting. Needless to say, the band candidate was elected.

-- Doug

Re: Vote-by-Phone

Martin Ewing <ewing-martin@CS.YALE.EDU>
Thu, 30 May 91 11:59:13 -0400

I am sure you [Roy] will receive a large number of responses to your carefully prepared piece on voting using voice-response systems. My particular focus is on the human-machine interface.

Limitations of VRS for complex transactions: I have used a number of VRS systems. The most complicated is Fidelity Investments FAST system, through which you can transact mutual fund purchases, as well as obtaining account balances and quotations. Fidelity's system requires you to enter a lengthy account number, a PIN, and various codes for fund numbers, etc. The voice prompts are good, and it is possible to do a lot of business this way. At the end of a transaction specification, you are given a accept/reject option and a transaction reference code if you do accept.

All these transactions can be handled alternately by phone with a human operator. It would be interesting to have Fidelity's statistics about VRS vs. live preferences among its customers. My strong feeling is that the system would appeal to technical computer/financial people, but would be very unappealing to people who are unused to menu-driven state machines, which, after all, are what VRS systems are.

The standard telephone (which is not even guaranteed to be touchtone) is an extremely limited computer I/O interface. It offers no immediate status information to help users understand where they are in the system, what choices will be coming up, what the alternative routes through the logic might be. Verbal prompts are entirely "local" to the situation the user is in at the moment. This is a very synthetic and un-lifelike interface, even for computer people. (Consider all the cues you have sitting in front of a Mac or X Windows

screen, for example.)

Furthermore, as a recent ex-resident of California, I can attest that voting can be considerably more complex than financial transactions. Basically, I think VRS is woefully inadequate when you may have 50 contests on a ballot, with lots of minor parties, etc. I would suggest that a little "consumer preference" research could be done with mocked up VRS systems to shed more light.

The Ideal Voting Interface: In Pasadena, we used the (sigh!) Hollerith Card voting system, in which you used a stylus to punch a hole in a suitably framed card. I feel this is a nearly ideal system. The card is a physical object which has the right data capacity, which the voter can manipulate before and after voting, and the kinesthetics are pleasing. "Chunk!" for each candidate. You can pore back and forth across the contests, and there is room in the book-like card holder for a fair amount of explanatory text. The cards are designed for machine reading. (Last time I heard, they were using 360/20s!)

In Connecticut, we now use voting machines. These inspire a lot less confidence for me. You pull a lot of toggles, the the big lever. There is no physical feedback that your levers actually did anything. There is very limited room for text, etc. The legends above the levers are inserted manually, and, if they slip a little, you can end up casting your vote in the wrong column. (I actually discovered this situation in a recent election.) Furthermore, the many unused levers are not blocked, so that is very easy to cast meaningless votes. The old-fashioned "advantage" of the mechanical systems is that you had the "party-line" lever, to vote all Democratic, or whatever. Fortunately, those levers are now disabled.

I am sure that an electronic interface, based perhaps on ATM technology, could be developed to handle the authentication and the logical details of voting. I am not sure, however, that these systems can give an appropriate level of voter comfort and confidence, which are extremely valuable for the political process.

Martin Ewing, Science & Engineering Computing Facility, Yale University

---

vote-by-phone

Margaret Fleck <fleck@robots.oxford.ac.uk>
Thu, 30 May 91 15:42:53 BST

When reading your recent posting on vote-by-phone on the risks newsgroup, I was puzzled about why you assumed the system would handle only push-button phones. There exist similar systems that can handle both dial and push-button phones: the US embassy in London uses one for its visa information line. This system uses only the digit 0, which can be used even for multiple-choice queries if you are patient, and performs an initial calibration step to discover what your 0 sounds like.

Margaret Fleck (University of Oxford)

Vote-by-Phone (Security)

Tony Harminc <TONY@VM1.MCGILL.CA>
Thu, 30 May 91 15:17:36 EDT

It needs to be remembered that the weakest link in a Vote-by-Phone system will be the voter. I can easily think of several tricks along the lines of the "phony bank inspector" often perpetrated on the elderly that could be done here. Automated dialing out to elderly voters a day or two before voting day with a message to "please enter your PIN for voting validation" would probably produce a large harvest. These could then be voted early in the day. Many people wouldn't complain - it's not clear what to do about those who do. Vast amounts of advertising telling people not to give out their PINs will just confuse the most vulnerable.

Tony Harminc

Re: Voting By Phone (Huggins, RISKS-11.71)

Matt Fichtenbaum <mlf@genrad.com>
Thu, 30 May 91 15:39:09 EDT

> ... The main motivation behind the amendment was to provide easier ways to
>vote for disabled Americans who may find it difficult to reach a polling place.

I hadn't realized that any such disabled Americans were running for office.

(Isn't English ambiguity wonderful?)

Matt Fichtenbaum

[Triply ambiguous. There is also the motivation to make it easier for people who want to vote (illegally) INSTEAD OF disabled Americans who would probably not be voting. That of course is ONE OF THE MAIN PITFALLS OF VOTE-REMOTE... PGN]

Re: Vote-by-Phone

William Clare Stewart <wcs@erebus.att.com>
Thu, 30 May 91 16:23:27 EDT

Vote-by-Phone, in addition to the usual risks about security, provides another marvelous opportunity for manipulating elections. Not only is the order of name presentation critical (as with paper and machine ballots, where layout manipulation is de rigueur), but vocal expression of the names and parties is also manipulable. In many places, such as New Jersey where ballot questions are written by the Legislature, with hopelessly biased "explanations" of how good the proposed law will be. Now they can do things like

(Happy, excited voice) Honest! George! Tweedledee!, Democrat!, Press 1!
(unimpressed voice) Walter Fritz Tweedledum, Republican, press 2

(If-you-really-must) Gene? um bbBurns? um LLLiberaltarian? um press 3
Oh, yeah, and for Alfred E. Anarchist, Down-With-Lawyers-Party Press 4

While it's not as effective as manipulating TV and press coverage,
most elections are decided by only a few percentage points.

Bill Stewart 908-949-0705 erebus.att.com!wcs AT&T Bell Labs 4M-312 Holmdel NJ

Vote-by-Phone - Promises and Pitfalls

Erik Nilsson <erikn@boa.mitron.tek.com>
Thu, 30 May 91 15:55:05 PDT

Studies of computerized vote counting (including Saltman's own extensive and insightful papers) reveal that user interfaces for existing computerized vote counting systems are inadequate. Vote-by-phone user interfaces promise to be worse yet. The telephone is just too narrow an interface for modern elections. At least with current systems you can see the task before you, and see your choices, once you have made them. At least with current systems you can skip the wording of a proposition, if you already understand it. In some elections, voters would spend most of their voting time listening to paragraph after paragraph of legally required proposition text, financial impact statements, and so forth. I find such a prospect less handy than my local polling place.

Even blind voters, who cannot take advantage of the visual user interface of current systems, may not find voting by phone such a boon. Currently, blind voters must have assistance to vote, but the assistant is a better interface than a phone. Just because a phone interface is no worse for blind voters than for sighted doesn't mean that phone interfaces are good interfaces for blind voters. There are better ways of helping blind voters than voting by phone.

People complain about the awkwardness of voice-mail, but vote-by-phone would have to be even more awkward: "Soil conservation board, vote for two. You have voted for zero candidates so far. If you wish to vote for candidate Washington, push 1, if you wish to vote for cadidate Jefferson, press 2, if you wish to vote for candidate Adams, press 3. If you wish to write in, press #, if you wish to spoil this ballot and start over, press *, if you wish to skip this constest, press # twice, if you wish to review your current choices for this office, press * twice, if you wish to hear your choices again, press # then press *." It is not clear to me that voter participation and drop-off would improve under such a system.

Saltman's article brings up many other important concerns. For example, making such a system secure would be difficult. As it stands, most observers council against sending unencrypted voting information over telephone lines. This system requires it.

Voting by phone? No thanks. - Erik

erikn@boa.MITRON.TEK.COM (503) 690-8350 fax: (503) 690-9292

Re: Vote-by-Phone - Promises and Pitfalls

Paul E. Black <paul@cirrus.com>
Thu, 30 May 91 16:20:29 PDT

My compliments. It sounds like you have thought this through well. A few thoughts occurred to me. Perhaps they may be of use to you. Here in California each voter already gets an individually addressed voter guide. Some of my suggestion only make sense where each voter gets something before hand. I twice served on the local election board (precinct clerk), so I have seen how people actually vote with the current system.

Identification: the PIN could be randomly assigned to each voter and sent with the voter's guide. If the PIN is associated with a voter's name, PIN's could be repeated: they would be pass codes. The voter states his name, which is recorded for auditing, and enters it through the keypad. The pass code confirms it.

Write-in votes: Instead of, or in addition to, write-in names entered through the keypad, the voter states the name vocally, and it is recorded. With a pre-mailed voter's guide, the voter could figure out the number codes corresponding to the name before calling.

Confirmation: I think it would inspire more confidence in the voters if after each vote the system repeated, "You voted for <name>. Press 1 if that is correct, otherwise press 2." Anything other than 1 causes the system to prompt for the vote again. (Clearly anything can be used instead of 1 and 2 as long as it is consistent. Perhaps 9 (Y) for yes and 6 (N) for no.)

Serial presentation: the voter's guide tells which number corresponds to each person. The voter is told that they can enter the number at any time. Thus voters with premarked ballots could go through the system rather quickly.

Another option or a refinement is to go through the names quickly the first time (e.g., "For president Washington, 1; Jefferson, 2; or Franklin, 3") then if the system does not detect an entry, detects an invalid entry (e.g. "4" in the above), or detects a help button ("#" maybe?), it reads the names in greater detail (e.g., "For president of the United States, to vote for George Washington, Whig, press 1; to vote for ...")

Overvote and undervote: In a election where it is "Vote for up to 3 of the candidates," the system states how many are left: "You voted for Jones, you may vote for up to 2 more." The voter may then cancel that vote, or not vote for the rest. The voter cannot overvote. If an undervote is not allowed ("vote for exactly 2"), the system refuses to continue (with the appropriate message) until all votes are cast or the voter indicates the desire to not vote on that at all.

Failure to complete: In case of hang up, either because of emergency or equipment failure (or accidentally bumping the 'phone), the safest thing is to erase the entire proceeding to that point, except to note in the database that a vote was interrupted (like a spoiled ballot). Perhaps after three failures, the system directs the person to talk with election officials.

Audit & accountability: the entire voting procedure should be recorded in as raw a form as feasible. Perhaps a slow tape like used for 911 would do. If not, a record of each input keystroke and a code indicating the system's message could be written to a write-only media such as optical disk.

Trial & development: perhaps Federal funding could help develop and test the concept and answer questions in a few areas for a few years. Another possibility is having an organization like ACM, IEEE, or a university try it out: they want to innovate, and those voters would tend to be more careful, give useful suggestions (i.e. help development) than the population at large. The results would not be fully extensible to the population at large, but it could be a place to start.

I feel the problem with low voter turn-out is a social, not a technical, problem. With the LONG hours and absentee ballots now available, there is really very little excuse for people not voting. I'm afraid the length of time voting over the 'phone or waiting to get a line would be seen as a similar inconvenience.

I hope this may be of some help.

Paul E. Black, CIRRUS LOGIC Inc MS 62, 3100 Warren Avenue, Fremont CA 94538 USA
{ames,uunet,amdahl,sun}!oliveb!cirrusl!paul paul%cirrusl@oliveb.ATC.olivetti.com

Search RISKS using swish-e

THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

ACM Committee on Computers and Public Policy, Peter G. Neumann, moderator

Volume 11: Issue 77

Friday 31 May 1991

Contents

Yet another "stupid computer" example

Allan Duncan <a.duncan@trl.oz.au>
Fri, 31 May 91 15:06:09 EST

More in the continuing saga of man versus machine.

Here are a couple of letters that appeared in the The Age (Melbourne, Australia). There is a sting in the tail.

Allan Duncan, Telecom Research Labs, PO Box 249, Clayton, Victoria, 3168, Australia (+613) 541 6708 {uunet,hplabs,ukc}!munnari!trl.oz.au!a.duncan

= =

15 May 91

I have discovered that The Bed of Procrustes still exists and, daily, people are being stretched or lopped to fit. Nowadays, it is called the Computer.

At birth, I was named Charles Edward Williams and, since my father was also named Charles, my family called me Ted, as an abbreviation for Edward. Consequently, I muddled along for 60 years as Ted/C.E./Charles Edward Williams. The exact term depending upon the formality of the occasion.

This state of affairs came to an abrupt end a few years ago, when the Department of Veterans Affairs tucked me under their wing. Immediately I became Charles E. Williams, and my feeble protests were brushed aside.

At first it mattered little, as the postman still delivered their mail, and the bank accepted their cheques. But as I found myself spending more time in waiting rooms, it became quite embarrassing to wake up and realise that the "Charles Williams" they were calling for the fourth time was me.

Recently, I asked DVA that, if they must adopt this American usage, would they at least employ it correctly, ie would they in future please address me as C. Edward Williams?

A few days ago I received a phone call from a young lady at DVA who said that, if I wished, they would address me as Edward C. Williams. In horror, I drew her attention to the vast legal implications of such an act. She stated, categorically, that the first given name must be the one spelled out, otherwise their computer could not cope.

Now I am not vindictive, but I believe any EDP manager who recommended the procurement of a computer system so inflexible that it cannot handle such a small variation from the commonplace deserves to be publicly executed.

C. Edward Williams

30 May 91

Always give credit where it is due. After my letter (15/5) a very "computer literate" gentleman from Veterans Affairs contacted me to say that henceforth, I will be addressed as C Edward Williams, instead of the present Charles E Williams. All that remains to be done is for their computer to inform all of its fellows of my change of name. DVA regrets that they cannot follow the C with a full stop. An attempt to do this causes the machine to have a fit of electronic epilepsy.

C. E. Williams

Will the real kremvax please stand up (Windley, Moscow ID)

<smb@ulysses.att.com>
Thu, 30 May 91 21:22:56 EDT

kremvax.hq.demos.su. is quite real. There is no direct IP connectivity; mail to the USSR is routed through assorted gateways selected via MX records. The good folks at Demos (a ``co-operative'') are quite aware of the story of kremvax; its use as a machine name is hardly co-incidental.

But really -- you're questioning the authenticity of such a machine name, when you're allegedly posting from a place named ``Moscow, Idaho''. A likely story.

--Steve Bellovin

---

kremvax.hq.demos.su (Windley, RISKS-11.76)

Douglas W. Jones <jones@pyrite.cs.uiowa.edu>
31 May 91 02:44:11 GMT

> The Naval Investigative Service (NIS) knows about it. I told them.

And I spoke to my congressman about it back in October '90 when the link to Moscow first came to my attention. Most important of all, though, the people at DEMOS registered the .su domain with the people at the Defense Data Network Network Information Center who manage assignment of top-level domain names. Yes, the government knows, but as is common with organizations that large, there is a sense in which they probably don't know that they know.

kremvax.hq.demos.su is in the headquarters of DEMOS software in Moscow (the domain name tells you most of that). DEMOS is acting as the gateway to the west for the RELCOM network in the USSR. Soon after the initial connection between DEMOS and the rest of the world, I sent a copy of Piet Beertema's great kremvax/kgbvax hoax to Vadim Antonov at DEMOS, and he said it was great fun. I gather it was fun enough that they copied some of the machine names.

Doug Jones

[Similar observations to those above from:
Michael O'Dell <mo@gizmo.bellcore.com>
David Fetrow <fetrow@orac.biostat.washington.edu>
Charles (C.A.) Hoequist <HOEQUIST@bnr.ca> .
I was going to wait to put out this issue, but decided to do it now in order to stave off a further flood of responses. PGN]

---

kremvax (Windley, RISKS-11.76)

Russ Nelson <nelson@sun.soe.clarkson.edu>
Fri, 31 May 91 10:24:56 EDT

The Soviets are neither stupid, ignorant nor humorless. DIG says:

```
;; ANSWERS:
kremvax.hq.demos.su.    345600  MX  100 fuug.fi.
kremvax.hq.demos.su.    345600  MX  120 nac.no.
kremvax.hq.demos.su.    345600  MX  200 mcsun.eu.net.
```

In my experience, the folks at hq.demos.su are hackers in the AI lab tradition, and not above a little tomfoolery.

Vote-by-Phone - Promises and Pitfalls (Saltman, RISKS-11.75)

David Canzi <dmcanzi@watserv1.waterloo.edu>
Fri, 31 May 91 00:19:34 EDT

Sure, the computer can be programmed to protect the voters' privacy. It can also be programmed not to, and the voters told otherwise. They will have no way of knowing. You can even show them source code for a vote-collecting program that respects their privacy. They have no way of knowing that that is the program that will actually be run.

If both the verification of the voter's identity and the collecting of votes are done by phone, I don't see how there can be any secret ballot without depending excessively on the honesty of those running the polls.

(I don't know how many things Americans typically get to vote on in an election. Assuming that the voter's social security number and vote can be encoded in 15 bytes or less and that there are about 150,000,000 voters, it'll all fit on one Exabyte tape.)

David Canzi

Vote by Phone (RISKS-11.76)

Erik Nilsson <erikn@boa.mitron.tek.com>
Thu, 30 May 91 19:23:41 PDT

AURKEN@VAXC.STEVENS-TECH.EDU writes:

> voting by phone enables a citizen to verify that his/her vote is
> actually counted, which is something that is practically impossible to
> do with existing election technologies.

All of the vote verification schemes that I am familiar with will work for paper, DRE (see below), and phone ballot methods. Any method that works for phone balloting can in principle be made to work for the other methods, using the following technique: For each ballot, the counting board calls a computer and re-votes the ballot by phone, thus using whatever verification scheme is proposed. Obviously, practical systems would probably omit the phone :-).

Vote verification is of little value without assurance that people who didn't vote weren't counted. Since voting by phone has no signatures, voting the dead is much easier. An inside operator could also monitor who has voted, and have confederates jam in last minuted calls using the IDs of people who hadn't voted, stuffing the ballot box. A wide variety of vote fraud techniques are facilitated by vote-by-phone, and a few new ones are doubtless created.

> voting transactions can be time-stamped to help guard against fraud

How does this guard against fraud? I'd much rather have a paper trail that takes large amounts of effort in a short amount of time to

undetectably wedge than a time-stamp that can be easily mass-produced
by a computer.

> allowing voters to vote for "none of the above" is an improvement on
> the normal method of voting

What has this got to do with voting by phone?

doug@NISD.CAM.UNISYS.COM (Doug Hardie) writes:

> The question is can it fit acceptably into our society. For example,
> there has always been an opportunity for poll watchers to challenge
> the registration of specific voters and their right to vote.

This is one of the things I don't like about vote-by-mail. With
elections officials pushing for easier permanent absentee ballots,
many states that don't have vote-by-mail are headed toward de facto
vote-by-mail. At least with vote-by-mail, you have a piece of paper
with a signature to challenge.

> how do you protect the computer collecting the votes from tampering by
> its users?

This is a problem even without vote-by-phone, as Hardie points out.
Vote-by-phone just makes it worse.

Martin Ewing <ewing-martin@CS.YALE.EDU> writes:

> I have used a number of VRS systems. The most complicated is Fidelity
> Investments FAST system

I have also used this system, although mainly just to change my default
password to make snooping on me harder. I'm a technical computer person, and I
found the system annoying, because the system repeatedly asks for the same
information over and over. Vote-by-phone would have to be even more
complicated, and probably would have less financial resources than FAST,
resulting in a less robust design.

> The standard telephone ... is an extremely limited computer I/O interface.

You said it.

> In Pasadena, we used the (sigh!) Hollerith Card voting system ....
> In Connecticut, we now use voting machines. These inspire a lot less
> confidence for me.

See Papers by Roy Saltman, Lance Hoffman, Howard Strauss and myself on the
problems with both of these systems. Ron Dugger had an article in the New
Yorker, and Eva Waskell has written several articles. Send me personal mail if
you'd like to see a more complete bib.

> I am sure that an electronic interface, based perhaps on ATM technology,

> could be developed to handle the authentication and the logical details of
> voting.

It already has been developed. They are called Direct Recording Electronic (DRE) machines. The current crop suffers from many of your mechanical complaints. A carefully designed second generation of these machines would ease many of our vote counting worries.

- Erik Nilsson erikn@boa.MITRON.TEK.COM

Re: the FBI and computer networks (D'Uva, RISKS-11.76)

<smb@ulysses.att.com>
Thu, 30 May 91 22:44:00 EDT

I fear we're wandering very far afield; I'll attempt to get in one last letter before our esteemed moderator cuts us off.... [Tnx.P]

I spoke a bit loosely when I used the phrase ``probable cause''; that's a technical term, and does not (quite) apply. Nevertheless, I stand by the substance of what I said. The FBI is not allowed to engage in systematic monitoring of speech without reasonable suspicion of criminal activity. The intent of the ban is twofold: to prevent the chilling effect of constant police surveillance on legal but controversial opinions, and to guard against abuses of official authority. The record amply supports both fears.

Certainly, a police officer may take appropriate action if he or she happens to observe an illegal act. If that act is observed through legitimate participation in a public forum, the officer is not thereby disqualified from acting. But monitoring without reasonable grounds to suspect *illegal* speech -- and precious little speech is illegal -- is not permitted. (Let me amend this statement a bit. Monitoring is allowed if demonstrably relevant to an actual criminal investigation.)

I'm not sure what you meant when you dragged in the war on drugs in D.C. The activists I mentioned in my initial letter were making controversial political statements, very much ``anti-establishment''. The monitoring was an outgrowth of the same mentality that produced local police ``Red Squads''.

To be sure, I'm not 100% certain whether these bans are statutory, regulatory, or judicial. I'll do a bit of checking and see what I can learn. Or perhaps one of the attorneys reading this list can provide a precise citation (or contradiction)?

--Steve Bellovin

Two books on privacy that may be of interest

<ts@cup.portal.com>
Thu, 30 May 91 23:03:00 PDT

Here are two books that may be of interest to those who have been

following the privacy discussion on RISKs:

"Your Right To Privacy" (subtitled "A Basic Guide To Legal Rights In An Information Society"), ISBN 0-8093-1623-3, published by Southern Illinois University Press, is one of a series of books from the ACLU. This is the second edition, and was published in 1990, so should be reasonably up-to-date.

One of the authors is Evan Hendricks, editor/publisher of "Privacy Times", and the other two authors are ACLU lawyers who work in the area of privacy.

Here's the table of contents:

The other book of interest is called "Low Profile" (subtitle: "How to Avoid the Privacy Invaders"), by William Petrocelli, published by McGraw-Hill Paperbacks in 1982, ISBN 0-07-049658-7. It includes interesting sections on bugs and on annoying people who you think are taping a meeting (whenever you would normally say "yes" or "no" in response to something, just shake your head -- this will drive the person taping you up the wall). Otherwise, it covers much the same ground as the ACLU book above (warning: I haven't finished either book yet, so I may be mistaken here!), although more emphasis is placed on protecting privacy from hostile people such as competitors.

Tim Smith

Credit reporting

Paul Schmidt <prs@titan.hq.ileaf.com>
Fri, 31 May 91 08:04:13 EDT

It strikes me that there is a fairly easy way for people to find out who is accessing their credit reports. Require that the data bank administrators immediately send mail to the person describing what was accessed, and for who. These letters could easily be computer generated, and the mailing costs included in the charge for the credit report.

I imagine things will get interesting when the people start to discover how many places their credit history is being sent.

More on Lossy Compression (ACM SIGSOFT SEN v16n2 p.5)(SEE RISKS-11.21)

David Reisner <synthesis!dar@UCSD.EDU>
Thu, 30 May 91 00:11:25 PDT

In the editor's note at the end of "Medical image compression & fertile ground for future litigation" [in _Software Engineering Notes_, adapted from RISKS-11.21 and subsequent commentary], PGN suggest that a lossless image compression algorithm may become lossy in the presence of noise. I presume Mr. Honig will comment on this, but just in case he doesn't, I hope this input will be useful.

There are, in fact, lots of compression algorithms that ARE lossy. They do not reconstruct the original data upon decompression, but rather data which is "acceptably close" by some measure. Obviously, these are not appropriate methods for traditional computer data (e.g. databases, text), but may be perfectly acceptable for other types of data (e.g. images, sound), depending on the application.

For example, the "fractal" image compression technique which has received a fair bit of attention over the past 18 months reconstructs only an approximation of the original image. The algorithm can be applied iteratively, and will produce a "better" image after each iteration, up to some limit. The relatively recent (and very useful) JPEG image compression standard is also "lossy" - only approximates the original image.

Both of these systems exhibit losses or "infidelities" that are mathematical in nature; they are at a level which is considered acceptable, but are not specifically engineered to be innocuous in the application domain. Mr. Honig's comment "discussion about how compression schemes could exploit the (finite) resolution of the human visual system to send only the information that was perceivable", strongly suggests that they are considering application domain specific types of compression and loss.

A current example of such a scheme is the Digital Compact Cassette (DCC) compression scheme developed by Philips, which uses about 1/4 the data rate of a Compact Disc (CD) to reproduce sound which is hoped to be indistinguishable from the CD. Philips developed an algorithm which is heavily based on human psychoacoustics (particularly hearing threshold curves and masking phenomena). The algorithm was then refined using the evaluations of trained listeners - a very unusual step (as opposed to using only "mechanistic" objective measurements).

Stepping back more directly to RISKS, when using these "lossy" methods, it may be difficult to know what data will be reproduced inaccurately (particularly when viewed from a domain-dependent "structural" perspective). Philips attempted to test and "measure" the quality of their algorithm in (an approximation of) the actual application domain, but they cannot KNOW that it will be successful for any given listener or program (music/sound) signal. For medical image compression, losses which are either not detected or determined to be unimportant in the testing and development process COULD cause injury or loss of life if they are of consequence during (potentially atypical) actual application. Thus, it would seem far safer to use the most rigorous imaging and transmission schemes possible, only trading off the costs of inability to transmit (due to financial or technical factors) versus "imperfect" transmission.

If "lossy" schemes are used, designers and users will need to understand (to the extent feasible) the quality/reliability of the information they are actually dealing with. Unfortunately, as when the calculator supplanted the sliderule, and as computer packages with preprogrammed algorithms supplant the calculator, people tend to loose a "gut feel" for the accuracy, and even reasonableness, of their answers (as well as loosing sufficient understanding to be able to innovate - a whole other type of "risk").

David Reisner, Consulting, Los Angeles CA USA (213)207-3004

Search RISKS using swish-e

THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

ACM Committee on Computers and Public Policy, Peter G. Neumann, moderator

Volume 11: Issue 78

Monday 3 June 1991

Contents

Lauda Air Crash

Paul Leyland <pcl@convex.oxford.ac.uk>
Mon, 3 Jun 91 13:36:39 +0100

The Times (London), Monday June 3rd 1991.

Lauda says crash engine failed

New evidence that the crash of a Lauda Air Boeing 767-300 in Thailand had been

caused by in-flight reversal of the thrust on one engine has stunned the aviation industry. Niki Lauda, owner of Lauda Air, made the claim in Vienna after returning from Washington, where the flight data and cockpit voice recorders of the jet were being analysed. The Austrian transport ministry supported the assertion. If the diagnosis were confirmed, the accident would be unprecedented, Herr Lauda said. The crash investigators have yet to comment.

The computerised airliner's systems have the capacity for self-analysis and should have corrected such a basic error. Reverse thrust is normally locked out during flight and only used on the ground. It is thought to be virtually impossible for reverse thrust to be deployed when the engine is pushing at maximum, as the jet would have been. The incident happened about 16 minutes after takeoff.

Investigators for Boeing, which manufactured the thrust reversers, were allowed access to the crash site for the first time on Friday. Herr Lauda said the flight data recorder was damaged and could not be used to analyse the crash. He said the cockpit voice recorder indicated an advisory light had come on seconds before the crash and that a voice was heard saying the light was glowing intermittently. Seconds later, First Officer Josef Thurner was heard saying: "It deployed." Herr Lauda took that to mean the reverse thrust was engaged. The entire incident, from the moment of the first warning light until the plane broke up, took no more than a minute. Last night a spokesman for the Civil Aviation Authority said that no checks were to be ordered immediately on 767s owned by British airlines.

LaudaAir Boeing 767-300 crash in Thailand

Carsten Wiethoff <cnwietho@immd4.informatik.uni-erlangen.de>
Mon, 3 Jun 91 11:57:10 MET DST

[...] Private Speculation: Could it be something like a simple overflow/sign error to cause the engine go from max forward to max backward thrust?

Lauda air plane crash

Ralph 'Hairy' Moonen <rmoonen@hvlpa.att.com>
Mon, 3 Jun 91 08:51 MDT

[...] Now when the media make something out to be a computer error, they hardly ever are specific. What I want to know is, was it a hardware error, or a software error. And certainly, wouldn't a mid-air reversal of thrust just rip off the wing, leaving the plane to plummet down totally out of control? Any air-experts out there willing to comment on this?

--Ralph Moonen

Tiland air crash

Mark Evans <evansmp@uhura.aston.ac.uk>
Mon, 3 Jun 91 10:04:16 +0100

[...] However the reverse thrust system is only used on landing. It would appear unlikly (not least because of the safety aspects) that reverse thrust in NOT under the direct control of the flight management system. Also mentions mechanical interlocks, these are presumably in addition to the hydrolic systems actuating the thrust deflectors being turned off. The principle is quite simple. The thrust deflectors are locked in place unless the plane is on the ground (also landing gear is down) and the control in the cockpit is activated.

Mark Evans, University of Aston, Birmingham, England

Re: AFTI-F16 (RISKS-11.61, 62, 64)

John Rushby <RUSHBY@csl.sri.com>
Sat 1 Jun 91 16:15:06-PDT

For RISKS readers interested in digital flight control systems (DFCS), I highly recommend the papers by Mackall and his colleagues on the AFTI-F16 (and some other) flight tests; [4] is particularly thorough and informative.

The following extracts from [6] summarize some of the points (fairly, I hope). It seems that redundancy management became the primary source of unreliability in the AFTI-F16 DFCS. *'s indicate footnotes; they, and the references are given at the end.

John

- -

A plausibly simple approach to redundancy management in an N-modularly redundant system is the "asynchronous" design, in which the channels run fairly independently of each other: each computer samples sensors independently, evaluates the control laws independently, and sends its actuator commands to an averaging or selection component that chooses the value to send to the actuator concerned. The triplex-redundant DFCS of the experimental AFTI-F16 was built this way, and its flight tests reveal some of the shortcomings of the approach [2, 4].

First, because the unsynchronized individual computers may sample sensors at slightly different times, they can obtain readings that differ quite appreciably from one another. The gain in the control laws can amplify these input differences to provide even larger differences in the results submitted to the output selection algorithm. During ground qualification of the AFTI-F16, it was found that these differences sometimes resulted in a channel being declared failed when no real failure had occurred [3, p. 478]. *1 Accordingly, rather a wide spread of values must be accepted by the threshold algorithms that determine whether sensor inputs and actuator outputs are to be considered "good." For example, the output thresholds of the AFTI-F16 were set at 15% plus the rate of change of the variable concerned; also the gains in the control laws were reduced. This increases the latency for detection of faulty

sensors and channels, and also allows a failing sensor to drag the value of any averaging functions quite a long way before it is excluded by the input selection threshold; at that point, the average will change with a thump [4, Figure 20] that could have adverse effects on the handling of the aircraft.

The danger of wide sensor selection thresholds is dramatically illustrated by a problem discovered in the X29A. This aircraft has three sources of air data: a nose probe and two side probes. The selection algorithm used the data from the nose probe provided it was within some threshold of the data from both side probes. The threshold was large to accommodate position errors in certain flight modes. It was subsequently discovered that if the nose probe failed to zero at low speed, it would still be within the threshold of correct readings, causing the aircraft to become unstable and "depart." This error was found in simulation, but 162 flights had been at risk before it was detected [5].

An even more serious shortcoming of asynchronous systems arises when the control laws contain decision points. Here, sensor noise and sampling skew may cause independent channels to take different paths at the decision points and to produce widely divergent outputs. This occurred on Flight 44 of the AFTI-F16 flight tests [4, p. 44]. Each channel declared the others failed; the analog back-up was not selected because the simultaneous failure of two channels had not been anticipated and the aircraft was flown home on a single digital channel. Notice that all protective redundancy had been lost, and the aircraft was flown home in a mode for which it had not been designed--yet no hardware failure had occurred.

Another illustration is provided by a 3-second "departure" on Flight 36 of the AFTI-F16 flight tests, during which sideslip exceeded 20deg, normal acceleration exceeded first -4g, then +7g, angle of attack went to -10deg, then +20deg, the aircraft rolled 360deg, the vertical tail exceeded design load, all control surfaces were operating at rate limits, and failure indications were received from the hydraulics and canard actuators. The problem was traced to an error in the control laws, but subsequent analysis showed that the side air data probe was blanked by the canard at the high angle of attack and sideslip achieved during the excursion; the wide input threshold passed the incorrect value through and different channels took different paths through the control laws. Analysis showed this would have caused complete failure of the DFCS and reversion to analog backup for several areas of the flight envelope [4, pp. 41-42].*2

Several other difficulties and failure indications on the AFTI-F16 were traced to the same source: asynchronous operation allowing different channels to take different paths at certain selection points. The repair was to introduce voting at some of these "software switches." In one particular case, repeated channel failure indications in flight were traced to a roll-axis "software switch." It was decided to vote the switch (which, of course, required ad hoc synchronization) and extensive simulation and testing were performed on the changes necessary to achieve this. On the next flight, the problem was found still to be there. Analysis showed that although the switch value was voted, it was the unvoted value that was used [4, p. 38].

The AFTI-F16 flight tests revealed numerous other problems of a similar nature. Summarizing, Mackall [4, pp. 40-41] writes:

"The criticality and number of anomalies discovered in flight and ground tests owing to design oversights are more significant than those anomalies caused by actual hardware failures or software errors.

"...qualification of such a complex system as this, to some given level of reliability, is difficult ...[because] the number of test conditions becomes so large that conventional testing methods would require a decade for completion. The fault-tolerant design can also affect overall system reliability by being made too complex and by adding characteristics which are random in nature, creating an untestable design.

"As the operational requirements of avionics systems increase, complexity increases. Reducing complexity appears to be more of an art than a science and requires an experience base not yet available. If the complexity is required, a method to make system designs more understandable, more visible, is needed.

"The asynchronous design of the [AFTI-F16] DFCS introduced a random, unpredictable characteristic into the system. The system became untestable in that testing for each of the possible time relationships between the computers was impossible. This random time relationship was a major contributor to the flight test anomalies. Adversely affecting testability and having only postulated benefits,*3 asynchronous operation of the DFCS demonstrated the need to avoid random, unpredictable, and uncompensated design characteristics."

Footnotes

1: Also, in the flight tests of the X31 the control system "went into a reversionary mode four times in the first nine flights, usually due to disagreement between the two air data sources" [1].

2: However, the greater the benefit provided by DFCS, the less plausible it becomes to provide adequate back-up systems employing different technologies. For example, the DFCS of an experimental version of the F16 fighter (the "Advanced Fighter Technology Integration" or AFTI-F16) provides control in flight regimes beyond the capability of the simpler analog back-up system. Extending the capability of the back-up system to the full flight envelope of the DFCS would add considerably to its complexity--and it is the very simplicity of that analog system that is its chief source of credibility as a back-up system [2].

3: The decision to use an asynchronous design for the AFTI-F16 DFCS was because "the contractor believed synchronization would introduce a single-point failure caused by electromagnetic interference (EMI) and lightning effects" [4, p. 7] --which may well have been correct given the technology of the early 1980s.

References

[1] Michael A. Dornheim. X-31 flight tests to explore combat agility to 70 deg. AOA. Aviation Week and Space Technology, pages 38-41, March 11, 1991.

[2] Stephen D. Ishmael, Victoria A. Regenie, and Dale A. Mackall. Design implications from AFTI/F16 flight test. NASA Technical Memorandum 86026, NASA Ames Research Center, Dryden Flight Research Facility, Edwards, CA, 1984.

[3] Dale A. Mackall. AFTI/F-16 digital flight control system experience. In Gary P. Beasley, editor, NASA Aircraft Controls Research 1983, pages 469-487. NASA Conference Publication 2296, 1984. Proceedings of workshop held at NASA Langley Research Center, October 25-27, 1983.

[4] Dale A. Mackall. Development and flight test experiences with a flight-crucial digital control system. NASA Technical Paper 2857, NASA Ames Research Center, Dryden Flight Research Facility, Edwards, CA, 1988.

[5] Dale A. Mackall and James G. Allen. A knowledge-based system design/information tool for aircraft flight control systems. In AIAA Computers in Aerospace Conference VII, pages 110-125, Monterey, CA, October 1989. Collection of Technical Papers, Part 1.

[6] John Rushby. Formal specification and verification of a fault-masking and transient-recovery model for digital flight-control systems. Technical Report SRI-CSL-91-3, Computer Science Laboratory, SRI International, Menlo Park, CA, January 1991. Also forthcoming NASA Contractor Report.

Lottery bar codes no risk, spokesman says

Martin Minow 01-Jun-1991 1222 <minow@ranger.enet.dec.com>
Sat, 1 Jun 91 09:33:46 PDT

>From the Boston Globe, Friday May 31, 1991 "Ask the Globe":

> Q. The state lottery's instant tickets now have bar codes with which sales agents can verify both their validity and the winning amount. What is to prevent agents or lottery officials from "reading" the codes on unsold tickets and taking the big prizes for themselves?
>
> A. Lottery spokesman David Ellis tells us that, once an instant ticket is "read" by a bar-code reader, it is invalidated. If a previously read bar code is reread, the computer "flags" the ticket as "previously cashed" or "cashed-stolen." The bar-code reader, Ellis adds, is "the first step in a long and complex series of protections" built into the game by Richard Finocchio, the lottery's computer manager. "The security system," he concludes with pride, "is the envy of lotteries around the world."

In sending this to Risks, I am *not* suggesting that confidence in their security system is misplaced: I can think of several ways to implement this that, given acceptable security at the Lottery central computer, would prevent cheating. I can also think of several ways that would appear safe, but aren't. However, both the question and answer raise interesting questions of trust (and, as dear Pres. Reagan would say, verification).

Full disclosure: I play the lottery twice a year -- when they send me their advertising freebie. In four years, I've won exactly one dollar.

Martin Minow minow@ranger.enet.dec.com

Re: Viper (Randell, RISKS-11.73)

Pete Mellor <pm@cs.city.ac.uk>
Fri, 31 May 91 17:14:40 PDT

> The only civilian customer for the technology has been the Australian National
> Railway Commission, which at the end of 1988 adopted Viper as the core of a
> new signalling system. The Australians have now gone so far with developing
> the system that they would have difficulty switching to another technology.

When I last heard of them (see RISKS DIGEST 6.48, 7.18, 7.36, 8.41, 9.1), the Australian National Railway Commission was suing its commercial supplier (Charter Technologies??) for precisely the same reason that Charter is now suing MoD.

Peter Mellor, Centre for Software Reliability, City University, Northampton Sq.,London EC1V 0HB +44(0)71-253-4399 Ext. 4162/3/1 p.mellor@uk.ac.city (JANET)

Re: The FBI and computer networks (Bellovin, RISKS-11.77)

<TK0JUT1@MVS.CSO.NIU.EDU>
Fri, 31 May 91 14:36 CDT

smb@ulysses.att.com writes:

> I spoke a bit loosely when I used the phrase ``probable cause''; that's a
> technical term, and does not (quite) apply. Nevertheless, I stand by the
> substance of what I said. The FBI is not allowed to engage in systematic
> monitoring of speech without reasonable suspicion of criminal activity.

We can cavil over nuances of specific terms, but smb is essentially correct. The FBI (and other gov't agencies) are generally, either by statute or policy, prohibited from routine systematic monitoring of speech outside of specific investigatory needs. This includes routine monitoring by informants or undercover operatives. Although the practice may be otherwise (see "The FBI's Misguided Probe of CISPES" by Gary M. Stern of the Center for National Security Studies), current policies are still (on paper, at least) guided by the Attorney General's Guidelines on FBI Undercover Operations" (Jan. 5, 1981) that restricts the use of undercover investigation, which is the most Constitutionally dangerous from of monitoring.

There is surely nothing wrong with law enforcement agents, whether in a private or official capacity, participating in cybercommunication. The line is crossed when participation moves to surveillance, data acquisition, and record keeping as occurs in political surveillance. The Secret Service may have overstepped this line when it set up it's "sting board" (Dark Side) in 1988 in a way that seems, uh, "empirically disfactual" with the SS Director's account of it.

Jim Thomas

Re: Voting by phone

Bob Rehak <A20RFR1@MVS.CSO.NIU.EDU>
Fri, 31 May 91 14:53 CDT

I don't see how one can keep their anonymity in this vote by phone scheme. Passing laws against release of voter info or entrusting the security of the voter info to people makes me very nervous. Having people in the loop causes a security problem by definition. Would the people in charge of the 'voter' data center be willing to give up their right to privacy so we can monitior their activities so they can be stopped immediately if they try to divulge any voter information. Will the system be TEMPEST secured so no electronic eavesdropping is possible. Will the 'voter' data center be guarded by elite commandos sworn to defend it to the death.

As I see it, if the data is stored somewhere, sooner or later the good guys or the bad guys will get hold of it some way or another either legally or illegally. Once the genie is out of the proverbial bottle, it will be too late to put him/her back.

Imperfect as it is, I like the way the system is now. If people were really serious about voting, they would take the time to vote. Having a vote by phone system will only allow for more abuse and fraud as some earlier respondents have suggested.

Bob Rehak, DBA At Large, BITNET: A20RFR1@NIU

Re: Voting-by-phone (RISKS-11.75)

Larry Campbell <campbell@redsox.bsw.com>
Thu, 30 May 91 23:42:33 EDT

This (voting by phone) is a classic example of an attempt to solve a social problem by the misguided application of technology.

What, really, is the problem for which this is supposed to be solution?

Invalids? Travellers? We have absentee ballots that work quite well, thank you.

Low turnout? Just make election day a national holiday, as it is in most civilized countries (but not the US).

Electronic voting? Who needs it?

Larry Campbell The Boston Software Works, Inc., 120 Fulton Street
campbell@redsox.bsw.com Boston, Massachusetts 02109 (USA)

---

voting by phone

<AURKEN@VAXC.STEVENS-TECH.EDU>
Sat, 1 Jun 1991 06:59 EST

There is a tendency to assume that computer-based voting systems such as voting by phone are more risky. I say "assume" because all election systems are risky and depend on certain procedures being carried out with integrity. But anyone familiar with the manipulation of paper or mechanical voting systems would want clarification of the statement that voting by phone relies "excessively" on the honesty of the operators of the system. In fact, allowing the individual voter to check his/her vote avoids passive reliance on the integrity of election administrators.

In this connection, verification of one's vote is possible under paper voting systems and others, but computer-based systems make it easier for the citizen to initiate and carryout verification. I say this on the basis of 5 years of development work with experimental voting systems in a computer-networking environment.

Grave-yard voting is a problem, but it is not clear that the problem would be worse with computer-based (phone) voting. It might be less frequent and more difficult to employ such maniupulation depending on the method of verification used.

Re time-stamping: the latest schemes of time-stamping and cryptographic coding based on distributed (not centralized processing) do make it practically impossible to break the system. Put another way, the amount of information that needs to be collected to break the system is so great, that watch-guard programs would detect would-be criminals.

Finally, using "none-of-the-above" is an improvement on plurality voting, which truncates information about voter preference orderings and is therefore undesirable from a theoretical point of view. This may not seem directly related to voting by phone, but Roy mentioned it as a possibility and it seems reasonable to extend the idea to consider other methods of voting that do not distort the voting process. Moreover, voting methods are related in the sense that it is not trivial to use them. I have designed interfaces for computer-based voting with different methods of voting and found what works and what doesn't work. Interfaces for voting by phone must be designed based on extensive experimentation and we may find that it is infeasible to use voting methods that have desirable social consequences.

Arnie Urken

Re: The Death of Privacy? (Robert Allen, RISKS-11.71)

Brett Cloud <hexmoon@buhub.bradley.edu>
Sat, 1 Jun 91 15:37:15 GMT

I agree with the spirit of this posting. Since we can not have complete privacy, we have at least complete access for everybody. I can readily see the day come when liberty will have as part of its definition, the freedom to access information.

People who abuse the system, could have their access taken away. Much

along the same lines as a robber being sent to prison. Also, a person on parole could be given varying degrees of access as their behavior warrented.

PC's are becoming so cheap and powerful, that I can not see an effective monopoly being maintained for long by (m)any central power(s). The people will take back their own power.

While granted, I'd prefer to have more privacy, I think it would be better to KNOW that information about me is availible as a matter of course, rather than THINK the information is private--when a privilaged subset actually has access.

If we are going to have as much known about us as appears to be the case, then the only way to level the playing grounds is by letting everone have, as a matter of course, the SAME access, unless and until they abuse the trust implied by the system.

If people know that their actions can be/are looked at, maybe they'll think twice about what they say or do. Granted that this is a poor sub- stitute for a proper set of values or a good conscience(sp?), but I think few would dispute that many people in power could use a constant reminder that they are answerable to the people.

Brett

Re: Credit reporting (Paul Schmidt, RISKS-11.77)

"David A. Curry" <davy@erg.sri.com>
Fri, 31 May 91 14:52:44 -0700

If you belong to TRW's Credentials Service, this is one of the "features": any time anyone accesses your credit report, they send you a nice little blurb the next day such as (from when I applied for my Gold Card):

[... assorted introductory stuff ...]

The following companies have requested and received copies of your TRW credit files.

Date	Company Name and Address	TRW Number	Type of File
06-07-90	AMERICAN EXPRESS 4315 South 2700 West Salt Lake City, UT	3459491	Credit

[... stuff about where to call with questions ...]

TRW Credentials costs $35/year. For this, you get credit card protection, unlimited copies of your credit report, and the little notes above. They also let you enter in all your financial data, so that it can be retrieved electronically with your "access number" (like a PIN) by banks and such when you apply for loans - so you don't have to fill out the forms (in theory

anyway, I never tried it).

Before anyone re-starts the discussion about the rip-off/non-rip-off nature of this service, it should be pointed out that:

- Any time you are denied credit, you are entitiled by law to a *free* copy of your credit report from the credit bureau(s) which supplied the information to the lender. You can then dispute any incorrect info.

- You can get a copy of your credit report at any time from any credit bureau for (usually) $8 and some assorted pieces of I.D.

- You only get the little blurbs when someone accesses your TRW file. TRW is not the only credit bureau in the country, although it's certainly one of the largest. I believe Equifax and EDS offer similar services, though.

So, unless you want the credit card protection and the little blurbs when your file gets looked at, the service is a rip-off. Me, I like the little blurbs, find the service fairly well-run, check my credit report once or twice a year, and don't mind paying the $35.

--Dave Curry

Credit Reporting

<WHMurray@DOCKMASTER.NCSC.MIL>
Sat, 1 Jun 91 09:27 EDT

[similar comment...]

Isn't the market great? On the other hand, require them to do by law what they are already prepared to do for a fee? Guaranteed to cost you more.

In an information society it is possible for the credit worthy to obtain the credit in minutes that was, in an earlier time, available only to the most well established in days or weeks. In part because of this, we all enjoy higher levels of commerce and a standard of living that would not have come about with out it. When we look at the effects of all of this on privacy, we should not forget the reason that we put the system in place. Yes, WE; the collective we. We did it; it was not done to us. In remedying the difficulties, we must careful not to overlook or destroy the benefits.

Search RISKS using swish-e

THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

ACM Committee on Computers and Public Policy, Peter G. Neumann, moderator

Volume 11: Issue 79

Tuesday 4 June 1991

Contents

CREATORS ADMIT UNIX, C HOAX

Jim Horning <horning@Pa.dec.com>
Tue, 4 Jun 91 11:41:50 PDT

>>>>>>>>>>>>>>>> T h e V O G O N N e w s S e r v i c e >>>>>>>>>>>>>>>>

Edition : 2336 Tuesday 4-Jun-1991 Circulation : 8466

VNS TECHNOLOGY WATCH: [Mike Taylor, VNS Correspondent]
========== [Littleton, MA, USA]

COMPUTERWORLD 1 April

CREATORS ADMIT UNIX, C HOAX

In an announcement that has stunned the computer industry, Ken Thompson, Dennis Ritchie and Brian Kernighan admitted that the Unix operating system and C programming language created by them is an elaborate April

Fools prank kept alive for over 20 years. Speaking at the recent UnixWorld Software Development Forum, Thompson revealed the following:

"In 1969, AT&T had just terminated their work with the GE/Honeywell/AT&T Multics project. Brian and I had just started working with an early release of Pascal from Professor Nicklaus Wirth's ETH labs in Switzerland and we were impressed with its elegant simplicity and power. Dennis had just finished reading `Bored of the Rings', a hilarious National Lampoon parody of the great Tolkien `Lord of the Rings' trilogy. As a lark, we decided to do parodies of the Multics environment and Pascal. Dennis and I were responsible for the operating environment. We looked at Multics and designed the new system to be as complex and cryptic as possible to maximize casual users' frustration levels, calling it Unix as a parody of Multics, as well as other more risque allusions. Then Dennis and Brian worked on a truly warped version of Pascal, called `A'. When we found others were actually trying to create real programs with A, we quickly added additional cryptic features and evolved into B, BCPL and finally C. We stopped when we got a clean compile on the following syntax:

```
for(;P("\n"),R-;P("|"))for(e=C;e-;P("_"+(*u++/8)%2))P("| "+(*u/4)%2);
```

To think that modern programmers would try to use a language that allowed such a statement was beyond our comprehension! We actually thought of selling this to the Soviets to set their computer science progress back 20 or more years. Imagine our surprise when AT&T and other US corporations actually began trying to use Unix and C! It has taken them 20 years to develop enough expertise to generate even marginally useful applications using this 1960's technological parody, but we are impressed with the tenacity (if not common sense) of the general Unix and C programmer. In any event, Brian, Dennis and I have been working exclusively in Pascal on the Apple Macintosh for the past few years and feel really guilty about the chaos, confusion and truly bad programming that have resulted from our silly prank so long ago."

Major Unix and C vendors and customers, including AT&T, Microsoft, Hewlett-Packard, GTE, NCR, and DEC have refused comment at this time. Borland International, a leading vendor of Pascal and C tools, including the popular Turbo Pascal, Turbo C and Turbo C++, stated they had suspected this for a number of years and would continue to enhance their Pascal products and halt further efforts to develop C. An IBM spokesman broke into uncontrolled laughter and had to postpone a hastily convened news conference concerning the fate of the RS-6000, merely stating `VM will be available Real Soon Now'. In a cryptic statement, Professor Wirth of the ETH institute and father of the Pascal, Modula 2 and Oberon structured languages, merely stated that P. T. Barnum was correct.

In a related late-breaking story, usually reliable sources are stating that a similar confession may be forthcoming from William Gates concerning the MS-DOS and Windows operating environments. And IBM spokesman have begun denying that the Virtual Machine (VM) product is an internal prank gone awry.
{COMPUTERWORLD 1 April}

{contributed by Bernard L. Hayes}

>>>
Please send subscription and backissue requests to CASEE::VNS

Permission to copy material from this VNS is granted (per DIGITAL PP&P)
provided that the message header for the issue and credit lines for the
VNS correspondent and original source are retained in the copy.

>>>>>>>>>>>>>>>> VNS Edition : 2336 Tuesday 4-Jun-1991 >>>>>>>>>>>>>>>>

Software Short (at) Circuit City: Senior Citizen spurned.

Peter Amstein <amstein@condor.Metaphor.COM>
Tue, 4 Jun 91 10:30:29 PDT

>From Herb Caen's column in the San Francisco Chronicle, June 4, 1991:
"Ron Lemmen took his old friend Nellie White to Circuit City [a local discount electronics chain - PA] to buy a TV set and after she wrote a check with more than adequate ID, the computer turned her down. It hadn't been programmed for somebody born before 1900 (Nellie's 92)..."

Old RISK of misconfigured printer

E/ACT Open Systems 04-Jun-1991 1446 <kaiser@heron.enet.dec.com>
Tue, 4 Jun 91 05:48:52 PDT

In 1968 I was a system programmer at the Columbia University Computer Center, which had a tremendous complex of IBM mainframes: a 360/91 tightly coupled to a 360/75, with a total of several megabytes of memory between them. Each computer had a disk farm, there was a 2321 Data Cell, a 2540 card reader, and a [number?] card reader/punch. And of course, several 1200lpm 1403-N1 printers.

Usually the computer room was a reassuring hum of noises ... off in the far corner, the very faint pulse of the PCU ("Plumbing Control Unit": the 91 was cooled by a closed-loop distilled water system!); the snicker-click of the 1315s and 2315s as the heads moved back and forth; the ka-CHUNK of the data cell as the selectors grabbed, turned, and released the magnetic cards in the cells; the susurration of the card readers and occasionally the clunk of the punch; and of course, the humming percussion of the printers.

One day I was in the room when suddenly it lapsed into near-total silence, except for the whiz of paper slewing out of one of the printers at high speed. The disks, card devices, data cell, and second printer had all stopped dead. And what was worse, very few of the 50 gazillion lights on the consoles of the computers were winking. Guessing immediately that something to do with the printer had brought the whole huge system to a halt, I ran over to it and hit (usually I don't like the word "hit" to mean "press", but this time I really did HIT) the STOP button. The printer stopped, but unfortunately nothing else came to life. Eerie dead silence, except for the water pump in the far corner. I set to work to find the problem.

We did figure it out: the listing on that printer had specified carriage control meaning "skip to the next punch in channel 12 of the carriage tape" -- but there was nothing punched in channel 12 of the carriage tape. And the system, it seems, had at that instant serviced all its interrupts except the one it was expecting from the printer -- which never came, because the only thing that could cause the interrupt (a punch in channel 12 of ...) never happened. So the entire multiprocessor system was at a dead stop waiting for the interrupt. What to do, what to do?

I removed the carriage tape and punched a hole in channel 12, then replaced it in the printer. I hit the START button, the paper slewed and stopped, the interrupt arrived, and the whole system came to life. Right?

Nope. Nothing happened. No sweat, I'm a system programmer, entitled to wander into the machine room and do anything I think I can get away with; so fine, I'll just warm-start the suckers and off we'll go. We're talking about $6,000,000 worth of computers, the finest IBM had built, servicing all the needs both academic and administrative (I mean, my PAYCHECK was calculated and printed on those machines!) of a prestigious university. One of whose trustees, by the way, was Thomas J. Watson, Jr. So I warm-started the system.

Unfortunately, that didn't work either. Nothing worked. Nor could IBM make it work. We had to reinitialize the whole system from scratch, the only time in my memory that that was necessary.

Now what to do about this terrible bug that could cause the whole machine to grind to an irreparable halt? A committee met several times to try to figure it out. (I wasn't invited. Too junior. Too technical.) The committee never came to a decision; they couldn't figure out whether to press IBM to solve the problem, or to try to find and fix it ourselves, or what.

I did my part. With no one's permission, I checked all the carriage tapes to make sure that they all had at least one punch in every channel, and I instructed the operators that whenever they made a new tape, they should make sure that every channel had a punch somewhere. End of problem.

---Pete

kaiser@heron.enet.dec.com +33 92.95.62.97

Boeing 767 crash

Steven Philipson <stevenp@kodak.pa.dec.com>
Mon, 3 Jun 91 23:41:16 -0700

I've received additional data on that is pertinent to the discussion of the 767 crash. Boeing tested the 767 during certification for thrust reverser activation in flight. Not only does in-flight deployment not cause damage, but the aircraft can remain in flight in this condition. This is because the thrust reversers are not as efficient as the non- reversed engines. There is still enough total thrust produced such that the aircraft can maintain flight with one engine at full throttle and the other at full throttle with the reverser deployed.

I realize that this information has no computer risk relevance, but speculation on the cause of this "computer controlled" aircraft has run high, even on the RISKs group. The above info answers some of the concerns that people had about operation of this aircraft. It also sheds some light on the fault tolerant nature of the Boeing hardware design, which should be instructive to those of us who design software.

Steve

Re: Lauda Air Crash

W.A.Simon <alain%elevia.UUCP@Larry.McRCIM.McGill.EDU>
Mon, 3 Jun 91 16:31:45 EDT

> New evidence that the crash of a Lauda Air Boeing 767-300 in Thailand had been
> caused by in-flight reversal of the thrust on one engine has stunned the
> aviation industry. Niki Lauda, owner of Lauda Air, made the claim in Vienna

This may have happened, but what about the ground witnesses who said the plane flared up like a fire cracker, and what about the small size of the pieces of the wreck, and what about the dispersion site surface? All of these are inconsistent with a simple loss of control resulting in an impact with the ground. There seems to have been some mid air explosion.

Alain (514) 934 6320 UUCP: alain@elevia.UUCP

Re: Lauda Air Crash

David Lesher <wb8foz@mthvax.cs.miami.edu>
Mon, 3 Jun 91 18:16:15 -0400

>Herr Lauda said the
>flight data recorder was damaged and could not be used to analyse the crash.

RISK of improvement, if true.

The old FDR's used metal scribes on stainless ribbon. They've been replaced by digital data recorders using magnetic tape. They offer more reliability, less error (in at least one famous case, the NTSB put the recorder in a centrifuge to explore the effects of high g-loads on the mechanical slop in the pen linkages!), larger number of channels - hence many more data points, maybe automatic reuse (as the voice recorder does) and likely lower cost.

But, according to friends in the airline industry, they also are far less indestructible. Makes sense - no matter what you do, ferric oxide on a plastic base melts at a lower temperature than stainless steel. And that does not even consider the Curie point of the oxide.

wb8foz@mthvax.cs.miami.edu

Re: AFTI/F-16 (John Rushby, RISKS-11.78)

A. Padgett Peterson <padgett%tccslr.dnet@uvs1.orl.mmc.com>
Mon, 3 Jun 91 16:34:16 -0400

Before launching into a discussion of John's posting, some background is necessary. Between 1979 and 1982, one of my assignments was on the AFTI-F16 program. My prime task was to augment the "user interface" between the designers and the FLCCs (FLight Control Computers), Bendix bdx 930, AMD 2901-based systems with a custom microcode, 4 Mhz cycle, and 450 nsec access UVPROM memory. Specs that seem pre-historic today but were what we had to work with.

During the flight test phase, as John points out, we had some "glitches", primarily from complex interactions that seem simple when explained but had us covering hallways with brush recorder outputs trying to figure out what happened. The telemetry and flight record capability available to us was typically (as I recall) limited to about 16 channels for each FLCC. Picking the correct software data points to monitor from in excess of 5000 locations was sometimes difficult.

Readers must remember that the AFTI-F16 was a technology demonstrator and for the era, we were "pushing the envelope" in a very steep learning curve not only for the digital flight controls, but for the entire process of designing digital flight controls. "What if" discussions abounded right down to the philosophical discussions of what the pilot was permitted to do. (At the time it seemed centered on the lowest common denominator thought that (IMHO) resulted in the Iranian debacle of 1980. There were political as well as practical problems to be solved.

I vividly remember one discussion concerning PLA (power level angle: throttle) authority. The P&W F100 engine had design limits (much like the red-line in a car) and the thinking at the time said to design the controls so that this point could not be exceeded. A few of us were of the opinion that this was a combat aircraft and that a fighter pilot should have the authority to exceed "design" limits if necessary to complete his mission. Warn him, but give him the option even at the risk of destroying his own aircraft. In combat, the rules MUST be different.

Today, it seems incredible that the opposing viewpoint existed, but it did and was quite pervasive in some governmental circles. Then, we were the mavericks.

>It seems that redundancy management became the primary source of unreliability
>in the AFTI-F16 DFCS.

Cost constraints & paper studies decreed that we would try a triplex design with hydromechanical back-up, in production, lessons learned on AFTI resulted in a Quadraplex system. Trying to develop a dual-fail-operational flight-critical system was not easy.

>...the unsynchronized individual computers may sample sensors
>at slightly different times, they can obtain readings that differ quite
>appreciably from one another...

Remember that I said "dual-fail operational". Synchronous operation would have eliminated such latency, but a "first-fail" could include loss of synchronization. Therefore asynchronous design was a level-1 decision.

Today, processing and sensor speed has increased to the point that this approach would not be a problem but at 500 kips, cycle rates were under 100/ second and when > MACH 1.3, a lot can happen in a couple of milliseconds.

> An even more serious shortcoming of asynchronous systems arises when the >control laws contain decision points. Here, sensor noise and sampling skew may >cause independent channels to take different paths at the decision points and >to produce widely divergent outputs. This occurred on Flight 44 of the >AFTI-F16 flight tests [4, p. 44]. Each channel declared the others failed; the >analog back-up was not selected because the simultaneous failure of two >channels had not been anticipated and the aircraft was flown home on a single >digital channel.

The pilot had a switch that allowed him to select which computer(s) was selected and could over-ride this digital decision if necessary. Note that the aircraft still had the hydromechanical back-up with "get home" capability if necessary. This condition HAD been anticipated.

> Another illustration is provided by a 3-second "departure" on Flight 36 of >the AFTI-F16 flight tests, during which sideslip exceeded 20deg, normal >acceleration exceeded first -4g, then +7g, angle of attack went to -10deg, then >+20deg, the aircraft rolled 360deg, the vertical tail exceeded design load, all >control surfaces were operating at rate limits, and failure indications were >received from the hydraulics and canard actuators.

I do not have the records here but suspect that this was one of the "find a long hallway" ones. This was probably the case where a combination of extremely high AOA in a near-stall condition caused the envelope to be exceeded on the back side i.e. the plane was no longer flying & the control surfaces had little effect. My memory may be going, but I seem to recall one set of readings that indicated near-zero air speed with an AOA > 80 degrees.

> The AFTI-F16 flight tests revealed numerous other problems of a similar >nature. Summarizing, Mackall [4, pp. 40-41] writes:

>"The criticality and number of anomalies discovered in flight and ground tests >owing to design oversights are more significant than those anomalies caused by >actual hardware failures or software errors..."

Easy words to say. Remember, this was a full-authority multiple-redundant flight control system containing five modes of flight with a computer that could only address 32k of memory (the upper bit of the 16 bit addressing was used to indicate an indirect operation).

>"...qualification of such a complex system as this, to some given level of >reliability, is difficult ...[because] the number of test conditions becomes so >large that conventional testing methods would require a decade for completion.

In other words, the only real way to test it and learn where the mistakes were

was to strap in a pilot and wish him luck. (of course thousands of hours in
a flight simulator connected to production hardware helped).

>The fault-tolerant design can also affect overall system reliability by being
>made too complex and by adding characteristics which are random in nature,
>creating an untestable design.

Huh ? Nothing in a digital system is random. period. Interactions may be
unanticipated, but not random. Things were a bit more difficult before PCs
though.

>2: However, the greater the benefit provided by DFCS, the less plausible it
>becomes to provide adequate back-up systems employing different technologies.
>For example, the DFCS of an experimental version of the F16 fighter (the
>"Advanced Fighter Technology Integration" or AFTI-F16) provides control in
>flight regimes beyond the capability of the simpler analog back-up system.
>Extending the capability of the back-up system to the full flight envelope of
>the DFCS would add considerably to its complexity--and it is the very
>simplicity of that analog system that is its chief source of credibility as a
>back-up system [2].

Doubletalk. Sure, an analog system is going to have trouble with a Mach 1.3
50 ft. terrain following mode (so are the pilot's kidneys). What we found
out was that you can make a plane do things with DFCS (digital flight control
system) that are impossible with an analog system. In TF, if you have a
failure, the back-up does not try to maintain that condition, instead a fly-up
is instigated and the aircraft returns to a maintainable mode.

> The danger of wide sensor selection thresholds is dramatically illustrated
>by a problem discovered in the X29A. ... It was subsequently discovered that
>if the nose probe failed to zero at low speed, it would still be within the
>threshold of correct readings...

At least we did not have this problem: on AFTI valid sensor ranges were
confined so that any sensor reading zero or full scale was automatically
declared failed.

All in all, I thought that AFTI was pretty successful & lead to the PDFCS
(Production Digital Flight Control System) program. We made mistakes
and learned from them. If anything, most thresholds were set too high so that
failures were declared that did not need to be, but we were kind of cautious
in those days. Probably the riskiest thing was to bet that technology would
allow us to replace that 450 ns memory with 250 ns units for a needed through
put improvement - three manufacturers had announced them but no-one had shipped
any when we froze the design.

In any event, first flight was almost exactly ten years ago, and the most
significant event was that the chase planes had to double their normal
clear-space distances since the AFTI-F16 could translate horizontally and
vertically without any warning, it was just suddenly someplace else.

Padgett

Search RISKS using swish-e

THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

ACM Committee on Computers and Public Policy, Peter G. Neumann, moderator

Volume 11: Issue 80

Tuesday 4 June 1991

Contents

Another Procrustes bed

Anastasios Vergis <plains!umn-cs!LOCAL!vergis@uunet.UU.NET>
Tue, 4 Jun 91 17:53:49 GMT

I had my first encounter with the Procrustes bed, when trying to give my forwarding address to Paragon Cable in Minneapolis, MN. No matter how much it was squeezed or stretched, their computer would accept it. You see, it was not a U.S. address. Being physically present there (I was returning the decoder box) I could observe exactly what was happening. The address was in Athens, Greece, zip code: 15235. When he pressed <return>, it would automatically erase "Athens, Greece" and put there "Pittsburgh, PA". Most certainly, the zip code

was "soft-wired" with the city & state info. It was disturbing that the program would not simply issue a warning. I offered to pay the outstanding balance (about two weeks service) on the spot, but they could not accept it as "a bill had to be mailed by the computer", and this would take 10 days or so. As I was moving in a week, most definitely the operator had a problem in his hands. It is interesting how the operator resolved the problem: he simply backdated the disconnection date, to coincide with the last day of the last bill, so there was no need any more for a forwarding address. Can't complain, as I got two weeks' free service ... Surely a good deal for Paragon Cable as well (think of the cost to upgrade the software). I can't help wondering how often they encounter this problem. The phone company, however, had no trouble accepting this overseas address.

-- Anastasios Vergis, University of Minnesota, CSci Dept.

Privacy and Network Monitoring

<[anonymous]>
Mon, 3 Jun 1991 12:07:33 xxx

By some odd coincidence, the recent privacy thread in Risks comes along right on the heels of an ugly incident at the company I work for. We have a very large internal network along with a system of newsgroups on a wide variety of topics. One of these is called "grumps" which is designed essentially for the venting of curmudgeonly humor. It is generally considered to be the electronic equivalent of the occasional water-cooler gripe session. Although humorous in intent, sometimes issues important to the running of the company surface there. I posted a satirical message last month, taking the company to task for some bit of silly official pomposity, and thought nothing more of it.

Imagine my surprise when two weeks later, my manager's boss called me into his office, with a copy of that message on his desk. He informed me that I should think carefully about sending out this sort of thing and that it reflected poorly on me and could jeopardize my professional advancement. Upon investigation, I discovered that our personnel department has very quietly taken on the job of surreptitiously monitoring traffic on certain internal "recreational" distribution lists. When something "offensive" is detected, it gets back, via the personnel system, to the offender's management.

I had a long talk with our VP of personnel who explained that they weren't "spying", they were just trying to keep "offensive" mail off the net. Of course, *they* decide what is offensive or not. There is a risk here, one which I don't recall having seen mentioned here before, and it is that personnel/management people operate under a very different set of values than the people in the technical community with whom I normally share such postings. For example, this VP pointed with pride to the fact that she doesn't have a computer in her office. The manager I talked to insisted that posting to a dl is a public act, whereas I view it as private in the same way as a conversation around the lunch table in a group of friends. These people have now set themselves up as social arbiters of a system which they themselves never use.

After thinking about this incident, I implemented an anonymous mail forwarding

system, which would allow people to express their opinions openly without fear of retribution on unspecified charges. Not surprisingly, word of this got around too. This system proved to be intolerable to Personnel. They could not stand the idea that anyone could say what they liked and couldn't be traced, despite the fact that the company itself operates a "Comment" system, which is designed to allow people to send anonymous comments to management. I was politely asked to stop my forwarding service. After thinking it over, I agreed, and I now regret that decision. The net result has been greatly decreased traffic on the grumps dl, and a major loss of faith on my part in the goodwill of the management of our company toward the people who work here.

Can printing public information be actionable?

Jerry Leichter <leichter@lrw.com>
Sun, 2 Jun 91 13:14:43 EDT

In classic "life imitates art" tradition, a case has been filed that resembles my "Mr. M" hypothetical (of the person who, for "numerological" reasons, publishes things like PIN's, private phone numbers, and so on).

The following is summarized from the Wall Street Journal (29 May 91, Page B6): American Airlines (AMR) has sued Travel Confidential newsletter and its publisher, Paul Edwards, to stop it from publishing lists of discount codes. The codes, which travelers are supposed to mention when making reservations, entitle them to discounts of 5% to 40% on airfare, car rentals, and hotel rooms. They are intended for people attending conventions.

AMR charges Travel Confidential and Edwards with fraud and racketeering for publicizing its codes, and asks for a court order banning such publication, $750,000 in punitive damages, and unspecified losses. "Travel Confidential is published with the sole purpose of facilitating, aiding and inducing the commission of fraud on American and other airlines, hotels, and car rental agencies," AMR claims.

Mr. Edwards says he is doing nothing illegal by pulling together information that is publicly announced by convention sponsors. "Every word comes from publicly available sources. There is not one iota of confidential or private information in this newsletter." He also denies that he is encouraging his readers to commit fraud. Edwards claims that airlines rarely even ask whether a traveler is attending the event that matches the code. "If they don't want people to abuse it, they should police it." (Where have we heard *that* before?) AMR says they are considering doing just that, and also claims that they could go after individual travelers for committing fraud by using the discount fairs.

-- Jerry

PS The same issue of the Journal, on page B8, discusses new voice-activated computer systems for bond trading. The risks that arise from traders perhaps being able to activate each other's computers are discussed (but of course dismissed by those who want the system as not a problem).

Re: the FBI and computer networks

Steven Philipson <stevenp@kodak.pa.dec.com>
Fri, 31 May 91 12:48:21 -0700

(D'Uva, RISKS-11.76)
>For example, a policeman does not need
>"probable cause" to stop your car when you are driving in an unsafe manner.
>The law has been broken, and that is enough to warrant the law enforcement

The policeman's observance of you driving in an unsafe or illegal manner constitutes probable cause. You cannot be stopped without probable cause (with the constitutionally questionable exception of sobriety checkpoints). Search after a stop for a traffic offense requires additional justification.

It may not be a good idea for people to post about illegal activities, but it does happen regularly. At least one newsgroup contains frequent postings in which persons report violating Federal regulations (usually inadvertently). Such postings are of questionable legal value as authentication is difficult (did Jones make the posting, or did someone who used his account make it?). Systematic monitoring issues aside, does a posting on the net constitute probable cause for real-world surveillance of the author? I don't have an answer for this. Is there case law that establishes precedent?

Arnie Urken writes [Re: Voting by phone]

> voting by phone enables a citizen to verify that his/her vote is
> actually counted, [...]

Does it? How is the voter to know that his vote is not routed to the bit bucket, or that a later disk crash doesn't obliterate it. California's antiquated Hollerith-card method produces a physical record of a vote. Which is more reliable? Which gives the voter a higher level of confidence?

Steve Philipson

Re: the FBI and computer networks (D'Uva, RISKS-11.76)

Rob Nagler <nagler@olsen.UUCP>
Tue, 4 Jun 91 11:40:42 +0200

The FBI are not just "law enforcement officials", they are public servants. The "public" are their employers. Suppose your house servant decides to look through your belongings, because they believe you might be doing something illegal. Do you have the right to tell them not to do it (even if you are doing something illegal)? My analogy is certainly trivial. The point is that many people seem to forget that the FBI, DoD, &c are working for us and not the other way around.

200 years have passed since "unreasonable search" was added to the US Constitution. The government of our "global village" must take into account the intent of the Founding Fathers, not just their words. In 1792 a "grep of

/usr/spool/news" was the house-to-house search of a city.

Rob nagler@olsen.ch

Government should have less access than everyone else

John Gilmore <gnu@toad.com>
Tue, 4 Jun 91 04:51:54 PDT

In RISKS 11.74, Andrew D'Uva asks, "Why should the U.S. Government have less access than a student at an American university (or a foreign one)?"

I've been rethinking privacy of electronic communications, particularly radio communications, since Congress is thinking about amending ECPA sometime this session. (No bills yet, but...)

My conclusion is that the government should be prohibited from intercepting *ALL* civilian radio communications, except in certain bands like AM and FM, while third parties should have full freedom to listen in on any band, as they did before 1986 and ECPA.

Jerry Berman of ACLU tells me that the real concern in ECPA was to prevent the government from spying on people. My proposal addresses that concern even more fully than his ECPA -- which only protects a minority of the transmissions. More importantly, a ban on the government monitoring communications is enforceable -- e.g. by the exclusionary rule, as well as by existing laws giving citizens the right to sue the government for collecting dossiers on their exercise of First Amendment rights like free speech. Speech over a cellphone is still speech and is still free.

A ban on interception by third parties is clearly not enforceable without direct confiscation of radio receivers. Then what's next? Typewriters and copiers, as in USSR? Shortwave radios that receive Radio Baghdad, when they only want you to hear their side of a war?

Before ECPA, if you transmitted information over the air and wanted to prevent its being overheard, it was *your* responsibility. You could encrypt it, use low power, hide it in noise, whatever. ECPA created classes of users who are absolved of this responsibility, such as cellular phone providers; the government picks up the tab for "enforcing" your privacy. Only trouble is that they are incapable of providing real privacy by passing laws, so the user ends up with no privacy at all. Had the onus rested on the transmitting party, it would be clear that it was up to cellular manufacturers to provide the privacy that people assume about "phones", or to stop marketing cellular walkie-talkies as "phones". But lobbyists were cheaper than privacy technology, so we started putting our personal lives on the air.

Think about it --

Re: vote by phone

Geoffrey H. Cooper <geof@aurora.com>
Fri, 31 May 91 13:26:55 PDT

In the vein of recent discussions about the "dumbing" of the work force, I note that the vote-by-phone proposal is good, but a little verbose and pedantic for my taste. I fear that the proposal is trying to out-stoopid the voters. (on the other hand, you have to be pretty good to listen to a list of ten choices and come up with the right number (ever try getting a pizza parlor to list how you can have it?). Maybe candidates will now try to be listed LAST on the ballot).

My belief is that vote-by-phone can be as complicated as filling out a regular ballot (as mentioned, in CA this can be a challenge). Also, it doesn't have to be an enjoyable experience (any more than is standing in line at the polling booth).

My twist on what was mentioned:

1. Voter requests vote-by-phone by mail.
2. Confirmation letter contains ballot with PIN on it.
3. Voter calls to vote and uses the PIN given.

The voter is warned that the PIN is the voter's right to vote: you lose it, you lost it; you show it to someone, you may have lost it. Suitable warnings are given about possible scam's to get PIN's. Reasonable mechanisms exist to deal with ballots that are lost or stolen a reasonable time before the election.

The ballot contains all the contests, numbered, and all the choices in each contest, numbered. Any choice is selectable by dialing a 3 (4?) digit number (2 digits => contest, 1 digit => choice).

The voter is advised to fill in the ballot to obtain the numbers of the people he/she is interested in voting for. Note that many voters do not vote in all the contests available (abstaining, or in some obscure local contests (or obtuse CA voter initiatives), a voter might not feel that he/she can make non-random decision).

The computer you call up is generally re-active, not pro-active. Thus:

- The user enters the code of the contest and his vote, selecting contest in his own order. This is faster, and makes it easy to not have a vote on something. It is also analogous to the way you vote by paper.

  As pointed out, the user can more effectively get the choices from the ballot than over the phone. If he doesn't have the ballot, what is he doing phoning the system?

- The entire ballot is constructed by making selections, but is not committed until the user specifically indicates that he is finished. Up until this time, the user may disconnect (accidentally or on purpose) and try again later.

Here is my vision of a phone call, which probably needs to be simplified:

<Welcome to phone-a-vote, over XX million served.
Please enter your PIN now>
beep-beep...
<Please vote>
beep-beep...
<Contest 23, District vice-scoundrel, you selected Bud Bundy>
beep-beep...
<Contest 56, Clean Sewers Initiative, you selected YES>
beep-beep...
<Contest 56, Clean Sewers Initiative, you selected twice. The selection has been erased. Please vote again.>
...
beep-beep...(0000)
<Your ballot has been accepted. Thank-you for voting.>
<click>

Maybe a special code runs through them all in order, so that you can check what you've done. Or maybe dialing 569 tells what was selected for contest 56.

[By the way, the supposedly anonymous messages might still be traceable based on the audit log that itemizes all e-mail to and from with a time stamp. So if your automatic reforwarder left the original time stamp, that was enough to nail the original sender!!! PGN]

Re: Voting-by-phone (Campbell, RISKS-11.78)

Paul Nulsen <pejn@cc.uow.edu.au>
Tue, 4 Jun 91 00:23:11 GMT

Larry Campbell asks: Electronic voting? Who needs it?

Although electing people to represent us in parliament is the generally accepted model for democracy at present, it is not full democracy. In a full democracy every voter should be able to vote on every issue, and this would be possible with electronic voting.

Such a system would clearly require checks and balances well beyond those needed for electronic voting alone. In practice parliaments and politicians would probably need to be retained to keep the political system operating day-to-day. There would also need to be stringent systems of review, to prevent hot-headed decisions and to prevent interest groups from hijacking the vote on particular issues.

This may not be Utopia, but anyone who complains about the voting of their representative should take heart that such a system may be achievable.

Paul Nulsen pejn@wampyr.cc.uow.edu.au

Lottery bar codes no risk, spokesman says (Minow, RISKS-11.78)

<king@ukulele.reasoning.com>
Mon, 03 Jun 91 16:12:35 BST

<> A. Lottery spokesman David Ellis tells us that, once an instant
<> ticket is "read" by a bar-code reader, it is invalidated...

That doesn't prevent people with access to unsold tickets from stealing winners and selling only losers.

Presumably losing tickets seldom if ever get read by the barcode reader even once, so an agent who sells one will not be trapped by the invalidation performed when he culls his supply of tickets. However, since indeed reading a losing ticket should be rare, I would hope that the security system will be suspicious of the operator of any barcode reader that gets too big a dose of losing tickets.

-dk

Bar-codes on lottery tickets

Alayne McGregor <alayne@geas.gandalf.ca>
Tue, 4 Jun 91 13:52:42 EDT

In RISKS-11.78, Martin Minow quoted a representative of the Massachusetts state lottery as saying that as soon as an instant ticket is read by a bar-code reader, it will be flagged so that it cannot not be cashed again. What was not clear was a) whether the physical ticket itself was flagged, b) the number of the ticket was stored in the card reader, or c) the number was stored in a central computer?

In case a), what is to prevent an unscrupulous person from xeroxing the ticket (perhaps onto the correct weight of card stock, if necessary) and bar-code-reading the xerox?

In case b), what is to prevent the person from going to another bar-code-reader for the next reading?

In case c), could not a bar-code-reader unconnected to the central computer read the stored information, which could then be decrypted? The system's security would then depend on the security of that encryption algorithm.

Alayne McGregor alayne@gandalf.ca

Lossy compression: Knowing versus guessing

Jerry Leichter <leichter@lrw.com>
Sat, 1 Jun 91 08:38:48 EDT

In Risks 11.77, David Reisner comments on the effects of using "lossy" compression techniques. His comments are quite interesting, but I think he,

and many others commenting on this issue early, miss an important point: What is new here is not the FACT of losses, but what we KNOW about them.

Reisner's example of the new Phillips Digital Compact Cassette (DCC) compression scheme provides an excellent example of this. It is quite true that such a system throws away information. On the other hand, *so does every recording scheme ever invented*. All recording schemes are bandwidth limited. All will saturate at high amplitudes. All analogue systems add noise. It's easy to contrast DCC with CD's and say "aha, they've thrown away some information" - but in fact CD's ALSO throw away information: The Nyquist limit means that they absolutely cannot record any information about about 22Khz, the 14-bit encoding places a limit on their amplitude resolution. In addition, CD's used for audio purposes use error correction schemes - what you hear may not be what was recorded, and will even vary from playback system to playback system. Of course, all these "losses" - sounds above 22Khz, the error correction "patches", and so on - have been chosen to be "unnoticeable" to the human ear. This is no different from the DCC scheme; the DCC scheme is just more clever about it. It's also no different from many older schemes, from FM (limited to 15Khz) to Dolby encoding.

A traditional photograph or X-ray isn't "exact" in any sense either. There is a finite grain size, a limited amplitude resolution (and a generally quite non-linear amplitude response), and so on. Grain size is chosen to be small enough to (mainly) be ignored by the human visual system. The details of response to different light levels and colors in film is chosen for its appropriateness in a particular use. Color snapshot film is built to "look pleasing", not to be "highly accurate" in any objective sense. X-ray film is built to produce high contrast of "medically interesting" things.

NTSC color television encoding uses less transmitted energy and bandwidth for chrominance than for luminance information because the human eye has much less sensitivity to loss of high spatial frequencies for chrominance. The color encoding used is inherently unable to represent some colors that the eye can perceive (certain dark browns). All of these choices were made based on studies of the human eye's abilities. In fact, JPEG is just uses more sophisticated versions of the same tricks - and interestingly JPEG is NOT necessarily lossy: JPEG is a class of parameterized compression algorithms, with the parameters chosen by whoever does the compression, and it is possible to set the parameters to avoid any (deliberate) losses.

What's the point of all this? Just that there is actually nothing new in losses in representation: They've been with us from the first time we sketched on cave walls. Early losses came about as inherent, uncontrolled side-effects of poorly understood processes. As we've become more technologically sophisticated, we've been able to understand the origins of these losses and ultimately either eliminate them (hiss, rumble, wow and such are non-issues for CD's) or deliberately choose where they will occur. Today's recording technologies, losses and all, are orders of magnitude better than what was available in the past.

However, from a political/legal/social point of view, there is one significant difference: What no one could understand or control, no one could be blamed or penalized for. If an important distinction is lost in a X-ray because the film's grain size can't represent it, well, that's the way it is. But when the

loss can be attributed to someone's particular, definite decision, all of a sudden blame can be attached: "If they hadn't chosen to save a few bucks on storage by compressing the image, my client would be healthy today." Once you can name the chemical added to the food, you can sue someone for adding it - and never mind all the thousands of chemicals already there that have never been analyzed.

Systems have to be built appropriately for their intended use. The more we understand and can control about a system, the more choices we can make - and the more choices we HAVE to make. When we were not in a position to make the choice, "nature" made it for us - but it WAS made.

-- Jerry

More on Lossy Compression => Rendering errors

Geoffrey H. Cooper <geof@aurora.com>
Mon, 3 Jun 91 13:06:27 PDT

>From: synthesis!dar@UCSD.EDU (David Reisner)
>There are, in fact, lots of compression algorithms that ARE lossy. ...

This is a part of a much more pervasive problem: rendering errors. For example, a digitally encoded image is ALWAYS an approximation of the continuous input. There are mathematical constraints for getting the right results out of a digital display system without encountering aliasing effects, but these require filtering -- and this filtering is generally assumed to be done by the viewer's eyes.

I'll talk about rendering of images, but the same applies to any area of digital signal processing.

The challenge of image processing is to play around as much as you can without exceeding a JND (just noticeable difference). Sometimes we go a bit further (e.g., 300 dpi laser printers, most computer displays) and accept what I'll call a JID (just ignorable difference), and some people end up pulling their hair out because they can't ignore what we want them to.

Many RISKs enter, in that the JND is a physiological concept, not a physical concept. Hence:

- JND is an averaged measurement, some people notice more (like people who can hear TV sets -- ouch!).

- Sometimes the JND is not a constant parameter, so a subtle change in the application can wreak havoc. For example, visual flicker sensitivity depends on frequency, brightness, and the part of the retina that is receiving the signal. When Cinemascope was tried out some years ago (a very wide curved screen), it was found necessary to decrease the intensity of the bulbs used in projectors or viewers would complain of flicker in the corners of the screen when they looked at its center.

- Multiple JND's typically apply to a situation; you have to take them all into account. For example, the set of pictures of Mars from the Viking I lander included an impressive sunrise with rings around the sun. The New York Times printed this picture in a two page spread. Actually, the lines were spurious contours (optical illusion), deriving from a linear quantization of gray levels in the digital camera. How many million people thought that there really WERE lines around the sun on Mars?

  (Moral: rendering errors can ADD to, as well as subtract from, detail in a picture)

- Sometimes the result is not processed by the unaided human eye. For example, if a doctor uses a magnifying glass (or a microscope!) to better see some fine detail on a rendered picture (especially with lossy compression, but even a photo will do), he may violate the limitations of resolution imposed by the imaging process. In this case, who knows what he might or might not see?

The solutions that I come up with:

- Over-engineer rendering so that the user is unlikely to exceed the limitations unknowingly imposed on him. This is what we do in photography. Obviously, this is what computer compression schemes are specifically trying to avoid...

- Educate the users to understand what they have. For example, a medical imaging system might have a warning notice on the screen that an enlargement of the image is not guaranteed to be accurate, or (better) may provide "safe" enlargement primitives that are guaranteed not to exceed the limitations of the compression scheme.

Any other ideas?

geof@aurora.com / aurora!geof@decwrl.dec.com / geof%aurora.com@decwrl.dec.com

---

Re: More on Lossy Compression

Phil Ngai <phil@brahms.amd.com>
Tue, 4 Jun 1991 17:53:38 GMT

I consider image compression schemes which take advantage of the eye's limited color resolution to be about as dangerous as audio systems which cut off at 20 KHz. As long as the data is to be used by humans, there are physiological limitations that are universal and exploitable. Of course, there are people who still think vinyl records are better than CDs.

Report problems with the web pages to the maintainer

Search RISKS using swish-e

THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

ACM Committee on Computers and Public Policy, Peter G. Neumann, moderator

Volume 11: Issue 81

Monday 4 June 1991

Contents

Re: RISKS-11.81!

"Peter G. Neumann" <neumann@csl.sri.com>
Tue, 4 Jun 91 19:19:19 PDT

Sorry, folks, I was pushing just a little too hard today, having gotten out three issues of RISKS, one before starting work this morning, one during lunch break, and one just before now, along with getting my normal workload attended to.

Unfortunately, RISKS-11.82 should have been RISKS-11.81. The file name was RISKS-11.81, but the issue said it was RISKS-11.82. So, RISKS-11.82 it has become. The easiest way out now is for me to declare that THIS APOLOGY is really RISKS-11.81, and then get on with RISKS-11.83 (but not today!). Thanks for your patience today. I hope I do not get too many desubscriptions for having flooded your mailboxes. (I suppose I could blame the hot weather, but it is still very pleasant here.)

Let me take this gratuitously serendipitous opportunity to thank all of you who have been applying the masthead standards fairly diligently of late. The rate of acceptable contributions has recently been much higher. But then it always tends to vacillate cyclically, depending upon the "subject:" matter. PGN

Search RISKS using swish-e

Search RISKS using swish-e

THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

ACM Committee on Computers and Public Policy, Peter G. Neumann, moderator

Volume 11: Issue 82

Tuesday 4 June 1991

Contents

---

risks of open anonymous ftp

Pete Cottrell <pete@cs.UMD.EDU>
Tue, 4 Jun 91 17:50:01 -0400

I have discovered some risks of having an open anonymous FTP environment on your machine. By 'open', I mean that there are one or more writable directories available for people using anonymous FTP into which files can be uploaded. This arrangement is popular on several of our professors' workstations, as it allows them to exchange files and papers with colleagues at other sites. It is particularly nice for dvi or binary files, which can't be sent directly via e-mail. Occasionally, we have seen a file called MAKE_MONEY_EASY or something similar advertising some get-rich-quick pyramid scheme that someone uploads. This hasn't been a problem in the past, but it has

become one when escalated by an order of magnitude or two.

Some background first: the USENET newsgroup alt.sex.pictures is used to distribute what are usually called X- or R-rated pictures. These pictures are uuencoded files, usually in the GIF format, sometimes in others. Because of the size of the pictures, a individual pictures is broken down into parts, usually 3 or 4, but sometimes up to 20. A fully assembled and decoded picture is sometimes as small as 25 or 30K, but is typically 150-250K and may be even larger. Monthly posted reports of USENET traffic flow show that this newsgroup is consistently among the leaders in terms of quantity of megabytes of traffic.

Many sites refuse to carry or forward this newsgroup. For some, it is simply a question of traffic; they don't want to double or triple their phone and modems costs to transmit the group. For others, it is a matter of the material itself. More than one group has been forced to shut down the group under orders from superiors, often under political pressure.

To make up for the lack of availability of the newsgroup, and also for the limited bandwidth it provides even if available, seekers of the GIF files look for ftp sites. A good site can have many pictures available, and the ftper can grab many megabytes of files at once. Several of these have been found in the past, but what typically happens is that someone will announce the location of such a site, at which point the poor machine is swamped with anonymous ftp sessions and traffic, forcing the administrators of the machine to turn off anonymous ftp. As a consequence, the source of ftp sites is few.

So, another tack must be taken and it is this: find a site that has a writable anonymous ftp directory, create gif directories, and ftp away. Requests and questions are communicated by creating files whose name is the request/question itself, like this:

```
-rw-r--r-- 1 ftp 1 May 23 18:57 more-asian-gifs-PLEASE

   or

1 -rw-rw-rw- 1 ftp 1 May 23 14:21 00-Otherwise-this-site-wo
uld-be-shut-down-soon
   1 -rw-rw-rw- 1 ftp 1 May 23 14:21 00+Please-do-you-file-tra
nsfer-at-non-prime-time.---7pm-6am.eastern-time
```

Announcement of new sites is handled in a similar fashion:

```
-rw-r--r-- 1 ftp 1 May 22 00:16 I-saw-somebody-suggesting-t
o-switch-to-xxxxx.yyy.zzz
```

People upload and download to their hearts conten

Magellan spacecraft performance; followup

Randall Davis <davis@ai.mit.edu>
Tue, 4 Jun 91 19:33:00 edt

The Magellan craft doing radar mapping Venus had several failures early in the mission, including one 32-hour outage, as noted in some previous Risks postings.

This update on subsequent performance is extracted from a 2 page article in

appeared in Aviation Week of 20 May:

The Magellan spacecraft successfully completed the first cycle of Venus mapping on May 15, producing more data than required despite occasional spacecraft glitches...

A second cycle of mapping was started May 16 to cover most of the surface that was not mapped on the first cycle, with emphasis on south polar regions that have not been seen before.

Ambitious plans for future use of the spacecraft are being formulated, including using aerobraking to circularize the orbit...

Magellan's basic mission was to radar map at least 70% of Venus' surface and 83.7% had been covered as of May 15. The Martin Marietta spacecraft has done a ``great job'' and the Magellan radar, built by Huges has been ``flawless, beautiful,'' said A. J. Spear, Magellan project manager at JPL.

Lauda Air Boeing 767 Aircraft crash

Hermann Kopetz <hk@vmars.tuwien.ac.at>
Tue, 4 Jun 91 10:37:28 +0200

Nearly all major newspapers in Austria had the main headline on Monday along the following topic:

Computer failure causes Boeing 767 airplane crash

Niki Lauda, the owner of Lauda Air (and former grand prix champion) gave the following explanation in a televised press conference in Vienna on Sunday at 1:00 p.m. (I watched it.):

Both the voice recorder and the data recorder have been recovered after last Sunday's crash of the 767 near Bangkok. The data recorder was unreadable because it did not withstand the crash. After an analysis of the voice recorder the following sequence of events has been established:

Sunday, May 26, 23:05 Bangkok time: The plane, coming from Hongkong took off from Bangkok airport. Everything was normal, the plane has climbed to 7000 m and was still climbing further.

23:16 An advisory warning light (lowest of three criticality degrees) started to blink intermittently. The copilot referred to the checklist which read (about): Another failure can cause the deployment of the thrust reversal. Expect normal operation of thrust reversal after landing. No immediate action to be taken.

23:18 The voice of copilot Turner: "It deployed" (i.e. the thrust reversal was activated while the plane was still climbing with high engine power). A few moments later one can hear an acoustic warning signal on the tape indicating that the forces on the plane are critical. Two seconds later the voice recorder stops, because the plane crashed.

I have been asked by newspapers to comment on the suspected computer failure but do not have any further information. Do you have access to any further information about the B 767, in particular:

* Do they use single or multiversion software?

* How is it possible that a dangerous state, which has been indicated, does not require any action? (Consider this happened in the first fifteen minutes of a 10 hour flight!)

Looking forward to some more information

Hermann --Tel 43 1 588018180--FAX 43 1 569149 -- ++++++ PLEASE NOTE THE CHANGE IN THE E-MAIL ADDRESS ++++++

[An anonymous commenter sent in this: "Speculation is now increasing that the thrust reversal deployment, while the system was under computer control, was part of the problem. I just spoke to my Airline Pilot Association friend who does all the interviews after such events, and he tells me that there is a mechanical system that is supposed to prevent the reversers from deploying until the plane is on the ground, but he says that they do break down and such a failure would allow a computer malfunction to deploy the reversers. He also says that contrary to what Boeing is saying, it can be VERY hard to avoid having a plane tear apart if the reversers deploy while the plane is in a high power situation (e.g. climbing--as was this plane). Note that the 767-300 is NOT a "fly by wire" plane in the sense the new Airbuses are, but that the engines are normally under computer control with no direct mechanical connection with the pilots." There is some redundancy in the following messages, and in the preceding ones, but I think that the subject is potentially too complex for me to try to do an accurate and careful differential reading and analysis, in the absence of more definitude. PGN]

Reply to rmoonen concerning "the wings ripping off"

richard shapiro <shapiro@Think.COM>
Mon, 3 Jun 91 12:19:42 EDT

No, thrust reversal in mid-flight wouldn't rip off the wing. It would have some potentially unpleasant control consequences, by introducing a very large yaw moment, but reverse thrust is far less efficient than forward thrust. Also, I understand that as part of the flight certification of an airplane, it must be able to fly with one engine at full reverse thrust. I don't know what might happen if the thrust reverser activated at low altitude, where there isn't a lot of time to recover, but the plane should hold together until it hits the ground.

Re: Lauda air plane crash (Moonen, RISKS-11.78)

Joe Morris <jcmorris@mwunix.mitre.org>
Mon, 03 Jun 91 12:57:23 EDT

Extracted from this morning's _Washington_Post_ (3 June 91) p. A11:

> "What happened in the plane is that the thrust reverser, for whatever reason, was deployed in the air," Lauda told a news conference upon returning to Vienna from Washington, where U.S. authorities are examining equipment retrieved from the wreck. His conclusions were echoed in a statement by Austrian Transport Minister Rudolf Streicher, who said a computer error may have activated the thrust reverser.
> [...]
> However, a spokesman for the Seattle-based Boeing Co. said a 767 should be able to continue flying even if the situation described by Lauda occurred. The Federal Aviation Administration will not certify any jet aircraft to fly unless it passes an in-flight test in which a thrust reverser is deployed at full power.
> [...]
> Some U.S. sources close to the investigation expressed irritation at the flow of statements from both Thailand and Austria as the investigation of the crash continues. In any crash, they noted, an agency can determine a final cause only after months of painstaking investigation.
>
> The sources, who asked not to be identified, did not rule out the possibility that the thrust reverser may have malfunctioned. However, Boeing spokeswoman Elizabeth Reese said that owners of the more than 350 767's now flying had never reported any thrust reverser problems.
> [...]
> To receive FAA certification, each type of aircraft produced [in] the United States must have a thrust reverser deployed at full power in flight. The pilot must be able to control the plane using normal procedures.

Joe Morris

Re: RISKS DIGEST 11.78

Steven Philipson <stevenp@kodak.pa.dec.com>
Mon, 3 Jun 91 12:40:05 -0700

Re: In-flight engine reversal as reported in _The Times_ (London), Monday June 3rd 1991.

> [...] If the diagnosis were confirmed, the accident would
> be unprecedented, Herr Lauda said.

A crash of a 767 is unprecedented. In-flight thrust reversal leading to an accident is not -- there is a long history of accidents from both intentional and unintentional in-flight reversing, for both jet and propeller driven aircraft.

>rmoonen@hvlpa.att.com (Ralph 'Hairy' Moonen) writes;

>And certainly, wouldn't a mid-air reversal of thrust just rip
>off the wing, leaving the plane to plummet down totally out of control?

No, it would not. The engine would depart the aircraft well before that level of stress could be reached. Application of significant amounts of reverse thrust would cause a severe controllability problem in and of itself though. If one engine were providing full foward thrust and the other significant reverse thrust, the result would be a very large yawing moment. The crew would likely notice this very quickly. It is possible that the reversers deployed as part of a engine failure that was already in progress. More data will be required before this can be ascertained.

Steve Philipson

Re: Lauda Air Crash (RISKS-11.78)

Jeremy Grodberg <lia!jgro@fernwood.mpk.ca.us>
Tue, 4 Jun 91 20:10:44 GMT

According to the Wall Street Journal, 6/3/91, In order to receive federal (US) certification, the Boeing had to *demonstrate* that the 767 could fly with one thrust reverser deployed (emphasis added). I take this to mean that they had to actually fly the plane this way.

The same report also said that Boeing engineers knew of one other time the thrust reverser deployed in mid-air, but that plane landed without incident, and the situation may not have been entirely analogous.

Jeremy Grodberg jgro@lia.com

RISKS of posting humor to the net

Phil R. Karn <karn@thumper.bellcore.com>
Tue, 4 Jun 91 19:31:15 EDT

Uh, the line

```
for(;P("\n"),R-;P("|"))for(e=C;e-;P("_"+(*u++/8)%2))P("| "+(*u/4)%2);
```

does *not* compile cleanly on my system (Sparc). The problem is with the operators "R-" and "e-". Change them to "R--" and "e--" and it will compile successfully, but drop core when it runs. Then initialize u, C and R to something reasonable (like "the address of an array of 100 ints initialized to 0', "10" and "10", respectively), and define P() to be printf(), and you'll get output that looks something like this:

```
| _| _| _| _| _| _| _| _| _| _|
| _| _| _| _| _| _| _| _| _| _|
| _| _| _| _| _| _| _| _| _| _|
| _| _| _| _| _| _| _| _| _| _|
| _| _| _| _| _| _| _| _| _| _|
```

```
| _| _| _| _| _| _| _| _| _| _|
| _| _| _| _| _| _| _| _| _| _|
| _| _| _| _| _| _| _| _| _| _|
| _| _| _| _| _| _| _| _| _| _|
| _| _| _| _| _| _| _| _| _| _|
```

Make the initial values of the array random, and you get something that looks like a maze:

```
 _ _ _ | _| _| _|   |
  _| | | | _ _ _ _ |
| _| _| _|    _| | |
| | _ _ _ _ | _| _| _| |
   _| | | | _ _ _|
 _ | _| _| _|    _|
| | | | _ _ _ _ | _| _|
| _|    _| | | | _|
 _ _ _ | _| _| _|   |
  _| | | | _ _ _ _ |
```

Cute, yes. Useful? You tell me...

Phil

Digital Fingerprints in California

Mike Caplinger <mc%miranda.uucp@moc.jpl.nasa.gov>
Thu, 30 May 91 09:48:16 PDT

I recently applied for a California driver's license, and was surprised to learn that the fingerprinting required for a license (right thumbprint) was now done by a digital scanner instead of with paper and ink pad. The RISK is obvious -- sometime down the road, when pattern matching of fingerprints has been more or less totally automated, the State of California will have a database ready to go without the hassle of scanning paper fingerprints in. It's my understanding that current matching technology is too labor- and computer-intensive to perform regularly on anything larger than a database of known felons, but with advances in computer power, matching against the whole population may be possible. Anybody know more about the California database, or how viable thumbprint matching may be? Would one expect many false matches using just a thumbprint? How many other states require fingerprints for driver's licenses, and does any other use digital scanners?

I suppose it's possible that the California DMV doesn't retain the digital data -- but I doubt it. I'm less certain but fairly sure that the "mugshot" is also taken with a video system. I could imagine it would be awfully tempting for law enforcement agencies to combine those two databases.

Mike Caplinger, MSSS/Caltech Mars Observer Camera mc@moc.jpl.nasa.gov

CPSR Review of FBI Net Surveillance

<cdp!dsobel@labrea.Stanford.EDU>
Tue, 4 Jun 91 18:25:15 PDT

I 'd like to add a bit of relevant information to the discussion. Computer Professionals for Social Responsibility (CPSR) is currently litigating a FOIA lawsuit against the FBI seeking information on the Bureau's policies and practices with regard to computer bulletin boards. A couple of months ago, we received a heavily censored copy of a 1985 internal FBI legal opinion entitled "Acquisition of Information from Electronic Bulletin Boards."

Although couched in terms of a prohibition, the opinion does *not* establish an across-the-board prohibition on monitoring and/or surveillance of computer bulletin boards. All that the opinion prohibits is a "comprehensive" monitoring program. Bulletin boards may be monitored, so long as Fourth Amendment standards are satisfied, i.e., where there is a "reasonable expectation of privacy," a warrant must be obtained. The opinion might not be using precise language when it refers to "bulletin boards," since most are public and do not generally involve an expectation of privacy. As I read the opinion, it permits warrantless monitoring of public bulletin boards on a case-by-case basis.

CPSR believes that such monitoring, even of public bulletin boards, is inappropriate. There is an undeniable "chill" placed on the free exchange of opinions when participants need to worry if the discussion is being monitored by government agents. The history of the FBI demonstrates that individuals expressing views deemed to be unpopular or "subversive" became the subjects of official scrutiny and extensive record-keeping. While some might argue that bulletin board discussions are completely open and that participants should expect them to be monitored, such a concession seriously erodes First Amendment values. How would we feel if we knew that every political meeting or community gathering we attended was monitored and recorded by government agents? Isn't that the sort of governmental conduct we so strongly condemned when it was practiced by the old communist regimes in Eastern Europe?

While it is unclear whether we will be able to learn anything about the implementation of the FBI's policy through our lawsuit, the legal opinion described above certainly raises questions that should be pursued. I would be glad to keep interested folks posted on developments, though I'd prefer to do so through private e-mail, i.e., "with an expectation of privacy." Send me a note if you'd like to be kept informed about the litigation.

David Sobel, CPSR Legal Counsel cdp!dsobel@labrea.stanford.edu

> ["... with an expectation of privacy" is subtle, in that apart from "privacy enhanced e-mail", e-mail goes over unencrypted local and global networks, is handled by some decidely unsecure systems, and is typically forwarded iteratively to other people. "... with some hope of privacy" might be more accurate! But I imagine David will get some requests from a few government RISKS contributors, who might like to know what "developments" are turning up... PGN]

Computers and Academic Freedom Groups Now at EFF.ORG

Jim Horning <horning@Pa.dec.com>
Tue, 4 Jun 91 12:22:59 PDT

CAF discusses such questions as : How should general principles of academic freedom (such as freedom of expression, freedom to read, due process, and privacy) be applied to university computers and networks? How are these principles actually being applied? How can the principles of academic freedom as applied to computers and networks be defended?

The EFF has given the discussion a home on the eff.org machine. As of April 23, less than two week after its creation, the list has 230 members in four countries.

There are three versions of the mailing list:

comp-academic-freedom-talk
- you'll received dozens of e-mail notes every day.

comp-academic-freedom-batch
- about once a day, you'll receive a compilation of the day's notes.

comp-academic-freedom-news
- about once a week you'll receive a compilation of the best notes of the week. (I play the editor for this one).

To join a version of the list, send mail to listserv@eff.org. Include the line "add <name-of-version>". (Other commands are "delete <name-of-version>" and "help").

In any case, after you join the list you can send e-mail to the LIST BY addressing it to caf-talk@eff.org.

These mailing lists are also available as the USENET alt groups 'alt.comp.acad-freedom.talk' and 'alt.comp.acad-freedom.news'.

Search RISKS using swish-e

THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

ACM Committee on Computers and Public Policy, Peter G. Neumann, moderator

Volume 11: Issue 83

Wednesday 5 June 1991

Contents

Electronic Gear Boxes at the Canadian Grand Prix

Lindsay "F." Marshall <Lindsay.Marshall@newcastle.ac.uk>
Wed, 5 Jun 91 12:30:30 BST

Mansell mystery deepens (The Guardian, 4 June 1991)

Mystery surrounds the precise cause of Nigel Mansell's dramatic retirement from the Canadian Grand Prix on Sunday. But the fact that yet again it centred on the electro-hydraulically actuated gearbox has led to murmurings in the

Williams camp that a manual-gearchange version of the current car should be rushed through for the second half of the season.

Problems associated with the Williams FW14's gearbox have been responsible for Mansell's retirement in four of this season's five F1 races. Williams immediate priority is to sort out the problem before the next grand prix in Mexico City on June 16 by pinpointing why Mansell's car lost all drive on Sunday with the chequered flag in sight.

The mystery deepened after the race when the car eventually returned to the Montreal padock: it fired up immediately and the gearchange worked perfectly. It all seemed to support the widely held view that today's breed of grand prix car is becoming over-reliant on complex electronics for the efficient operation of its engine.

This viewpoint is strongly supported by the Honda president Nobuhiko Kawamoto, the man largely responsible for the Japanese company's pre-eminent position in F1. "We are in danger of introducing a breed of computerised dinosaur", he said in Montreal. We are facing a situation where the electronics may become more comlpicated than the engines. This aspect of F1 threatens to become ever more expensive".

In the race, Gerhard Berger's McLaren-Honda retired after only four laps with just such a malfunction of its engine-management computer. Meanwhile, McLaren have a similar gearbox to William's under development, but the team chief Ron Dennis will not compromise his cars' competitiveness until he is satisfied the system is bulletproof.

Computer-controlled fuel system problems in 747-400

"Peter G. Neumann" <neumann@csl.sri.com>
Wed, 5 Jun 91 11:57:36 PDT

Richard Fairley picked up the Mainichi Daily News as he was boarding a 747-400 to return from Narita to San Francisco on Saturday, 1 June, and found on the front page an article on a 747-400 fuel problem experienced at the end of March on a NY-to-Narita JAL flight. I do not recall seeing a report of this before in the U.S. press. I abstract from the article somewhat tersely, as follows:

> The 747-400 (popularly known as the high-tech jumbo) has five fuel tanks, with 13+38+52+38+13 tons of fuel distributed with lateral symmetry, the 52 being in the fuselage. The computers are programmed to automatically draw from the 52, then the two 38s until they approach 13 tons, at which point all four wing tanks are used simultaneously to maintain proper weight distribution across the wingspan. On this particular flight, the outer wing tanks were depleted prematurely, while the fuselage tank was not depleted. The result was that the wings were too light, arching the wings upward. The operating ratio limits were exceeded. The fuselage tank is supposedly pressurized at twice the wing tanks so that the outer tank valves can remain open.

Fairley commented: "I found it particularly interesting that the article

reports there was no trace of the abnormality. If the problem had been more severe, it is unlikely that the cause of a crash could ever have been detected." (The article notes that the incident was detected only because JAL had been placing flight engineers as observers [this is a two-man cockpit-crew aircraft] on its flights in an attempt to find design problems in the new plane!)

PGN muses: Perhaps this could have begun with a loss of pressurization in the fuselage tank, with the computer system doing exactly what it was programmed to do, but with a false assumption about the actual pressure...

KAL 007

"Peter G. Neumann" <neumann@csl.sri.com>
Wed, 5 Jun 91 9:33:51 PDT

More is emerging on the KAL 007 shoot-down, 8 years later, resolving some of the mysteries but leaving other ones. Recent articles in Izvestia revealed "that the Soviet Union lied after the shoot-down when it said it had attempted to contact the errant airliner, that it did find the remains of the aircraft (including the black box), and that it apparently uncovered no evidence that the plane was on a spy mission." But they also interviewed the pilot Lt.Col. Gennadi Osipovich, who said, "I had no idea that it was a passenger aircraft..." Osipovich also stated that prior to the shoot-down the U.S. had increasingly been violating Soviet airspace, including various reconnaissance flights, presumably to calibrate the Soviet responsiveness. One overflight of 15 minutes caused a reprimand for Osipovich himself, and had "put the Soviet air command on edge."

An article in The Nation, 3 June 91, pp. 724-5 raised old several RISKS- and technology-related questions that still seem unanswered:

* Why had the U.S. tracking system failed to follow the plane and alert it?
  (or had it and is simply not admitting it?)
* What had U.S. intelligence learned of the Soviet's responses?
* Why were the U.S. radar tapes erased?

The article concludes with this: "But the lack of concrete evidence supporting the spyflight scenario does not exonerate the Reagan Administration's propaganda campaign. Both sides acted deplorably...." (E.g., "... the President ignored U.S.-collected intelligence that demonstrated the Russians didn't know what they were chasing.")

Thrust Reversal in the real world

<[anonymous]>
Wed, 5 Jun 91 11:10:12 xxx

While it is true that the 767-300 was certified for operation with accidental thrust reversal, a very senior airline pilot who knows these planes has told me (when I asked him about this very topic in light of the recent crash) that in

the "real world" of flying it can be a different matter.

The problem is that during periods of maximum thrust (such as climbing, as was the airliner in question) the sudden deployment of the reversers could result in a violent "pinwheeling" of the plane. He points out that this can be extremely difficult to correct, and can rapidly result in an overspeed condition (and in fact, the overspeed warning can apparently be heard on the cockpit voice recorder from the crash). Such conditions can result in rapid disintegration of the plane as engines and wings are damaged, which could of course result in fires as well!

He also mentioned that there is a mechanical system that is supposed to prevent the thrust reversers from deploying unless the aircraft is on the ground--but he said that these do break down from time to time, which could result in a situation where computer control, alone, could theoretically deploy the reversers in flight.

Whether or not thrust reversal was indeed related to the particular crash is an open question at this time, but remember that just because an aircraft has been "certified" for a certain set of conditions, doesn't necessarily mean it will do you much good under a particular set of complex real world circumstances, and possibly multiple failure modes.

VIPER lawsuit withdrawn

Martyn Thomas <mct@praxis.co.uk>
Wed, 5 Jun 91 12:05:50 BST

Charter Technologies apparently went into voluntary liquidation on June 4th. Before doing so, it withdrew its lawsuit against the UK Ministry of Defence, probably because it could not afford to pursue it.

There has been a lot of criticism of MoD and others for claiming that Viper is a proven microprocessor when the development process has not been submitted to "proof by theorem-prover" from specification to netlist. I believe that this is mistaken criticism, and reveals some fundamental misunderstandings about the nature, and value, of proof.

No degree of mathematical analysis of a development process can give absolute certainty of correctness, and nor can any other technique. Isn't it essential that anyone in a senior role, developing or purchasing systems or components for critical applications, understands this?

VIPER is a very high integrity microprocessor. No fault has ever been discovered in its behaviour, so far as I am aware. This needs to be emphasised, in case the lawsuit has given the impression that there is something wrong with VIPER. I do not believe that anyone has even *suggested* that VIPER does not perform according to specification.

The VIPER development and verification methods have been described in detail, including the fact that four of the theorems were too difficult for the HOL theorem prover, and that the lower levels were verified by exhaustive

simulation using a simulator which had not itself been formally analysed. [The company which develops and markets this tool, ELLA, used to belong to Praxis]. There has been no attempt to present this development route as anything other than what it is: a very high integrity development, stopping short of full axiomatic proof.

We must beware of having the term "proof" restricted to one, extremely formal, approach to verification. If proof can only mean axiomatic verification with theorem provers, most of mathematics is unproven and unprovable. The "social" processes of proof are good enough for engineers in other disciplines, good enough for mathematicians, and good enough for me. Occasionally, the use of theorem provers will be cost-effective for the extra level of assurance they probably provide, but we harm our industry if we do not recognise that there are very effective, and very formal, verification strategies using higher-level logics and formal arguments, and that these are legitimately described as "proofs".

My main concerns are firstly, that the reputation of VIPER and of the development technologies should not suffer from any misleading impression of the basis of the lawsuit. Secondly, that we should not slip into a belief that there are verification techniques which can deliver certainty that a system or component cannot fail. If we reserve the word "proof" for the activities of the followers of Hilbert, we waste a useful word, and we are in danger of overselling the results of their activities!

Martyn Thomas, Praxis plc, 20 Manvers Street, Bath BA1 1PX UK.
Tel: +44-225-444700. Email: mct@praxis.co.uk

Listening? (John Gilmore, RISKS-11.80)

<Eric_Florack._WBST311@xerox.com>
Wed, 5 Jun 1991 08:33:15 PDT

=-=-=-=
>My conclusion is that the government should be prohibited from intercepting *ALL* civilian radio communications, except in certain bands like AM and FM, while third parties should have full freedom to listen in on any band, as they did before 1986 and ECPA.
=-=-=-=

Many two-way services are content specific. There are specific channels for just about every type of business on the business bands, for example. How would you suggest that these be enforced without routine monitoring?

Free speech is not the issue in situations like what I suggest. FOr example, the business bands, let's say a taxicab channel, for example, is not the place to be discussing political thinking. The issue as I say, is not free speech, but rather, the effective and efficient use of the bandwidth.... a matter for the FCC to determine, certainly. How to be effective in enforcing traffic laws, without routine monitoring?

My point here is not just this one exception, of course. My point is that your

demand for bans on ALL routine monitoring by governmental agencies is far too broad a call.

Let's please make sure that in your (IMHO, overblown) concern about government monitoring we don't cripple the government's ability to enforce laws which allow the day to day operations of telecommunications equipment to be smooth.

Combatting the Network Monitors

Richard Johnson <richard@oresoft.com>
Wed, 5 Jun 91 11:53:53 PDT

In RISKS-11.79, an anonymous poster tells of the chilling effects of people in his company discovering they were being electronically "eavesdropped" by personnel. Here are a few ideas this individual might wish to employ to restore some of the sense of community they lost. I mention them publicly because they touch on a lot of privacy conflicts we've been discussing. Sorry about the length.

1. If they are not pre-screened by these same personnel department meddlers, drop a note in one or more of the suggestion boxes you mentioned. Might not work, since most companies actually ignore unsigned suggestions and they're already sensitized to you.

2. I suspect top-level management is not aware of the chilling effect that *this* policy is having on company morale. While a well-meaning policy, its effect has been to insulate the real decision-makers (at the corporate or site level) from the actual feedback they need to decide well. In their wisdom, they saw fit to provide several avenues for formal and informal criticism to climb the chain of command. Someone in the middle of the chain has blocked this criticism. The end result can only be less efficiency and poorer decisions from the top.

   Somehow you might make the TOP_LEVEL people aware. This might mean the awful end-run around management (probably a bad move), posting a note like the above paragraph to the same monitored distribution list, a memo to your boss with a CC to the _boss_, or an anonymous, computer-printed, memo physically displayed in obvious places.

3. (If you're desperate)
   Continue posting as before, only encrypted. This kind of mitigates the personnel-weenee's argument that the information is "public" on a closed distribution list.

4. Continue posting as before, only quietly circulate key code phrases that are complementary on the surface and might have alternate meanings.

5. Continue posting, making sure that the watchdogs get thoroughly confused, overworked, *blamed* for all kinds of things.

6. Set up your own e-mail distribution list and exclude the offenders.

Obviously, you don't want to get extreme until it's clear the company is going to tell you to take a hike anyway. Also, there are some people (very closed-minded, elitist ones IMO) who honestly believe that since you do this on company equipment and on company time, your views and information are also "the company's". This view is not universal, and is probably being legally debated right now, but that doesn't stop the meddlers from believing in the "rightness" of their position. I believe it was Confucius (or maybe Lao Tzu?) who said basically "You must first forget what you know before you can learn."

7. (If you are _truly_ desperate)
Tell the world exactly who is doing the dirty deed. Name names, dates, and times. Specify the company and be sure to cowtow properly to the top-level people's mal-implemented plans.

Of course you might find out they really DO want to censure their employees. Which leads inexorably to ...

8. Look elsewhere for work, or grab the best talent there and start your own company.

Richard Johnson richard@oresoft.com richard@agora.rain.com

Re: Digital Fingerprints in California (Caplinger, RISKS-11.82)

Michael Robinson <robinson@cogsci.Berkeley.EDU>
Tue, 4 Jun 91 20:49:16 -0700

>I suppose it's possible that the California DMV doesn't retain the digital data
>-- but I doubt it. I'm less certain but fairly sure that the "mugshot" is also
>taken with a video system.

It is.

>I could imagine it would be awfully tempting for
>law enforcement agencies to combine those two databases.

It is, and they will.

But, as with most risks, there are countervailing risks. The California driver's license (and its relative, the California identification card) is intended to be positive legal identification.

California Vehicle Code, Sec. 14610:
It is unlawful for any person:
(a) To display or cause or permit to be displayed or have in his possession any cancelled, revoked, suspended, fictitious, fraudulently altered, or fraudulently obtained driver's license.
(c) To display or represent any driver's license not issued to him as being his license.

> (g) To photograph, photostat, duplicate, or in anyway reproduce any driver's license or facsimile thereof in such a manner that it could be mistaken for a valid license, or to display or have in his possession any such photograph, photostat, duplicate, reproduction, or facsimile unless authorized by the provisions of this code.

This language is repeated in the section covering identification cards.

You don't have to have a legal ID, but if you do have one, it has to identify you. At least in theory. Obtaining fictitious identification has always been trivial, and it is almost always used for illegal purposes.

A while ago, I read in RISKS of a woman who obtained fraudulent identification and spent large amounts of another woman's credit. The risk of fraudulent identification is, IMHO, far greater than the risk of positive identification.

The DMV has a statutory obligation to enforce "one man, one card" to the best of its ability by whatever means are technologically feasible. In this case, the technology may skirt the margins of a potential tool of repression, but doesn't get me nervous yet. I don't see how the thumbprint/photo database would allow law enforcement to threaten my rights or privacy in any novel manner.

What does get me sort of nervous is the magnetic stripe on the back. The only advantage I can see to that is the ability to process a lot of people really quickly...

Michael Robinson USENET: ucbvax!cogsci!robinson

RFD: comp.online moderated

Robert Jacobson <cyberoid@milton.u.washington.edu>
Tue, 4 Jun 91 19:48:32 PDT

I would like to propose the creation of a new newsgroup, COMP.ONLINE. The purpose of this newsgroup would be to discuss the phenomena of being "online" -- what it means to be part of an electronic community.

To my knowledge, there are no newsgroups dealing broadly with this issue. Individual newsgroups may deal with the conversations happening locally, as in the various muds newsgroups; or the topic may come up spontaneously and then die, as it has in comp.society on occasion. Yet the experience of being online is central to what all of us do here: it deserves some special attention.

I suggest putting this new newsgroup in the comp. hierarchy because being online is irrevocably tied up with the use of computers and information technology. It could also go in rec. (since we often recreate online) or soc. (because we are a social happening) or alt. (where nearly every- thing else ends up). But comp. feels right to me.

I propose further that this newsgroup be moderated. I offer to do the moderation, at least initially. I have been a host on USENET (sci.

virtual-worlds) for nearly a year; before that, I hosted two conferences on The WELL and ran a legislative BBS for the California State Assembly. My credentials are in order.

Please let the online crowd know what YOU think about this proposal. Also, please crosspost this announcement to such other newsgroups as you think are appropriate. After approximately one month of discussion, I will call for a vote on creating comp.online .

Thanks for your attention and your ideas.

Bob Jacobson, Moderator, sci.virtual-worlds

Associate Director, Human Interface Technology Laboratory, Washington Technology Center, c/o University of Washington, Seattle 206-543-5075 (Employment given for purposes of identification only; the HIT Lab hosts only sci.virtual-worlds and has no connection to this proposal.)

Correction Re: Writer steals stories via computer

Rodney Hoffman <Hoffman.El_Segundo@Xerox.com>
Wed, 5 Jun 1991 11:06:57 PDT

A footnote to an item in RISKS 11.74. The 'Los Angeles Times' ran the following correction on June 4:

"FOR THE RECORD"

"A Times article on May 29 incorrectly stated that free-lance writer Stuart Goldman pleaded no contest to stealing fictional story ideas planted by police in Fox Television computers. Goldman, in fact, pleaded no contest only to unauthorized access to a computer system."

Amendation Re: Computers and Academic Freedom Groups Now at EFF.ORG

Peter G. Neumann <Neumann@csl.sri.com>
Wed, 5 Jun 1991 13:01:03 PDT

Actually, the first person named in the writeup reproduced in RISKS-11.82 regarding the academic-freedom mailing list was Carl Kadie (kadie@eff.org), which was left out due to an editing foulup even before it was routed to Jim Horning... Sorry for the lack of attribution. PGN

Search RISKS using swish-e

THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

ACM Committee on Computers and Public Policy, Peter G. Neumann, moderator

Volume 11: Issue 84

Thursday 6 June 1991

Contents

"MAN CATCHES COMPUTER VIRUS!" -- A new computer risk?

Mike Corbett <mcc@moscom.com>
Thu, 6 Jun 91 14:09:31 EDT

[WWN's Computer Story Generator Strikes Again!]

MAN CATCHES COMPUTER VIRUS!
Bizarre illness jamming up his brain waves!

Caption: SICK COMPUTER passed on a bizarre virus to programmer John Stevens, above, after it became ill from an infected software program.

By Michael Todd, Special Correspondent, {Weekly World News}, 18 June 1991

John Stevens has a lot in common with his home computer: Both think logically, both like numbers and both are sick with a virus - the same virus! Stevens, a computer programmer who works out of his home in a Philadelphia suburb, is convinced his lingering and debilitating illness is something he got from his sick computer. And the victim's doctor agrees. "I've run every test I can think of to trace the origin of his illness," said Dr. Mark Fordland. "He has a virus, but it's not like any virus I've ever seen."

Stevens, 32, said his computer began to show signs of a virus - a software program designed to eat up an destroy other software data - about a week before he got sick. "I was careless about borrowing software programs from other people I didn't know well," Stevens admits.

Dr. Fordland, himself a computer expert, agrees. "Borrowing software programs from friends and strangers is like having sex with someone you don't know well. When you sleep with someone, you sleep with everyone they've ever slept with. When you borrow someone's software program, you're connected to everyone who's ever used that program." Dr. Fordland concludes that Stevens' symptoms are identical to that of a software virus' attack on a computer. "Stevens has become forgetful, like something is eating up his memory, his data. He has less and less energy. He can't hold onto thoughts. Even an EEG (electroencephalogram) of his brain waves keeps changing. It's becoming more and more erratic. "This virus could just eat him up until his mind is a blank and he's like a vegetable," the doctor said.

[Wow! Sure brings home the point that we should all practice "safe computing". Mike]

Re: WWN Strikes Again!?

Peter G. Neumann <neumann@csl.sri.com>
Thu, 06 Jun 91 19:00:00 PDT

As a veganophile, I take offense to WWN's insulting the vegetable kingdom. But, stay tuned for the sequel, when WWN discovers vegetable matter is not so dumb as it looks, and can actually be used in building computers:

- Venus flytraps as input devices?
- High-Q-cumbers (without leekage) and toroidal turnips (/root/a/bagels?) as storage devices?
- Phototropic switches, albeit somewhat slow in changing state? (Sun tried tomatoes, but they wouldn't work!)
- Poly-Okramatic display screens?
- Tree-structured directories using live bee trees?
- Artificially intelligent roboDENDRALs? (apologies to HERB Simon)
- Century plants for long-term archiving?

Let the buyer beware? No, let the celery beware!

By the way, when Ada Lovelace fixed the computer system,
she became a Babbage-Patch Doll.
Don't forget the net reprimand, TOO-MANY-HOPS [SPOIL THE BREATH?],
and please pardon my (corny?) ingrained rye humor.
It's gone but not ergotten. (There must be a fungus amongus.) PGN

VIPER and formal specification of hardware

<Anonymous>
Thu, 06 Jun 91 12:17:33 xxx

A story I'd heard about the VIPER chip from someone who had been associated with it was that after the designers at RSRE had taken the high level design and gone on to produce an ELLA description of it, they had to send that out to the fabricators. A couple of companies where chosen to fabricate it, on gate arrays I believe. Apparently the engineers at one of the companies had a go at hand-optimising the layout, thus endangering all the previous work!

A previous attempt at producing a formally specified CPU at Cambridge University could have run into some problems when it was realised -- during fabrication -- that they'd forgotten to spec out fully the startup state of the computer. Fortunately the process used ensured that the chip would start up in a usable state.

In my own experience at formally specifying hardware I've found that its good for the abstract behaviour of computers, such as how the ALU should behave. You can take a high level spec and synthesise the same behaviour from the specifications of 74-series TTL and PALS. What you can't do is design out the failure cases. For a software routine you can give preconditions for all arguments and then check them at the start of each invocation, calling error handlers when the conditions fail. It's hard to do the same thing for hardware when the preconditions include things like the supply voltage being within 1/2V of +5V, or the timing constraints of signal setup and hold times. When these things are violated the system does tend to behave extremely badly.

Conclusion: Formal Specification and Verification of Hardware are unlikely to ever be able to guarantee the reliable operation of computers, except within clearly defined constraints.

This is no reason not to try, however. I mean, imagine if a big company like, say, Intel, produced a microprocessor, called something like an i486, with a bug in its maths. Imagine the trouble that would cause? Perhaps if the formal techniques will someday be able to handle complex chips such problems will disappear, or at least be reduced.

Patriot missile failure followup (More on RISKS-11.70)

Martin Minow 06-Jun-1991 0908 <minow@ranger.enet.dec.com>
Thu, 6 Jun 91 06:19:22 PDT

This is heavily edited from an AP article in the Boston Globe, 6-June-1991:

> The computer in the Patriot battery whose radar had picked up the
> incoming Scud failed to track the missile... Thus no computer instructions
> were given to the Patriot missiles and none were launched, the Army said.
> The Patriot computer screen did not show an incoming Scud because the
> computer software could not calculate the missile's path quickly enough.
> This was attributed to two factors the Patriot systems had not previously
> encountered in Saudi Arabia: The computer had operated continuously for four
> days prior to the moment of attack, and a faster than usual Scud missile speed.
>
> The lengthy period of nonstop operation had reduced the computer's capacity to
> make calculations. ....
>
> Improved computer software to correct the Patriot problem arrived in Saudi
> Arabia ... one day before the attack, but priority for installing the new
> tapes was given to Patriot batteries deployed closer to Iraq. ...
>
> Army officials at Huntsville, Ala., site of the Patriot project office, had
> disclosed privately last month that a computer software glitch was to blame
> for the failure... It had not previously been made known that the Army knew
> of the Patriot computer problem before the fatal attack.

Huh? Bit rot? Or, perhaps, a main memory failure that caused the program to swap/page/thrash and consequently not be able to keep relevant data in main memory. Hmm, maybe it was keeping a continuous event log in memory. Or, maybe the Patriot software was written in Lisp and it chose the wrong time to garbage-collect.

Martin Minow minow@ranger.enet.dec.com

Lauda 767 crash

"Peter G. Neumann" <neumann@csl.sri.com>
Thu, 6 Jun 91 8:29:42 PDT

I am told that Boeing has a generic specification for the engines, which all engine manufacturers have to follow. The thrust reversers are activated as follows:

Activation occurs with a 28-volt output from a four-input AND gate. This AND is not ttl, it is diode logic at 28 volts, and very simple.

One of the inputs comes from the FADEC. It is a combination of "engines at idle" and "weight on wheels" (the latter is combined in the FADEC for convenience).

One input comes directly from the setting of the throttle lever. It is a microswitch on the reverse position on the throttle quadrant.

One input comes from the spoilers. It is a microswitch detecting that the spoilers are fully deployed.

One input comes from the flaps. It is a microswitch detecting that the flaps

are at 25 degrees or more.

This is seen to conform to best practice. The computer system is not critical, and the rest of the system design is very simple. There seems to be a common point in the AND gate, but the reliability of such a simple system should be easy to establish. If 28 volts somehow got beyond the AND, then presumably the reverser would deploy, but such speculation seems idle at present. It doesn't feel like a FADEC failure. BUT, if the reported cockpit failure signal somehow reports the activation of the three non-FADEC signals, then the FADEC becomes critical; but how then to explain what would seem to be a triple failure followed by a FADEC failure? The mystery remains.

Lauda Air flight data

Brian Hayes - Sigma Xi <hayes@concert.net>
Wed, 5 Jun 91 19:58:05 -0400

Several RISKS readers have mentioned that the flight-data recorder transcript from the crashed Lauda Air 767 seems to be unreadable. But some of the flight data may be available from another source. Quoth Aviation Week (June 3, p. 92):

The aircraft's Loral-Fairchild flight data recorder and Sunstrand cockpit voice recorder have been recovered and appear to be in good condition.

Authorities already have vital recordings of the Lauda transport's performance parameters up to the moment of the crash. Boeing 767s are equipped with the advanced Arinc Communications Addressing and Reporting System (ACARS). It automatically updates, batches and relays aircraft and engine performance and maintenance information to ground stations every few seconds via private VHF or HF radio networks. This information is forwarded to Lauda maintenance offices in Vienna.

[Also reported by John Knight, jck@neptune.cs.Virginia.EDU]

Re: Thrust reversers

Jim Sims <sims@starbase.mitre.org>
6 Jun 91 22:50:08 GMT

Not *all* use of thrust reversers inflight is unintentional or catastrophic. NASA was (and prob still is) using a Gulfstream G-II (when I worked there) as a Shuttle landing simulator.

To simulate the shuttle's glidepath, you take a G-II up to altitude, deploy full flaps, drop the landing gear ('dirty' the plane), and then apply full thrust reversers. Yes, it drops just like a rock/shuttle...

DECUS AI SIG Symposium Representative The MITRE Corporation
7525 Colshire Drive MS W418 McLean, Va. 22015

Re: Lauda Air Crash -- an old C-47 incident

Wm Randolph Franklin <wrf@mab.ecse.rpi.edu>
5 Jun 91 21:59:53 GMT

Some decades ago, a C-47 (I think) hit Wright Peak in northern New York State, a popular hiking spot. There are a few big pieces, and thousands of pieces less than an inch square scattered over, say, a half-mile area. Much of that plane shattered like glass. A larger plane with large, full, fuel tanks would be scattered farther.

As for the observed flare, if the observers are accurate, which is always doubtful in disasters, maybe the reversed thrust tore the engine loose, or a piece of the engine hit the fuselage.

Wm. Randolph Franklin
Wrfrankl@Rpitsmts.bitnet (518) 276-6077
ECSE Dept., 6026 JEC, Rensselaer Polytechnic Inst, Troy NY, 12180

Thinking like a manager (Challenger)

Ed Nilges <EGNILGES@pucc.princeton.edu>
Thu, 06 Jun 91 17:09:58 EDT

From Michael Davis' article "Thinking Like an Engineer: the Place of a Code of Ethics in the Practice of a Profession", Philosophy and Public Affairs, Spring 1991, Vol. 20 #2:

> "Lund's first response was to repeat his objections. But then Mason said something that made him think again. Mason asked him to THINK LIKE A MANAGER INSTEAD OF AN ENGINEER (the exact words seemed to have been "take off your engineering hat and put on your management hat.") Lund did and changed his mind. The next morning the shuttle exploded, killing all aboard. An O-ring had failed."

Compression losses, microphoto artifacts

Leslie DeGroff <DEGROFF@INTELLICORP.COM>
Wed, 5 Jun 91 13:49:06 PDT

An aside related issue to compression losses in photographic data is that of photographic or processing "artifacts". A recent issue of Science had an article on problems of carbon chains being misinterpreted in a number of cases in electron and various scanning microscopy, this was primarily about physical "artifacts" but when your dealing with highly (computer) processed signals looking for edges, low contrast/low threshold regions you have issues (and risks) with putting things in that don't really exist or the misinterpretation of physical artifacts from the preparation and handling of specimens. As a big deal with all kinds of microscopy this has implications for attempts to automate or semiautomate medical work such as pap smears. Recent articles in CA, have made a big issue about risks with the quality of such services...

Like several other posters, I think that the real problem is going to be

"litigate if there is a chance of winning" law system and "devil we know vs the one we don't, conservative" medical system rather than technical issues... The real limit in most cases is the human in the loop interpreting!!!! My guess is that within ten years technically the scanners, computers and softwares will be available to have annual whole body scans with resolutions in the cubic millimeter scale and have the ability to early screen for most cancers, most hidden circulatory problems when most of them are minor surgery rather than life or death medical heroics. The capabilities of the medical system to use it, and our resource allocations to deploy them probably with triple that to 30 years before general use. Les DeGroff

---

Erasing Calif license mag strip (Re: Nishioka, RISKS-11.63 [and .09)

Mark Seecof <marks@capnet.latimes.com>
Thu, 6 Jun 91 15:25:38 -0700

I still have an "old" California driver's license (it'll expire in late '92).
I fear that when I get a "new" one, the magnetic strip on the back may accidentally be erased by some chance encounter with a strong magnetic field. After all, I've had credit-card strips fail.

(Side notes: when credit-card strips fail the card-issuers don't rewrite the mag strip, they just give you a whole new card. Actually, failed strips are a problem for merchants as well as credit-card users because merchants get a discount on the fee they pay to the bank if they "swipe" a card rather than just taking an imprint).

Because it is unlawful to "alter any driver's license in any manner not authorized..." (CVC 14610(h)) a police officer would have probable cause to arrest the holder of a license with a bad mag strip if he became aware of that circumstance (after, say, discovering that a portable reader can't read the strip). Note that a police officer doesn't need probable cause to inspect your driver's license if you appear to be in control of an automobile (CVC 12951). (Refusing to produce the license is an offense.) Now, unless the prosecutor could prove that the erasure was deliberate, the license-holder probably wouldn't be convicted but would already have spent the night in jail, or if cited and released would at least have had to come to court. Worse, a license holder might be violating the law and not know it, because the strip isn't human-readable.

Any system that might code information on the mag strip that didn't appear in human-readable form on the license card is inherently evil. Data on mag strips is fragile. I don't see how I'll be able to guard against the accidental erasure of the mag strip on any license issued to me. Given my innocent predilection for toying with permanent magnets and the fact that I work with various sorts of electrical and electronic equipment, who can say when an accidental erasure might occur? Why, it could even happen within minutes of my receipt of the new license!

I hope that the Legislature will see the RISKS here and change the law to exclude the data on driver's license mag strips from protection by the anti-tampering rules.

Mark Seecof <marks@latimes.com>

My opinions are not those of my employer. (My employer's opinions appear on the third-from-last page of the Metro Section weekdays or of the Opinion Section on Sunday.)

[Reminder: Alan Nishioka discusses the format in RISKS-11.63.]

Re: Digital Fingerprints in California (Caplinger, RISKS-11.82)

Gary Greene <garyg@zip.convergent.com>
Wed, 5 Jun 91 13:40:19 PDT

>I recently applied for a California driver's license, and was surprised to
>learn that the fingerprinting required for a license (right thumbprint) was now
>done by a digital scanner instead of with paper and ink pad.

Seems to me I've heard the above stated about a thumb print being required on California licenses in Risks before, however I just renewed my license in person (I'm an inveterate procrastinator about some things and had to go in to get a renewal by my deadline), a new photo was shot, but no thumb print taken ...nor have I ever submitted a thumb print to them in the past. I received my nice new card with the magnetic stripe and holograph several weeks ago.

>... Anybody know more about the California database, or how viable thumbprint matching may be? Would one expect many false matches using just a thumbprint? How many other states require fingerprints for driver's licenses, and does any other use digital scanners?

I'm not a specialist whose comments would bear relevancy on the above issue, but my impression is that a thumb print is useful mostly for general i.d. purposes, since it is only one digit. It is true that so long as there are enough match points that any finger can be used by a police agency to establish identity, however most latent prints from a crime scene are partials and it is rare that a full set of usable prints can be lifted. Not being a police officer I can't comment on the frequency that a thumb print is available. Current commercial scanners of reasonable price can now scan at about 1200 dpi (scanners under $7-8k). This ought to be good enough resolution to avoid mismatching i.d.

My photo was still taken with the old optical camera by my local DMV office. Of course, this doesn't prevent them from scanning the photo in later, but from the appearance of mine this doesn't seem to have occurred.

While on the one hand I hate government intrusion and dislike the idea of a national or even state police data base, having been the victim of grand theft once I can appreciate the availability of some way that police can identify criminals in the event of crime. The officer who dusted my premises (at my request) wasn't hopeful that the prints would be useful. Unless the person who commits the crime has a prior booking record there is no way to match the prints, even if the computer base and time to match the prints is available (neither were in my case ...the prints went into the case file and the officer

said that the only person who might ever look at them would be an officer trying to match up a pattern of similar crimes with a suspect; in short someone with a hobby-case).

In order for a California DMV thumb print to be used by a police agency it appears that a number of prior things need to happen. First, *all* crime records and other police records need to be consolidated into one data base, on-line at a central location. That's a lot of paper! We are only now reaching the point where this is practical technologically (i.e., companies like mine, Unisys, are marketing such paperless systems to banks now). The second thing necessary is that a budget be found to scan in this massive records data base from the existing paper files. This is also no mean task, and would require more than a few manhours to accomplish. The equipment budget to set up the system would be expensive also, though that part of the task would be manageable during normal economic times. Since the state and local governments here in California are currently bankrupt for all practical purpose I doubt that we will see any move in this direction in the forseeable future.

Consolidating all this with the DMV system would seem to multiply the practicalities of the task beyond reasonable economic-political considerations. You think the Prop 13 revolt was bad? This would put the Jarvis-Gann people in bed with the ACLU and several others. I can here several politicians saying !!wow!! with glistening palms while the bureaucrats shudder. :->

Gary Greene, Unisys/Convergent Technology, San Jose, California

---

Re: Digital Fingerprints in California

Alan Dahl <morpho!alan@uunet.UU.NET>
Wed, 5 Jun 91 15:12:37 PDT

Sorry to burst your balloon, but current matching technology is perfectly able to search a database of the size indicated (20,000,000 1-finger records). We are in the process of converting our system to a newer 2-times faster machine that should make this sort of search even easier. With a MORPHO AFIS (Automated Fingerprint Identification System) the search would not be too labor-intensive either. Our system is not very labor intensive at all. It is true, however, that some other companies' AFIS systems are too labor intensive for this sort of work.

We currently have an installation in New York with over 4.5-million 10-finger records and regularly run hundreds of latent and tenprint searches a day against this record database. Average tenprint to tenprint matching time is under 2 minutes/search. With a 20-million record database and the same hardware matching time would increase to about 3 minutes or so per search. Adding more hardware could shorten this down to 30 seconds if the customer desired. The current accuracy rate is 98% matched in the first position with most of the other 2 percent in the second position. Whether that print is a thumbprint or not will not affect the accuracy of the search at all.

We have talked to the State of California DMV about installing an AFIS system for commercial driver's licenses only. As far as I know everything is on

hold and there are no plans at this time to purchase such a system either from us, or our competitors.

A combination AFIS/mugshot system will probably be a reality in the near future, many jurisdictions desire such a system.

There are serious legal ramifications to using driver's license fingerprint data for anything else besides checking for duplicate licenses and aliases. Most states have laws that state that someone must be suspected of a crime before their prints can be searched against a criminal database. It is likewise illegal to search a suspected criminal's prints against a database of people who have not been suspected of a crime (such as databases of applicants for gun permits or police job applicants or driver's licenses). If the State of California passed a law legalizing such action and the Supreme Court let it stand (not too likely, I hope), it would technically be easy to implement such a system.

What is more worrisome is that the driver's license data could perhaps be used for checking the legality of applicants for welfare, food stamps, and other non-criminal uses.

Alan Dahl, North American MORPHO Systems, 1145 Broadway Plaza, Tacoma, WA. 98402 PH: 1 (206) 593-8021 ...uw-beaver!amc-gw!morpho!alan
(please DO NOT use uunet!amc-gw!...)

Re: Digital Fingerprints in California (Robinson, RISKS-11.83)

Mike Morris <morris@grian.cps.altadena.ca.us>
Thu, 6 Jun 1991 16:30:37 GMT

>A while ago, I read in RISKS of a woman who obtained fraudulent identification
>and spent large amounts of another woman's credit. The risk of fraudulent
>identification is, IMHO, far greater than the risk of positive identification.

There was a case widely reported of a rather-well-off lady who obtained something like 15 fraudulent IDs and got on the welfare rolls with most of them. When she was caught, it caused a _big_ stink.

>... I don't see how the thumbprint/photo database would allow law enforcement
to threaten my rights or privacy in any novel manner.

You don't read much futuristic SF do you... Lets say that a video tape was made of a mugging - a Rodney King-type video tape, only different. Now image enhance it and run it against the data base and come up with probable IDs.

>What does get me sort of nervous is the magnetic stripe on the back. The only
>advantage I can see to that is the ability to process a lot of people really
>quickly...

There was a writeup in ca.driving a while back on the format and what's in it (no, sorry, I dodn't save it). It's essentially 3 tracks of the same info that is on the face of the license. The cops will be getting hand-held ticket

printers with "swipe" card readers for accuracy. The current method of hand copying the data leads to inaccuracies. Also the ticket printers will be uploaded regularly with outstanding warrant info.

Mike Morris WA6ILQ PO Box 1130 Arcadia, CA. 91077 818-447-7052 evenings

Search RISKS using swish-e

THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

ACM Committee on Computers and Public Policy, Peter G. Neumann, moderator

Volume 11: Issue 85

Saturday 8 June 1991

Contents

DoD News Release on missed Scud intercept at Dhahran

Lt Scott A. Norton, USN <norton@manta.nosc.mil>
7 Jun 91 16:25:47 GMT

Here is the DoD News Release that provides some information on the failure of Patriot batteries to intercept the Scud missile that hit the Dhahran barracks.
-Scott Norton <norton@NOSC.MIL> [Quoted text follows]

Assistant Secretary Of Defense, Public Affairs, Pentagon, Washington DC
A/V 225-3886 (912)695-3886

- - - - - - -

DEPARTMENT OF DEFENSE NEWS
WEDNESDAY, JUNE 5, 1991

* * * * * * * *

Department of Defense News Editor: Mr. Frank Falatko

- - - - - - - - - - - - - - -

MEMORANDUM FOR CORRESPONDENTS, WEDNESDAY JUNE 5, 1991

REPORT ISSUED ON SCUD MISSILE ATTACK

The Department of the Army announced today the results of its review of the investigations pertaining to the Scud missile attack against Dhahran, Saudi Arabia, on February 25, 1991:

That evening a Scud missile impacted into a warehouse used by U.S. Forces as a barracks in Dhahran, Saudi Arabia, killing 28 and -wounding 98 U. S. Army soldiers.

Two investigations were initiated shortly after the attack.
One focused on Patriot operations and the other on actions taken at the barracks that was attacked.

The investigation of Patriot operations concluded that an inexact computer software calculation is the most likely explanation as to why the battery did not effectively detect or track the incoming Scud. A similar problem of this nature was first documented on February 20 after analysis of an earlier Scud engagement. The four days of continuous operation by the battery, caused by increased day and night Scud activity, are thought to have compounded this software problem. Updated software fixing this problem and containing other improvements arrived at the battery's location on February 26.

The investigation of the barracks concluded that Scud attack procedures were properly followed. More specifically, upon warning of a potential Scud attack, soldiers had instructions to go inside or get under cover in either concrete bunkers or bomb shelters, if available, and to put on helmets and chemical protective gear. It was impossible to determine precisely how much warning time the soldiers ha but it appears that they were alerted approximately 30 seconds prior to the Scud's impact. Both U. S. and Saudi emergency medical response was timely.

The investigation of Patriot operations was conducted in theater by officers from the 11th Air Defense Artillery Brigade. An independent technical

review from the Patriot Project Office at Redstone Arsenal concurred with the findings of the investigation.

Six Patriot batteries were located in the Al Jubayl-Dhahran- Bahrain area. Two were positioned to engage this Scud missile. One of these batteries was out of action for repair of a radar receiver. The remaining battery was operational and prepared to engage an incoming Scud missile.

The operational battery was positioned to fire in the automatic mode against Scuds threatening an area surrounding the Dhahran air base. Scuds threatening outside of this protected area but within the Patriot's engagement capability could also have been engaged manually. The barracks was located in this manual engagement zone. Because the Scud was not effectively detected or tracked by the radar, engagement in the manual mode was precluded.

The investigation reconstructed the circumstances of the Scud attack and evaluated the possibility of Patriot hardware, software, or operator error.

Based on diagnostic checks conducted before and after the attack, hardware failure was ruled out. Operator error was also eliminated as a cause based on a review of Patriot crew procedures.

The Army deeply regrets the loss of life and extends its sympathy to the families of those who died or were injured.

Thrust reversers (Sims, RISKS-11.84)

Mary Shafer <shafer@skipper.dfrf.nasa.gov>
Thu, 6 Jun 91 22:35:42 PDT

Yes, they're still using these two Shuttle Training Aircraft (STA). One of them was here at Edwards last week, for rehearsal for the current mission. JSC will send one (or both, it varies) the day before the landing. They'll put it up before landing, to get the winds aloft for the subsonic portion of the approach and landing.

>To simulate the shuttle's glidepath, you take a G-II up to altitude, ...

I've flown a lifting body approach in a TF-104G Starfighter. Dirty up and pull the throttle back to flight idle (no reverser) and drop like an HL-10/rock/shuttle. From the backseat it's damn spectacular.

I've seen video/film footage of inflight thrust reverser deployment for transport aircraft. This is required for FAA certification of civil transports. It's usually a somewhat boring bit of film, since nothing dramatic happens. All you really see is the reverser deploying, which is kind of cute for clamshell reversers.

However, the YF-12 and the SR-71 exhibited a phenomenon known as the "unstart". Essentially the engine control system (I hesitate to refer to this as a computer) would get goofed and the inlet would swallow the shock. The airplane would yaw violently and lose 10,000 ft. One of our test pilots likened to it being broadsided by a train. The control system was modified and unstarts went away, much to everyone's relief.

Mary Shafer shafer@skipper.dfrf.nasa.gov ames!skipper.dfrf.nasa.gov!shafer
NASA Ames Dryden Flight Research Facility, Edwards, CA

RISKS of Management Attitudes

Tim Steele <tjfs@tadtec.uucp>
Sat, 8 Jun 91 15:05:53 BST

When I was working for a British computer company (and major defence contractor) ten years ago, I had an unfortunate experience.

A friend came to me and said that he had discovered that it was possible to enter the on-line personnel database with *no* passwords from any terminal in the building. I found this difficult to believe, so he demonstrated this to me in a highly effective manner, retrieving data on several senior employees. The personnel records included fields for driving licence endorsements and confidential manager's assessments of the employee.

I was stricken by conscience, and eventually decided to visit Personnel and explain what I had been shown without revealing my friend's name. I urged them to tighten up their security.

Subsequently, Management decided it would be easier to discipline the guilty party than to add passwords to the personnel system. A hunt was started, and my friend was located on the grounds of above average intelligence and a propensity to work late (we all scrambled for the door at 5pm!). He was severely disciplined and threatened with dismissal.

As you can imagine, I didn't feel too good about it...

The thing that really annoys me is that it *was* a cheap solution...

Another occasion when this came up was during my employment with a large American computer company some years later. I discovered that a hacker was probing our network, getting into workstations and then destroying them by the use of "rm -rf /" as super user. The penetration was usually achieved by logging in as the lp pseudo-user which had no password and had a normal Bourne shell, then exploiting the world-writable / directory. Both of these security holes were included in the Unix distribution produced by that company.

I laid a trap for the hacker, and we eventually obtained water-tight evidence leading back to a terminal port in an office occupied by one employee.

The evidence was submitted to senior management. We knew that the Company's written policy in such matters was to summarily dismiss the employee concerned, so we assumed the outcome was not in doubt.

The management action taken was to ask the employee whether he was responsible for any malicious action. He was not confronted with the evidence. He denied any such action, and the matter was dropped.

That company is connected to the Internet...

Tim

Company BBS eavesdropping

Andy Duane <aduane@urbana.mcd.mot.com>
Fri, 7 Jun 91 9:08:23 PDT

In RISKS-11.80 (not 11.79 as previously cited), an anonymous poster tells of the chilling effects of people in his company discovering they were being electronically "eavesdropped" by personnel.

In 11.83 there are some suggestions for how to deal with this.

Well, I'd like to relate a "happy" story about BBS eavesdropping. My old company had a long-standing BBS called "graf" (short for "graffiti"). It was a mostly anonymous company-wide BBS that anyone could read or write to. Most engineers did both, and much of middle and upper management at least read it. This was pretty much an electronic suggestion box, although you'd be amazed at what discussions cropped up from time to time. The articles themselves were anonymous, although a central encrypted log was kept showing who wrote what. This log was maintained by "GRAF-man", who was *not* a manager of any type. The log was only to be used if a serious breach of law or policy was observed, and this almost never happened. All very nice indeed.

Well, I moved to a new company, and brought the code to GRAF with me. When I arrived there, the personnel manager informed me that she thought it was a great idea, but only if I would remove from the code all traces of logging! She wanted to be sure that it was not possible to trace an author at all.

This BBS was not only a great morale booster among the engineers, it provided a good way to let your superiors know what you thought without having to sign your name.

Andrew L. Duane (JOT-7), Samsung Software America, One Corporate Dr., Andover, MA 01818 decvax!cg-atla!samsung!duane

---

Re: Government should have less access? (Gilmore, RISKS-11.80)

Michael L. Duerr <motcid!duerr@uunet.UU.NET>
7 Jun 91 18:31:20 GMT

Remember, the risk here is of the government running open - loop with surveillance technology. Harassment is not protected by exclusionary rules. As for dossiers - by saying the magic words "National Security", the government can ignore Freedom of Information Act requests. You would never know that there is a dossier, only that you get audited every year, get thoroughly searched at customs every time, etc.

Unless there are meaningful sunlight laws the technology should protect the citizens from the government. Current trends like [constitutionally dubious] national security preemptions, censorship (a la gulf war), excessive fees for access to government information, new forms government employees must sign ensuring secrecy in all departments, etc. highlight a trend toward greater privacy for the government and less for citizens. Any invasive technology thus poses serious problems.

Could it happen here? Well - would most people even notice if it was?

---

data over radio (Gilmore, RISKS-11.80)

Martin Ewing <ewing-martin@CS.YALE.EDU>
Wed, 05 Jun 91 14:36:25 -0400

But telephone traffic has gone "on the air" for a long time via microwave links. This is becoming less of a problem as optical fiber becomes more universal, but a classical activity of foreign embassies has been to set up eavesdropping equipment to intercept microwave traffic passing overhead, especially in Washington. There was (and is) no legal protection here, except that it has always been unlawful to divulge any communication you may have intercepted from such a common carrier circuit.

At the risk of being flagged in Big Brother's computer, I wonder if there are publicly documented instances of microwave telephone or data transmissions being tapped for nefarious purposes, besides the embassy example.

Re: Government listening to the airwaves (Florack, RISKS-11.83)

John Gilmore <gnu@toad.com>
Fri, 7 Jun 91 01:41:42 PDT

> Let's please make sure that in your (IMHO, overblown) concern about government
> monitoring we don't cripple the government's ability to enforce laws which
> allow the day to day operations of telecommunications equipment to be smooth.

Let's enable the microphone in every room (there's one in most rooms already -- in the telephone) so we don't cripple the government's ability to enforce laws which allow the day to day operations of society to be smooth.

Why should your over-the-air conversations be any less private than those in your house, business, or car?

> Many two-way services are content specific. There are specific channels for
> just about every type of business on the business bands, for example.
> How would you suggest that these be enforced without routine monitoring?

How about allowing the "owners" of these bands to record conversations and provide them as evidence in a suit? Why should we pay the government to listen to every band, when the band's users are already listening and are even motivated to report and prosecute regular abusers?

If special equipment is needed to track down the abusers, I'm sure that commercial services will be glad to do it -- some of them for a contingency fee that comes out of the proceeds of a successful suit.

> Free speech is not the issue in situations like what I suggest. FOr example,
> the business bands, let's say a taxicab channel, for example, is not the place

> to be discussing political thinking.

Telegraphy was not considered a medium for free speech -- and the laws and regulations around it definitely and obviously didn't have the First Amendment in mind -- because who would pay $5/word for free speech in the days of penny newspapers? But those regs became the precedent for telephone regulation, and later radio and TV, and later cable. Who would suspect that the Fairness Doctrine, or Federal regulation of the content of signals traveling in local coaxial cables, would come out of prohibitions on use of private code books in international telegraphy? [We're having to fight and pray that the same precedents are not upheld in cases involving computer communications, or we lose our speech rights in that medium too.] See Ithiel de Sola Pool's great book _Technologies of Freedom_.

> The issue as I say, is not free speech,
> but rather, the effective and efficient use of the bandwidth.... a matter for
> the FCC to determine, certainly.

It seems to me that effective and efficient use of the bandwidth would be for the *users* to determine. The FCC didn't think ASCII was effective use of bandwidth in the amateur radio service until the late '70's -- transmit in Baudot, or lose your license! FCC's concern is *politics*; users are the ones who want to have high bandwidth and high reliability of communications.

The Bush Administration thinks so highly of FCC's ability to allocate spectrum, that it wants to *auction* 200MHz previously reserved for the government, rather than have FCC parcel it out politically.

Re: Listening? (Eric Florack, RISKS-11.83)

Geoff Kuenning <desint!geoff@uunet.UU.NET>
Thu, 6 Jun 91 03:44:15 PDT

> Many two-way services are content specific. There are specific channels for
> just about every type of business on the business bands, for example.
> How would you suggest that these be enforced without routine monitoring?

Well, what sort of leaps (or perhaps pole-vaults) to mind is that the FCC could wait for a complaint, and then monitor to verify the complaint. Note that this is not "routine monitoring." Most of the business bands (e.g., taxicabs) are not going to suffer too severely in the meantime, relative to the U.S.'s historical and constitutional predilection for freedom and restricted government even at the expense of inefficiency.

Geoff Kuenning geoff@ITcorp.com uunet!desint!geoff

EFFector Online 1.07: S.266 Loses First Round

Christopher Davis <ckd@eff.org>
Fri, 7 Jun 91 17:42:51 -0400

EFFector Online|EFFector Online|EFFector Online|EFFector Online
EFFector Online|EFFector Online|EFFector Online|EFFector Online
Volume 1 Issue:1.07
Friday June 14, 1991

SENATE ANTI-ENCRYPTION BILL WITHDRAWN
WILL BE REPLACED BY A NEW OMNIBUS CRIME BILL -- S.1241
SENSE OF CONGRESS LANGUAGE RESTRICTING ENCRYPTION REMOVED

When Senate Bill 266 was proposed, some of its provisions would have restricted the rights of individuals to secure online communications through the use of encryption programs. The specific language was:

> "It is the sense of Congress that providers of electronic communications services and manufacturers of electronic communications service equipment shall ensure that communications systems permit the government to obtain the plain text contents of voice, data, and other communications when appropriately authorized by law."

Let stand, this language would have a chilling effect on encryption. It would inevitably compromise individual privacy in telecommunications. The Electronic Frontier Foundation and several other groups determined to oppose this provision.

In the last issue of EFFector Online, we reported we would register our opposition to this clause. In this case, Senator Patrick Leahy (D. Vermont), who chairs the sub-committee on Technology and the Law --a sub-set of the Senate Judiciary Committee-- was the key to this issue.

This week the EFF met with Leahy's staff to present our reasons for the removal of the language dealing with encryption. Today, we were informed that the encryption clause has been eliminated from the new crime bill which replaced the bill originally known as S.266. In addition, Leahy's sub-committee on Technology and the Law has undertaken to study the issues of encryption and telecommunications technology.

To continue this dialogue, Computer Professionals for Social Responsibility, the Electronic Frontier Foundation, and RSA will be holding an invitational workshop on privacy and encryption in Washington later this month. Following the workshop, a press conference will be held to announce a set of policy recommendations on cryptography.

The conference will take place on Monday at 2:00 at the National Press Club (14th & Pennsylvania Avenue N.W.). All interested parties are invited to attend.

-==--==--==-<>-==--==--==-

Please direct all mail regarding EFFector Online to:
editors@eff.org

Proposed Credit Reporting legislation

"Mike Cepek, MGI" <cepek@vixvax.mgi.com>
Fri, 07 Jun 1991 21:44:03 CDT

>From a 7-Jun-91 Associated Press article (c/o Minneapolis Star Tribune):

"Four house members [...] have proposed legislation to update the Fair Credit Reporting Act of 1970.

"Among their proposals are providing consumers with a free copy of their credit report on request, requiring prompt correction of errors [isn't this already required?], requiring credit bureaus to notify consumers after adverse information is placed on their record and prohibiting the release of information for marketing lists unless consumers consent."

The article goes on and on about the tribulations of two men after credit agencies `merged' their records with others with the same name (middle _initials_ were used, one dropped a Jr.).

One lost his job because his Equifax record was `updated' to indicate `his' guilty plea to a charge of attempting to purchase cocaine [excuse me, what is this doing on a _credit report_?]. "Equifax [...] admitted making a mistake, but said it promptly corrected it."

The second man had bill collectors after him about a $1,776 Discover card bill -- of course he doesn't have a Discover card. "Even though it took nine months to clear his record [...] he [said] he feels lucky. [...] `If this had happened four months ago, I probably would still be living in an apartment,' he said." (He bought a house and car prior to the problem.)

This happened to me. It only took me _two months_ to get it fixed. No, those 60+ and 90+ payments records aren't mine, I said. No, I've never lived in North Dakota ("my" former address). No, my spouse's name isn't Kathy (my wife gave me the evil eye about that one). And come on, wake up you guys, my middle initial is not `J'! (they did know that).

While I have a personal vendetta to fulfill by assisting this potential legislation, I ask that other U.S. RISKS readers get involved. While I don't have all the details, I would think that any RISKS regular would strongly support those bits I have mentioned.

-- Michael *K* Cepek

Caller-ID and Risks/Benefits of reusing commands

David Lesher <wb8foz@mthvax.cs.miami.edu>
Sat, 8 Jun 91 8:41:12 EDT

After a long and bitter fight between Bell South and the opposition - spearheaded by the {state, local, federal} law enforcement community and the domestic violence groups - the PSC approved Caller-ID in Florida. They mandated universal free per-call blocking, activated by *67, and per-line blocking for

some LE offices/shelters. (Bell wanted no per-line, and per-call limited to a narrow list of LE offices.)

But it sounds as if Bell South still wants her pound of salt. I hear they've ALSO set up *67 for a per-call UNBLOCK on a blocked line. So the cop (who has NO way of confirming that the line she's using is/isn't line-blocked) dials the same *67 she uses at home, and guess what. The result (besides an appeal) is that I hear no one is planning to order the per-line block. Hmmmm.

wb8foz@mthvax.cs.miami.edu (305) 255-RTFM

UUNET sending Usenet tapes to the FBI

Rick Adams <rick@uunet.uu.net>
Fri, 7 Jun 91 17:12:24 -0400

> Uunet has revealed that they have sold compiled Usenet traffic
> on tape to the FBI. FCC men and telco security [people] are
> known to read the Telecom Digest. God only knows who reads RISKS.

"revealed" is hardly the right word. UUNET sends news to over 800 organizations. Thats never been a secret. We also send news out via tape. There are two reasons to get a tape. 1) Phone calls are too expensive (E.g. Mayalsia or Indonesia) or 2) Site security does not allow modems.

In the case of the now legendary "UUNET sending compiled usenet traffic to the FBI":

1) We gave them a news feed just like any other customer.
2) This was the Violent Crime group at Quantico. They're the behavioral science folks who track the serial killers around the USA. (If you saw "Silence of the Lambs", that was the VICAP group at Quantico). These guys are sharp, fully professional and completely ethical. One of them actively participates with the CERT group.
3) They got Usenet feeds for the same reason everybody else does. -- Once you throw away the 98% crap, you're usually left with some really useful source programs and technical information. (The FBI employs UNIX wizards too!)
4) We stopped sending the tapes years ago, when they became concerned about possibly picking up a virus from one of the programs on the tapes.
5) They gave me a nifty official FBI coffee mug which is now sitting on my desk.

So yes, UUNET has sold USENET tapes to the FBI. Yes, we were paid for this nefarious service (one coffee mug). Yes, the conspiracy freaks have had a field day ever since.

The time to start worrying is when the FBI starts getting news and pretends to be "Quantico Computing Systems" or something. Not when they do it under their own name.

---rick

p.s. how come no one noticed the uucp site "stu", which is at the FBI headquarters building in Washington, DC. (Soon to be West Virginia due to the most outrageous example of porkbarreling by Sen. Byrd I've seen in years)

p.p.s I know that NSA and CIA employees read Usenet and have for (But I don't *think* we're sending it to them...)

The Activated Active Badge Project

<Anonymous>
Fri, 7 Jun 91 11:45:28 xxx

Place: Pod 26 Commons
Time: 10:30am, Friday, June 7
Title: The Activated Active Badge Project
Speaker: Nicolas Graube Cambridge EuroPARC

Olivetti's Active Badge are small devices capable of emitting at regular intervals an infra-red signal which is in turn received by captors placed in every offices, corridors and public places at EuroPARC. Introducing these badges is not an easy task as they are immediately perceived as tracking and logging devices and thus subject to possible misused. I will first reviewed the BirdDog experiment conducted at EuroPARC whose goal was to introduce active badges and study users reactions. Then by following lessons learnt from this experiment I will introduced a distributed architecture for badges and a more general usage of these devices. Within the Activated Active Badge project, badges are no longer considered as tracking devices but are viewed as contextual multi-functional remote controllers. The main goal of the project is to give control to the user both in the specification of its badge semantics and in the becoming of data generated by its badge. I will introduce a simple rule based language enabling this specification. However because the description of the badge semantics using this language is very much a programming exercise, I designed a graphical interface enabling the iconic description of badge activity. I will conclude by listing possible future extensions and showing a video of interfaces designed for controlling Active Badges.

Search RISKS using swish-e

THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

ACM Committee on Computers and Public Policy, Peter G. Neumann, moderator

Volume 11: Issue 86

Tuesday 11 June 1991

Contents

The RISKS of political correctness in computer science

Ed Nilges <EGNILGES@pucc.princeton.edu>
Sun, 09 Jun 91 00:36:11 EDT

An article in Communications of the ACM for November 1990, "Women and Computing", by Karen A. Frankel, cites Danielle Bernstein of the Kean College of New Jersey on Edsger Dijkstra's comments in Communications for December 1989. In the Dijkstra article, "On the Cruelty of Really Teaching Computer Science", Professor Dijkstra argued for a reform in computer science education, basing it on formal mathematics and logic rather than on early exposure to the computer. Bernstein, according to Frankel, feels that Dijkstra is being sexist! This is because, Bernstein claims, that women prefer experimentation and teamwork to the sort of solitary abstract thinking that Dijkstra emphasizes in all of his work.

Bernstein is echoing other feminist authors on logic and mathematics, including Andrea Nye. Nye's "feminist reading of the history of logic", Words and Power,

"deconstructs", if you please, the history of logic from the pre-Socratics to Gottlob Frege (the 19th century German mathematician who attempted to found mathematics on logic.) Nye, and apparently Bernstein, believe that solitary abstract thinking is a typically male activity and to force women to engage in it is sexist.

Nye presents a rather vicious caricature of Frege as a solitary old man. Nye avoids any mention of Frege's intellectual honesty when the young Bertrand Russell presented him with evidence that his theory was so flawed (by the paradoxes of set theory) as to be unusable.

Unfortunately, if comp.risks is any guide, Dijkstra is right and Nye and Bernstein are wrong. Given the scale and potential for disaster in errors in software, programmers need to do MORE solitary and abstract thinking...not less.

I teach the C programming language as a consultant at a major midwest financial firm from time to time. In my classes, I have two distinct groups of students: Americans and Russian emigres. The Russian students are significantly more adept, although they are programmers originally educated in Soviet technical institutes and universities that lag far behind American schools in computer technology. When I talked to the Soviet students, I learned that they had greatly benefited from a mathematical background that included calculus in grade school. Add to this the UNavailability of machine time in the Soviet Union (waits of a week for time on batch systems not unheard of), and these programmers became skilled at the solitary, highly abstract, and distinctly non-experimental activity of writing carefully designed programs and of desk checking code.

Meanwhile, many of my American students, educated in the regimes of experimentation and of teamwork that Bernstein recommends, are confused and bored by the C programming language, with its more structured syntax, its lvalues, and its rather difficult semantics. I admit to using a rather formalist approach to teaching including railroad diagrams of syntax and playing computer, but I do try to liven things up with jokes described by some students (alas) as "corny."

I find NO sex differences. Russian emigre women in these classes are just as adept as their male counterparts, whereas the American women by and large had more difficulty. [There were American exceptions, students just as able as the emigres, but NO outlier Russians: no Russians were confused by the course.]

It is true that teamwork can sometimes lead to better software. But Gerald Weinberg et al. introduced the notion of "structured walkthrough" in the late Sixties NOT as a way to design software, but as a way to review software, and "typically male" solitary and abstract thinking a la Frege (not to mention Frege's intellectual honesty) is an excellent preparation for the most grueling structured walkthrough. Also, the results of group CREATIVE effort (as opposed to group review effort) can often resemble the famous camel: "a horse designed by committee". The history of software is littered with the bleached bones of such camels, including Cobol.

It's sad that political correctness should find its way into formal computer science where MATHEMATICAL correctness is what is needed. Anti-racist,

anti-war, anti-sexist "political correctness" is needed nowadays, and I am doing some work in the applicability of "critical theory" (the philosophical background of political correctness) to software creation. But forcing teachers of introductory computer science to be "politically correct" and avoid hard subjects in order not to be sexist does a disservice to the profession and to women computer scientists.

There's a Ford in your future (and your past!)

John Moore <anasaz!qip.john@asuvax.eas.asu.edu>
Sat, 8 Jun 91 8:30:26 MST

CNN has been running a story about a Ford Motor Co. "customer flight recorder." This is a device that is installed in a car when a customer has an intermittent problem. Mechanics can later read it out and attempt to diagnose the problem.

There seems to be some risk to this. If one has an accident while this is installed, the data in the machine might be used in a subsequent lawsuit or prosecution. Presumably it is recording speed and other operating parameters.

John Moore, 7525 Clearwater Pkwy, Scottsdale, AZ 85253 (602) 951-9326
HAM:NJ7E ...{asuvax,mcdphx}!anasaz!john or john@anasaz.UUCP

Public Key Crypto Freeware Protects E-MAIL

Philip Zimmermann <prz@sage.cgd.ucar.EDU>
Fri, 7 Jun 91 11:39:59 MDT

At a time when the Government seems bent on keeping the public from having access to electronic privacy technology, there is now a freeware MSDOS software application that protects E-mail and files via public key cryptography. Philip Zimmermann's program, PGP (Pretty Good Privacy), provides privacy and authentication without the hassles of managing keys associated with conventional cryptographic software. No secure channels are needed for users to exchange keys. PGP combines the convenience of RSA public key cryptography with the speed of conventional cryptography, fast message digests for signatures, data compression, and sophisticated key management. And PGP performs the RSA functions relatively fast. PGP is RSA public key cryptography for the masses.

PGP version 1.0 is now available through electronic distribution for MSDOS in the compressed archive file PGP10.ZIP, containing the executable binary and user documentation. This release file can be found on BIX, Compuserve, FidoNet, in comp.binaries.ibm.pc and alt.sources on Internet, the WELL, PeaceNet, EcoNet, EXEC-PC, and many other BBS systems. A separate file, PGP10SRC.ZIP, contains all the C source code and can be found on most of these same networks.

--Philip Zimmermann, Author of PGP (Pretty Good Privacy)

[Added postscript:] The manual directs end users to contact PKP for patent licensing, and gives their phone number, and warns of their patent. I also warn of probable export restrictions. Source code is under FSF Copyleft, which makes it hard to make any commercial proprietary derivations from the source code. I'd like to make this additional statement:

PGP is an educational effort. I want people to know how they can protect the privacy of their personal electronic communications and confidential information. PGP provides an educational example; an independently-developed working prototype that illustrates how it can be done. I want to guarantee that the detailed knowledge of, and access to, this technology cannot be suppressed by Government. Once people know that real security and privacy is possible, I hope that they will make lawful use of it in accordance with patent law.

The inventors and patent holders of the RSA cryptosystem deserve renumeration for their brilliant contribution to cryptography. I strongly urge end users of PGP to obtain licensing of the RSA algorithm from Public Key Partners. The "PGP User's Guide" provides more detailed patent information and how to contact PKP.

Airbus offers autothrottle option, from FLIGHT INTERNATIONAL

Robert Dorsett <rdd@cactus.org>
Sun, 9 Jun 91 18:49:45 CDT

RISKers may recall a threat by Airbus Industry (documented in "Airbus May Add to A320 Safeguards, Act to Counter Crew 'Overconfidence'", AVIATION WEEK & SPACE TECHNOLOGY, April 30, 1990, p. 50) to extend flight-path protections, following the crash of an Airbus A320 in Bangalore in early 1990. In that crash, it was believed that the pilot had kept his energy state too low. Thus, even though the aircraft was said to be "protecting" the pilot from a stall, it was still too slow to recover from the steep glide path. The following article by Julian Moxon appeared in the May 1, 1991 FLIGHT INTERNATIONAL.

"Airbus Industrie has decided on an optional change to the A320 autothrottle software, which is designed to prevent pilots allowing the aircraft to crash because it has insufficient flying energy.

"The modification, to be offered to all A320 operators, follows an earlier, Airbus mandated, autothrottle update resulting from the 1991 crash of an Indian Airlines A320.

"In that incident, the pilots allowed the aircraft's speed to decrease below flying speed. The mandatory software changes cause an automatic, small, increase in engine thrust enabling the engines to spool up faster if the pilot has to advance the throttle suddenly.

The software update is designed to warn pilots who are hand-flying the aircraft that its flying energy is becoming dangerously low. This could occur with the autothrottle switched off and the aircraft in an excessively nose-high attitude.

"'The A320 is stall protected,' says Airbus engineering vice-president Bernard Ziegler, 'but not against lack of sufficient energy. So we're introducing a new concept: to provide the crew with a warning about the aircraft's energy status.'

"Ziegler says the modifications are the only ones that have had to be made to the A320 flight control software since the aircraft was introduced. He says there will be no change to the flight control laws of the A330/A340, '...which proves we got it right from the beginning.'"

As a historical note, Ziegler was a point man in Airbus's scam to clean up the controversy after the Habsheim crash. Only pilots make mistakes, see...

Robert Dorsett rdd@cactus.org ...cs.utexas.edu!cactus.org!rdd

---

More on Thrust Reversal Accidents

Falconer <rteasdal@polyslo.CalPoly.EDU>
Tue, 11 Jun 1991 04:22:33 GMT

The loss of an aircraft due to an uncommanded thrust reverser activation is not unknown. Earlier this year, a USAF C-5A transport was destroyed on takeoff at Ramstein AFB in Germany, during a Desert Shield deployment flight. The accident was blamed on the mechanical failure of a thrust reverser detent, which took place during full-thrust climbout. The C-5 became uncontrollable and crashed seconds after wheels-up, with complete loss of life. It is quite fortunate that the big bird was not serving as a troop carrier at the time; as it was, I believe that about twenty lives were lost, all of them aircrew or supernumerary passengers.

Russ Teasdale -- rteasdal@polyslo.CalPoly.EDU -- (Falconer)

Computer Privacy (cont'd) -- Letter to The Economist

<cdp!mrotenberg@labrea.Stanford.EDU>
Mon, 10 Jun 91 16:45:04 PDT

Ed Ravin (11.63) and Paul Johnson (11.66) noted the recent article in The Economist on Computers and Privacy. The article is particularly important because the Europeans are now considering an extensive directive on data protection in anticipation of the formalization of the European Community in 1992.

I sent the following letter to The Economist which appeared this week (June 8). I post it here because there continues to be some confusion about the opposition to Lotus Marketplace.

> Sir- Your raise important questions about computers and privacy (May 4th). In the United States, consumers and privacy advocates joined forces to oppose the release of Lotus Marketplace, which

would have provided information about consumers' income and buying habits. This was not, as you suggest, because small organizations might obtain information available to larger organizations. We opposed Marketplace because information that was provided for the purpose of obtaining personal credit was going to be sold for direct marketing without any effective mechanism for consumers to opt out. This practice may well be illegal under the Fair Credit Reporting Act, and was clearly unethical.

It is generally true, as you say, that more information is better. The problem with the sale of personal information is that it often occurs without the knowledge or consent of the individual involved. It is a form of unjust enrichment that accrues in greatest measure to those organizations that are most deceptive in their collection of personal information. To condone this practice is foolhardy.

Marc Rotenberg, Washington DC,
Computer Professionals for Social Responsibility

Freedom, Privacy & Technology SIG

Lance J. Hoffman <hoffman@eesun.gwu.edu>
Tue, 11 Jun 91 8:55:37 EDT

[Forwarded by Professor Lance J. Hoffman, Department of Electrical Engineering and Computer Science, The George Washington University, Washington, D. C. 20052 (202) 994-4955 fax: (202) 994-0227]

BMUG, Inc. Computer Professionals for Social Responsibility
. . . . . Berkeley Chapter

Special Interest Group on Freedom, Privacy and Technology
Formed by BMUG and CPSR/Berkeley

The "Special Interest Group on Freedom, Privacy and Technology" has been formed in a unique effort by the Berkeley Macintosh User Group (BMUG) and the Berkeley chapter of Computer Professionals for Social Responsibility (CPSR/Berkeley).

Judi Clark, principal organizer of the interest group for BMUG/CPSR-B, said it will hold free monthly meetings, open to the public, on Sunday afternoons, at the BMUG office, 2055 Center St., Berkeley - a half block from the Berkeley BART station.

The inaugural meeting will begin at 2 p.m. on Sunday, June 30, 1991. It will feature a discussion of "Current Freedom and Privacy," by Alameda County Assistant District Attorney Don Ingraham and futures columnist and computer entrepreneur Jim Warren. The comments will focus on protecting personal privacy, personal property and traditional constitutional freedoms in the "Information Age." It will include issues raised at the recent First Conference on Computers, Freedom and Privacy, a landmark event that received extensive

national press and was described by one television reporter as the "constitutional convention of cyberspace." Mr. Warren chaired that Conference, and Mr. Ingraham served on its Program Committee.

Ms. Clark said it will be the first in an ongoing series of presentations on electronic freedom and privacy issues, cosponsored by BMUG and CPSR/Berkeley as part of the formation of a unique "special interest group" on such issues.

"We will encourage public consideration of the current issues in our changing technology - issues that will inevitably affect all our lives, whether or not we personally use computers," Clark said.

The group will begin with a series of free presentations by professionals from the fields of telecommunications, law, marketing and information management, with plenty of time for questions and discussion, she said.

Clark said the decade of the 1990's will be pivotal in terms of laws, regulations and policies relating to increasingly pervasive electronic media: Individuals, organizations and governments are increasingly dependent upon computers, databases and telephone-line networks.

"The collection of information into databases and libraries has a legitimate and often commercial value," she said. "Most of this information needs to be readily available to enhance sound decision-making by individuals, organizations and governments."

"However, such unbridled public access to vast amounts of often personal information will prompt growing concerns about privacy, and these concerns need to be considered early in the policy making process, before they get lost," Clark said.

Some specific issues to be addressed in coming months include:

o How the Constitution's Bill of Rights defines "freedom" and "privacy" in the First, Fifth and Sixth amendments - a particularly timely issue during the 200th anniversary year of the Bill of Rights.

o How the legal system will deal with the new technology, such as the NCIC 2000, a nationally accessed database system used by the FBI, police departments and their patrols, and others.

o What do the terms "secondary use" and "search and seizure" mean in terms of computerized data and network information?

o What role credit companies, utilities, and medical facilities might play in the future.

Please feel free to post this release anywhere you wish. Thank you for your interest and support.

For more information, contact Judi Clark, 549-2684 (BMUG), 261-3718 (direct), fax: 261-1869 (direct) or e-mail judic@well.sf.ca.us June 5, 1991

Search RISKS using swish-e

Report problems with the web pages to the maintainer

Search RISKS using swish-e

THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

ACM Committee on Computers and Public Policy, Peter G. Neumann, moderator

Volume 11: Issue 87

Tuesday 11 June 1991

Contents

Re: The impact of formalism on Computer Science education

Hal Pomeranz <pomeranz@isis.dccs.upenn.edu>
Tue, 11 Jun 91 13:17:21 EDT

I was dismayed by Ed Nilges' (egnilges@pucc.princeton.edu) article in RISKS-11.86. Ed discussed a recent CACM article by Karen Frankel, citing Daniele Bernstein's criticisms of Edsger Dijkstra's proposed reforms for Computer Science education. Ed's analysis of the situation appears to have some huge holes in its logic.

Essentially Dijkstra recommends that Computer Science education be based on formal mathematics and logic rather than early exposure to and experimentation with computers. Bernstein notes that women tend to prefer experimentation and

teamwork to solitary abstract thought, and accuses Dijkstra of sexism on the basis that the proposed educational reforms would present a barrier to women in Computer Science.

Ed concludes "Dijkstra is right and Nye and Bernstein are wrong" because he believes that the sort of solitary thinking about formal mathematics and logic encouraged by Dijkstra's reforms will lead to better (less error prone) software. It has not been sufficiently demonstrated to me that this sort of thinking leads to better software, but that is not the basis on which I would like to argue with Ed.

Bernstein's criticism of Dijkstra relates not so much to the practice of programming and other areas of Computer Science, but rather to the education of future programmers. Several studies have noted that, from an early age, girls in Western societies are not encouraged to take up activities which lead to careers in scientific fields, particularly Mathematics, Computer Science, and Engineering. Bertstein's criticisms are, I believe, pointing out that the changes proposed by Dijkstra would be yet another barrier to women wishing to enter the field of Computer Science. It would be akin to requiring a student who only knows conversational German to learn something from a German technical article-- there is a "language" barrier which is very difficult but not impossible to overcome. However, if I were that student I wouldn't even bother.

Ed goes on to support his argument with a description of his own experience teaching C programming to American and Russian emigre students. He notes that, due to scarce resources, the Russian students are learning in an environment that is similar to the one that Dijkstra proposes. He states that he finds "NO sex differences". This may be true, but is the ratio of women to men in his courses the same as the ratio of women to men in the population (choose your own demographics) as a whole? If, as I expect, this ratio is much lower than the ratio for the general population, then it would suggest that the Russian curriculum is discouraging to women. The Russian women in Ed's classes are those few women who are able to "hack it" in the rigorously mathematical and abstract Russian system.

It may well be that more formal training turns some people into better programmers. It is certainly the case that formal training turns a lot of people off or presents an impossible obstacle to many groups (not only women). I believe that many of these people could become excellent programmers, or professors of Computer Science, or researchers, etc. However, if Dijkstra's proposals are widely implemented, chances are that none of this latter group will get the opportunity. This, then, is Bernstein's criticism of Dijkstra's proposal.

It is unfortunate that Bernstein slings the word "sexist", and that Ed feels threatened enough to counter with the (now) negatively connotated term "politically correct" which raises all sorts of spectres of thought police.
All education would benefit from massive dose of new and different thinking, so as to encourage marginalized groups to participate more fully, rather than a retreat to older, more formal approaches which would only push groups on the outside farther out.

Hal Pomeranz pomeranz@dccs.upenn.edu

Fighting phone hackers in SoCal

Mark Seecof <marks@capnet.latimes.com>
Tue, 11 Jun 91 10:29:55 -0700

Excerpts from an article published in the
Los Angeles Times May 17, 1991; page E1.

Edited and submitted to RISKS Digest by
Mark Seecof <marks@latimes.com> of the
L.A. Times Publishing Systems Department.

[elisions and bracketed comments mine --Mark S.]

``Little Phone Company on a Hacker Attack''
By Susan Christian, Times Staff Writer.

[Introductory blather...]

[...] in the last seven months [small long-distance company] Thrifty Tel's [security chief] has put seven hackers in jail. And she has made 48 others atone for their sins with hard cash and hardware. The case that [security chief] Bigley calls her biggest coup--involving a 16-year-old Buena Park boy whose alleged theft of computer data cost Thrifty Tel millions of dollars--is pending in Orange County Superior Court.

Thrifty Tel has become one of the most agressive hacker fighters in California, according to Jim Smith, president of the California Assn. of Long Distance Telephone Cos. (Caltel). ``[Bigley] is tough,'' he says. ``I would not want to be a hacker on her network.'' So far, the company has collected more than $200,000 in penalties and reimbursements from hackers.

``We do not have a hacking problem any more because we stood up and punched them in the face,'' Bigley proclaims. ``These kids think that what they're doing is no big deal--they're not murdering anyone,'' Bigley says. ``They think we're terrible for calling them on it. Their attitude is extremely arrogant. But these are not just kids having some fun. They are using their intellect to devise ways to steal. And these are not kids who need to steal. They come from white-collar families.''

For Thrifty Tel Inc., the battle of wits started a year ago. [...Thrifty Tel is ten years old, went public in '86, and serves 7,000 customers in SoCal.] [...Last year the hackers discovered them. Hackers use computer programs to try many possible code numbers until they find the ones which unlock the system.]

``The first quarter of 1990 we came in with a half-million-dollar net profit, and everything was going great,'' Bigley says. ``Then the next quarter, all of a sudden we were lopsided. We were getting bigger bills from our carriers than we were billing out to our customers.'' With a little investigation, the company pinpointed the culprits: hackers who were eating up telephone time at as much as ten hours a ``conversation.'' Because hackers exchange information

and solve secret codes via long-distance modem connections, circumventing expensive telephone charges has become their mainstay. ``It was so frustrating to sit here and watch these hackers burn through our lines,'' says Bigley, a 33-year-old San Fernando Valley resident. She has been vice-president of operations at Thrifty Tel for four years. ``I had technicians out changing customers' codes that they'd just changed a few weeks before.''

But Bigley is not the sort to throw in the towel. [...She is hard-working and persistent.] First, she devoted a couple of months to educating herself about hacking. She monitored Thrifty Tel's computers for unusual activity--telephone calls coming into the switching facility from non-customers. ``They believe that because they're sitting in a room with a computer they're safe,'' Bigley says. ``The problem is, they're using their telephone; we can watch them in the act. It's a lot easier to catch a hacker than a bank robber.'' Bigley started making a few calls of her own. If the infiltrator seemed major league, like the Buena Park boy, she contacted the Garden Grove Police Department, whose fraud investigators went into homes with search warrants. If the hacker seemed relatively small, however, Bigley took matters into her own hands, telephoned the suspect and presented an ultimatum: Either pay up or face criminal charges.

A non-negotiable condition of Bigley's out-of-court settlement provided that the guilty party relinquish his (or, infrequently, her) computer and modem. Thrifty Tel donates the confiscated weapons [computers] to law enforcement agencies.

Teen-age hackers tend to be ``very intelligent and somewhat introverted,'' says Garden Grove Police Detective Richard Harrison, a fraud investigator who has arrested many of Thrifty Tel's suspects. Most of the parents he has dealt with were oblivious to their children's secret lives, Harrison says. He suggests that parents educate themselves about their children's computers. ``If a kid is spending a whole bunch of time on his computer and it's hooked up to a modem, he's not just running his software. What is he doing on that computer? Does he really need a modem?''

[ed. note-- this officer may be an expert on fraud but is clearly unqualified to make such sweeping assertions about what (young) people do with computers. Playing rogue can eat up as much time as hacking while the modem remains idle.]

Not all hackers are young computer fanatics testing their limits. ``The hacking problem is two-fold,'' says Caltel president Smith, also president of the Sacramento-based long-distance telephone company Execuline. ``First, we have Information Age fraud, which is an outgrowth of the proliferation of computers in households. We have all these kids who want to talk to each other on bulletin boards, and if mom and dad had to pay for all those phone calls, the cost would be prohibitive. Then we have professional fraud--adults as well as kids who attempt to gain access to our codes for the purpose of selling the codes. They have made a big business out of hacking.'' Smith's company has waged a more low-key defens[e] against hackers than Thrifty Tel. ``I wish I had the time to devote to hacker fraud that she [Bigley] has been able to devote,'' he says.

Therein lies the reason that many telephone companies decline to file charges against hackers, says Roy Costello, a fraud investigator for GTE. ``Smaller

carriers don't have the time to allow their people to do the investigation and then carry it through the court system,'' he says.

[... Stuff about the sticktoitiveness of Thrifty Tel's Bigley and how she thinks that hackers are immoral and wants to defeat them.]

Re: There is a Ford in your future (and in your past) (RISKS-11.86)

Ed Wright <edw@sequent.com>
Tue, 11 Jun 91 9:42:16 PDT

I would suggest that equipment of this type would negate some risks, rather than create new ones. Currently if there is an accident sorting out who was at fault (in non no-fault states) winds up being a long involved process which primarily benefits members of the legal community, and costs the taxpayer lots of money in the form increased insurance premiums down the line, and increased taxes to cover court expenses. With a recorder on board that showed one party was clearly speeding, or failed to apply brakes, resolution could be more straight forward. At worst resolution would be no more involved than it is now.

I am often intrigued by people apparently worrying about the risk of "getting caught". I would presume that if a driver is not speeding or otherwise inappropriately operating the vehicle, then a recorder could be a benefit in resolving a suit, or more mundanely detecting malfunction before it becomes expensive, or in detecting driving habits that are expensive. At worst it would be a nonentity like the controller that runs the cruise control.

Re: There's a Ford in your future (and your past!) (RISKS-11.86)

<tada@ATHENA.MIT.EDU>
Tue, 11 Jun 91 14:39:48 -0400

In other words the risk is that the police might be able to actually determine the cause of an accident based on evidence, rather than on the possibly true account of the participants based on their possibly correct memory?!?

Perhaps the real risk is that the device might be used to determine where your car had been, and when. Like, if the police used it to find out if you had been at a crime scene.

(Perhaps an even greater risk is that of preventing some helpful technology from coming to the market based on the fear that maybe it will stop someone's illegal or unethical behavior as well as helping those who have nothing to lose and something to gain from the new technology. While we should be concerned over privacy concerns, we should also be concerned about the overall benefit to society, etc...)

-michael j zehr

Re: There's a Ford in your future (and your past!)

Bruce Oneel <oneel%heawk1@heawk1.gsfc.nasa.gov>
Tue, 11 Jun 91 12:39:00 EDT

It's been a while since I've read car magazines, but, in the late 70's to early 80's GM started putting engine control computers in some of the more expensive cars. These were to aid in diagnosis. If certain engine parameters were exceded then the computer would remember them and then could dump them out to the mechanic when poked the right direction. I do remember that over rev, temp, and oil pressure were mentioned as being monitored. It would allow a mechanic to say "Well, this really wasn't meant to spin all the way to 8000 rpm..."

bruce

Re: There's a Ford in your future (and your past!) (RISKS-11.86)

Brinton Cooper <abc@BRL.MIL>
Tue, 11 Jun 91 14:09:44 EDT

John Moore writes, regarding a Ford Motor Co. "customer flight recorder..." that is installed in a car when a customer has an intermittent problem (and which) mechanics can later read and attempt to diagnose the problem. He asserts a "risk" in that data so recorded might be used in legal activities following an accident while such a device is in use.

On the other hand, one might ask "risk to whom?" The principal risks in the use of such a device seems to be to the careless driver and to negligent auto manufacturers. Flight data recorders on aircraft seem to be a risky only to the extent to which they fail to provide sufficient information on the cause and responsibility for a crash.

Do we really want to hide behind arguments about "risk" in an effort to avoid responsibility for our actions? One of the great (potential) contributions of computers is their ability to provide information which can improve the safety of our transportation systems. (Yes, I'm aware of the risks of doing this improperly, carelessly, etc.) The risk in John Moore's world seems to be NOT to collect the "flight" data.

-Brint

Active Badges: Article in 16 May "Economist" (RISKS-11.85)

Bob Ayers <ayers@Pa.dec.com>
Sat, 8 Jun 91 17:08:25 -0700

The use of "active badges" at Xerox EuroPARC was the subject of a one-page article in the 16 May "Economist." The article discussed the basic technology, and also discussed the risks of

> "as long as users actually wear their bleepers, the system records where each person has been during the day, for how many minutes, and

with whom. Soon, it will be able to record telephone conversations and identify types of meeting, too ... this will be an 'aide memoire,' but it will also be a way in which managers can keep tabs on their employees."

Re: The Activated Active Badge Project [RISKS 11.85]

<Peter.Robinson@cl.cam.ac.uk>
Tue, 11 Jun 1991 18:00:13 +0100

The article has prompted me to report an interesting risk of using active badges. The main concern here when the system was installed was that the system would assist a thief in identifying empty offices for nefarious purposes. We now have evidence of such a use, albeit for a very minor theft of intellectual property.

I was somewhat surprised the other week to walk past a printer in the Laboratory and see it printing out a draft copy of a book on which I am working. I hadn't printed it. A quick check by our systems manager determined that it had been printed by one of the students in the Department. A further check determined that the student had used the active badge system to verify that I was not in the vicinity when he printed the draft. Unfortunately for him, the print queue jammed for six hours and the job was released at precisely the wrong moment...

The moral seems to be that the risk of systems revealing locations (automatic vehicle identification for road tolls, on-line credit card processing, active badge systems and so on) is not that they allow other people to know where you are (after all, anyone could hire a private detective to tell them that), but that they tell people where you are not.

- Peter Robinson.

Caller-ID

arthur rubin <a_rubin@dsg4.dse.beckman.com>
Tue, 11 Jun 91 14:38:37 PDT

The proposal for Caller ID in California (probably the PUC gave the minimal conditions they would accept) was to have free per-call blocking, no per-line blocking, with no mention of ovverides, except: a blocked call would still be recognized by Call Trace or Call Return. I don't know the current status of the proposal.

---

re: Caller-ID and Risks/Benefits of reusing commands

Andrew Tannenbaum <trb@ima.isc.com>
Tue, 11 Jun 91 18:49:11 -0400

I see that the telco's are fighting to prohibit normal users from specifying per-line blocking of Caller-ID. Is anyone selling phones that will automatically prepend the call-block code (*67 or whatever) whenever you dial, effectively circumventing the lame telco restriction? You can already program it into your speed-dials buffers, but this would allow you to forget about it when you dial normally.

Andrew Tannenbaum Interactive Cambridge, MA +1 617 661 7474

Knock, Knock! (Heritage Cable)

Ed Greenberg <edg@netcom.com>
Sat, 8 Jun 91 14:58:15 PDT

This is quoted from Action Line, a write-in column of the San Jose Mercury News. The paper was dated 8-Jun-1991.

"Q: The other day, I was visited by a representative of Heritage Cable, stating he was here to investigate the purchase of an illegal de-scrambler that he said I bought in 1987. He also stated that he had every right to inspect the line that went into our household. I felt outraged to be woken up -- I work nights -- for such a rediculous and demeaning experience. I've had cable at this address since 1986. Does the Heritage Cable representative have the right to inspect inside our house?

"A: They do, says Mark Solins, Heritage's director of field service. Solin says the cable company receives lists from the Federal Bureau of Investigation every so often with names of people who bought de-scramblers for the purpose of obtaining a cable station without paying the cable company for the right to the air waves. The FBI doesn't monitor all de-scrambler sales, but does get involved if it learns of illegal activity. Solins says the contract you signed when you signed up for cable allows a company rep the right to inspect the cable service and line. Solins says your name popped up on a recent list the FBI sent to Heritage. Solins says no illegal de-scrambler was found in your home. Evidently, someone who used to live in the rear of your property ordered the de-scrambler, under your name and address and used it to pick up cable waves without subscribing to the service."

Ed Greenberg, P. O. Box 28618, San Jose, CA 95159 Work: +1 408 764 5305

[Also contibuted by Mark Thorson, who prefaced the item with this:
"Although not directly related to computer RISKS, it's easy to see how electronic means for detecting illegal cable hookups could be adapted to exploit this mechanism for running roughshod over individual privacy. Mark Thorson (a.k.a. mmm@cup.portal.com)." Mark also added EMPHASIS to the line beginning "SOLINS SAYS THE CONTRACT YOU SIGNED ..." PGN]

Report problems with the web pages to the maintainer

Search RISKS using swish-e

THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

ACM Committee on Computers and Public Policy, Peter G. Neumann, moderator

Volume 11: Issue 88

Wednesday 12 June 1991

Contents

Massive war resistance movement? 1.7 million defective resistors

"Peter G. Neumann" <neumann@csl.sri.com>
Tue, 11 Jun 91 17:02:24 PDT

1.7 million resistors used in F-15s, Patriots, radars, and other systems are being recalled and checked for flaws. Some were shipped back in 1989, others more recently. The resistors were made by Philips Components of West Palm Beach, which is aware of only three failures. The defense contractor Eldec is facing "financial losses because the military is not accepting its shipments of electronic equipment while it searches for the defective resistors." "Philips officials said the resistors also were sold to civilian customers, including commercial aircraft manufacturers." [Stark abstracting of an AP item from the San Francisco Chronicle, 8 June, p. A15] [Instead of resisting defectors, we have defecting resistors.]

> [The risk that a systematically reproduced fabrication flaw could
> be perpetuated though many systems using the flawed component type

is truly a frightening one. The notion of a universal Trojan horse circuit that would fail at roughly the same time throughout the world is even more frightening. (You know how accurately appliances can be made so that they work until just after the warranty expires? Well, that technology could be applied to age-specific fail-certain components. But then, beware of Byzantine systems using multiple sources of separate and supposedly independent sets of circuits where it turns out that one component always comes from the same vendor...!]

Computers and Exporting

<rmoonen@hvlpa.att.com>
Tue, 11 Jun 91 21:20 MDT

In a recent discussion with colleague's of mine, we came up with another difficult point in the information frontier. Legal definition of 'export' does not cover all methods of transport and representation.

Take for instance the DES export restriction. Sources for des have been posted on Usenet. Granted, it was with distribution USA. However, with modems being cheap, and telephone lines readily available, there is nothing to stop someone logging in on a USA Usenet supporting site. Who has now breached the anti-export regulation? The site for being accesible from abroad? The user who downloads the sources? The poster?

What's more, what gets restricted. Sources? Binaries? What if the sources are crypted? They are no longer useable as a program. Not in executable form, not after compilation. (Even if the compiler doesn't blow up :-). Are crypted binaries export resticted?

The problem becomes more complex when you take Patent laws (PKP RSA Patent) and copyright laws into account also.

This discussion started, when I mentioned that our Usenet servers get USA distribution news, while I live and work in The Netherlands. Does this mean that anyone posting export resticted sources that, because of network structure also get distributed outside of the USA, is commiting a crime? I hardly think so. Could someone with more legal experience comment on this?

--Ralph Moonen --rmoonen@hvlpa.att.com

Re: Formalism versus Experimentation

"Eric Postpischil" <edp@jareth.enet.dec.com>
Wed, 12 Jun 91 06:01:04 PDT

In regard to the question of formalism versus experimentation in the education of computer science, let us assume, for the sake of argument, that we are interested primarily in women's achievement and that women prefer experimentation and teamwork to solitary abstraction. Even granting these assumptions, is not the proper question to ask "Which method of teaching women

is best for their learning?" rather than "Which method of teaching women most addresses women's preferences?". That is, even if we assume experimentation and teamwork is best for women, this does not necessarily mean teaching with experimentation and teamwork will produce better women computer scientists than would teaching with formalism.

Sexism, programming, and social goals

Jerry Leichter <leichter@lrw.com>
Wed, 12 Jun 91 08:56:24 EDT

Hal Pomeranz is "dismayed" by Ed Nilges' attack on comments in a CACM article that claim Dijkstra is "sexist" for calling for more formalism in computer science education, since it is observed fact that women are discouraged by subjects based on formal mathematics and logic. He claims that "Ed's analysis of the situation appears to have some huge holes in its logic." I am dismayed by Pomeranz's apparent new definition of "logic."

What's really going on here has nothing to do with "logic"; it is a disagreement on basic goals. Dijkstra and Nilges have the following as their goal for computer science education:

Goal EFF: Computer science curricula should be constructed to educate students in the techniques that have been found to be most effective in producing working, usable, safe, programs.

Pomeranz, Nye and Bernstein (whose CACM comments Nilges was responding to) have the following goal:

Goal EQL: Computer science curricula should be constructed so that women have an fair chance to enter the field of computer science. We determine that this goal has been attained when the percentage of women in the field matches that in the general population.

Having chosen a goal, one can apply logic or empirical investigation to determine whether particular steps are appropriate to it. One can attack Dijkstra by pointing out that few real systems are amenable to the level of formalization he used. One can attack a program attempting to encourage women to take logic courses so that they will be prepared for a Dijkstra-style computer science curriculum by showing that women don't wish to take such courses, or do poorly in them.

However, the choice between the goals (if indeed a choice is necessary) has nothing whatsoever to do with computer science. It touches on fundamental polical and social policies that apply equally well in all fields. Change the references to computer science curricula in the goals to "corporate management structures" and you get a pair of goals that are equally being debated. Change "women" to "blacks" and you get another pair of currently debated goals.

At one time, there was broad agreement that Goal EFF was the only important

one. Then Goal EQL was proposed. Those supporting this goal have gone through three distinct phases:

1. The goals are compatible: Men and women are fundamentally equal. The only reason we haven't attain them is because of current (later, past) discrimination. If we eliminate the discrimination (and through special compensatory efforts make up for the past discrimination) we will soon attain both goals simultaneously.

2. Men and women are essentially different and have different and complementary perspectives on problems. By striking out on their own, women will find new approaches to computer science problems, thus enriching the field. (This particular phase wasn't very visible in computer science, but was universal for several years in such fields as history and psychology.) By working to attain Goal EQL, we will simultaneously attain Goal EFF.

3. Men and women are fundamentally different, and it is inherently unfair to require women to adjust to the male way of doing things. This unfairness is basic, and Goal EQL is essential. Goal EFF is a minor thing in comparison, and any conflict between the two goals must be decided in favor of Goal EQL.

(Before all this, of course, there was a Phase 0: Goal EFF is central, Goal EQL is "nonsense", because "the gal's just don't have a head for logic". Isn't it amazing how far we've come in 30 years?)

My own view is essentially compatible with Phase 1, though I certainly have no objection to those who believe in Phase 2 and are willing to try to create new perspectives: It's hard work, but any such effort has the chance of receiving a major payoff.

Debate with those who espouse Phase 3 is impossible: They have decided that such things as logic and evidence are in and of themselves sexist or racist or whatever. Without such things, debate and reasoned discussion are impossible; all that is left is resort to emotion, rabblerousing, and force (fortunately, usually manifested as laws and regulations). As long as they remain marginal and without influence, they can simply be ignored. When they begin to attain influence, they can be answered only in the same terms.

-- Jerry

---

re: Politically correct computer programming

Martin Minow 12-Jun-1991 0950 <minow@ranger.enet.dec.com>
Wed, 12 Jun 91 07:15:20 PDT

Regarding the discussion of the impact of formalism on Computer Science education, may I point out that "Computer Science" is more than the craft/profession of Computer Programming. It is certainly reasonable to teach computer programming by example, and with very limited exposure to queuing theory, statistical analysis, and the theory of finite-state automata -- after all, we do not introduce accountants to their profession by forcing them to *prove* that 1+1=2.

On the other hand, once one enters the real world, it is indeed necessary to "prove," in some rigorous manner, that the stack will not overflow, that the iteration will converge to a solution, that the ring-buffer will work both when it is empty and when it is full, that the compiler will parse all legal programs and reject all incorrect programs, that the stop light will never show green in both directions, that the database can respond to 200 queries per minute, and so on. For these problems, an understanding of formal methods is essential.

Whether one should learn theory before, during, or after practice is, of course, an open question and one related to university traditions and the use one plans to make of the education. Both, however, are essential and I must respectfully disagree with Hal Pomeranz's claim that people "turned off by formal training" will become excellent programmers. I also disagree with the implicit claim that women are, as a class, less able to absorb formal methods and, consequently, excluded from the profession.

Martin Minow minow@ranger.enet.dec.com

Re: The impact of formalism on Computer Science education

Geraint Jones <Geraint.Jones@prg.oxford.ac.uk>
Wed, 12 Jun 91 11:06:40 BST

The mild altercation between Ed Nilges (RISKS-11.86) and Hal Pomeranz (RISKS-11.87) just goes to show how hard it is to understand someone else if we don't make an effort to see the world from the other bloke's (apparently) cockeyed stand point. Just suppose, for the moment, that bridge building, or as one has to say these days civil engineering, is best approached by the more formal knowing-what-you-are-doing route; and just suppose that education in formal techniques does discourage partcipation by (say) right-handed people.

In that case, one might expect to be able to get more right-handers into the subject by encouraging an experimental approach. However, you would not be educating them as good bridge builders. On the other hand, a rigid adherence to formal bridge design techniques would tend to make civil engineering a profession of a minority of the population. Bridges would become magical objects little understood and much feared by the rest of us. Now, do you want to live in a world where bridges are essentially experimental constructions in which you wouldn't want to trust? No. Or would you prefer a world in which we worship bridge-builders and live in fear and awe of their constructions? Of course not.

I hope you can't tell which side of the argument I would defend if pressed. g

---

Conflicting goals (was Re: the impact of formalism...)

timothy shimeall <shimeall@taurus.cs.nps.navy.mil>
Wed, 12 Jun 91 09:35:51 PDT

Before diving into accusations of sexism, let's be sure that we are

working to the same goal:
Dijkstra (and apparently Nilges) is trying to promote the improvement of quality of programming, building better code with fewer bugs.
Bernstein (and apparently Pomeranz and Frankel) is trying to promote the improvement of participation in programming, allowing more people (in this example, women) to program.
These are BOTH laudible goals, but they are different goals and may conflict. All people (both men and women) do not have an equal talent for mathematical reasoning or inclination thereto. Is it sexist to point out that those with a high level of talent for mathematical reasoning have tools (mathematical techniques) available to use that those with a low level of talent do not have? Is it sexist to suggest (as Dijkstra has) that for some projects with a high need for quality, only those familiar and trained in mathematical reasoning (i.e., only those with the needed mental tools) should be allowed to program? Isn't there a need to differentiate programmers by background and ability, particularly in developement of life-critical systems?

I don't believe that a high level of mathematical reasoning is needed for every programming project. Well-explored, low-risk application areas with a plethora of examples to work from may not demand mathematical reasoning for their programming. There is thus room in the programming profession for some without this talent. I applaud those who seek to encourage sexual equality in hiring those with the needed talents and inclinations for programming. As one who spends a LOT of time inducing individuals (of both sexes, the US military services do not consider sex when selecting for graduate education, and thus our student body is roughly 30% women) to reason logically about programs and programming, I welcome ANY efforts to improve the volume of participation in - and/or level of quality of -- software development.

Tim

Re: Formalism versus Experimentation

<Eric_Florack.Wbst311@xerox.com>
Wed, 12 Jun 1991 07:41:47 PDT

=-=-=-=
Ed concludes "Dijkstra is right and Nye and Bernstein are wrong" because he
-=-=-=-=

IMHO, Ed's right. Since what we are dealing with, when we program, is logic, should we not have the ability to reach conclusions in a logical manner? To that end, should we not have above a passing understanding of logical thought?

I am dumbfounded by:
=-=-=
... Bertstein's criticisms are, I believe, pointing out that the changes proposed by Dijkstra would be yet another barrier to women wishing to enter the field of Computer Science.
=-=-

While you are most correct in your assesment of a lack of educational

even-handedness amongst the sexes, I question your conclusions.. Do we attempt to change laws of chemestry and electricity because of a particular group of students' inability to learn the laws as they are? IE: do we attempt to change reality to aid some people's ability to deal with it effectively? Why, then do you conclude that to learn computer logic, one need not learn logic, first? Is it simply because of one 'minority' or another's inability to deal with that progression?

You say:
=-=-=-=
All education would benefit from massive dose of new and different thinking, so as to encourage marginalized groups to participate more fully, rather than a retreat to older, more formal approaches which would only push groups on the outside farther out.
-=-=-=

It is the retreat from the more formal, (and yes, harsher) learning environments, the 'massive dose of new ideas' that have placed this country into the educational crisis it's in today, where nearly 50% of high school students cannot read effectively. In the 'marginalized groups' as you put it, these percentages are even higher... we expect less of them, so they produce less. What you suggest is more of the same.

It's sorta like the drunks in a car. THe car is in reverse and they notice they're headed for the cliff. THe drunk that's driving comes to the conclusion that the car will move forward if he pushes the gas pedal down real hard. The result, of course, is very predictable.

Sorry, Hal. No sale here.

Eric Florack:Wbst311:xerox

Are women a computer risk? And what about foreigners?

Jean-Francois Rit <rit@flamingo.Stanford.EDU>
Wed, 12 Jun 91 10:31:08 -0700

The discussion revolves around straightening the three following inconsistent propositions:

1 Abstract logic is necessary to the computer industry
2 Logic is not compatible with women
3 Women must have an equal access to the computer industry

Negating one of these propositions is sufficient to make them all consistent. Therefore the issues are:

1 Is more abstract logic necessary to the computer industry? In particular, is it necessary to avoid computer related risks?
This is the abstract, purely technical argument. You can try to prove this, but it won't be easy. A substitute is relating anecdotes in comp.risks.

2 Is logic incompatible with women? This is probably not what should be discussed in this forum. Unfortunately I personally think this is the weakest point and therefore the thing that should be "fixed" if that were the case.

3 Should an equal access of women to the computer industry be enforced, no matter what added risks this involves?
This is the political (in a broad sense) argument.

More than a "Men against women" issue, the discussion stems from accepting or not that politics interferes with pure technic. Computer related risks address the impact of computer technology on society and employment in the computer industry is unavoidably one of them.

Hal Pomeranz likens requiring the use of formalized logic to that of a foreign languages as an arbitrary but effective way of discouraging people from entering a field. What about non-anglophone students who want to enter the computer industry or let's say computer science research?

Most of them have *at best* a knowledge of conversational english, yet they have to access to hard technical literature. Those who are not proficient enough or cannot adapt are definitely weeded out. You can find this perfectly normal or unacceptable depending on how much you think cultural imperialism is relevant to computer education.

Jean-Francois Rit Tel: (415) 725 8813
CS Dept Robotics Laboratory e-mail: rit@cs.stanford.edu
Cedar Hall
Stanford, CA 94305-4110

Caller ID -- The Risks are already here!

Lauren Weinstein <lauren@vortex.com>
Tue, 11 Jun 91 18:59:08 PDT

The Caller ID (CID) situation in California is still undetermined, other than that per-call CID blocking will definitely be provided at no charge, since this has been mandated by state law. It is decidedly unclear whether or not such blocking will be effective on interstate calls, since such calls are an FCC, not PUC (Public Utilities Commission), matter. A similar unclear situation exists with regard to 800 and 900 calls (remember that most 800 calls already have CID attached to them, at least on customer bills--and you can sign up for instant delivery of the caller numbers if you want them). Current rules seem to imply that CID blocking will not apply to 800/900 calls.

I recently sent a letter to the California PUC promoting the need for per-line CID blocking, and asking a number of questions regarding call-return operations when the original caller had blocked their CID (the key question: since it is proposed that call-return would still function in this case, what number would show on the phone bill of the person activating call return in the case of message-unit and toll calls? Would it be marked "private"? Would only a partial number be shown?

As for per-line blocking, I feel strongly that subscribers should not be required to take *extra* steps to maintain a level of privacy that they have already come to expect over the years. Particularly when people are in unusual locations, or under stress, elderly, in a hurry, etc., they are the least likely to remember about dialing special codes--even though they might especially need their number privacy in those situations. Nor should subscribers be forced to purchase special equipment to dial blocking codes for them when they're calling from their "normal" location.

I have proposed that all unlisted/non-published numbers have caller-ID blocked by default, with all subscribers offered a one-time opportunity to choose the mode (blocked or unblocked) that they prefer without charge, after which further changes in the per-line CID blocking status would be subject to a fee. I have also proposed the availability of codes to change the per-line CID blocking status on a per-call basis (both for enabling and disabling CID).

There is a fascinating publication that relates to all of this. It was originally provided to me by a company that builds equipment for CID number capture (Automatic Number Identification -- ANI capture). While it is primarily oriented toward use on existing 800 ANI capture systems, it is obviously looking forward to full-scale CID availability for non-800 calls.

The publication is called "Inbound/Outbound" -- "Using Technology to Build Sales and Deliver Customer Service". It was a supplement to "Inbound/Outbound" magazine from July 1990. It is heavy on the promotion of MCI ANI delivery systems, which isn't surprising when you notice that the publication was prepared under the direction of MCI employees. Many manufacturers of ANI related equipment and systems (including name/address database lookup services) have ads within.

It is a veritable cornucopia of endless praise for ANI/CID systems--I was unable to find a single negative statement concerning these systems. As far as they are concerned, ANI/CID is the best thing to happen to sales since the invention of the phone. There are database services who can search between 60 and 90 million name/address entries "instantly" over networks in response to incoming ANI phone number info, and others who will take a tape or floppy and get you the info "offline" at a lower price.

One of their suggested applications for ANI/CID is hanging up on or refusing to answer calls from "suspicious" phone numbers with which you've had problem calls in the past (the RISKs are obvious). Another is recognize the phone number of your better customers and route them to operators ahead of all the other poor slobs waiting for assistance. Yet another is call back people who hang up without waiting for an answer on your sales lines.

Overall, they list a range of applications (including various authentication applications) that seem to imply that (1) Everyone wants everyone to know who they are when they make a simple call, (2) Your customers will always call you from the same phone number, and you have the right to call them back on whatever number they happen to call you from, and (3) People hardly ever change their phone numbers.

They also throw out the usual arguments about the use of ANI/CID in emergency situations, even though we all should know by now that 911 services are exempt

from CID blocking.

Most of the associated privacy RISKs with this technology have been discussed in this forum before, but I want to emphasize the incredible degree to which the intertwining of ANI/CID and database services can result in instant information about the caller (or rather, about the caller's phone number!) being provided to the entity being called, (though not necessarily accurate information, of course!)

Not only can name/address be provided from the caller phone number, but also other nifty data such as "dwelling unit code" (what kind of residence are you living in? Do you live in a "bad" part of town?) and "wealth code" (are you rich? Does the company even want to bother talking to you?), and numerous others.

There is also apparently talk of connecting into the credit inquiry databases so that, essentially, when you call a firm, it is possible that everything about that call will have been determined based on the voluminous information they were able to dig up from your phone number during a couple of rings! How you will be treated, who will answer your call, how long you wait in the queue, what they will say to you, and a range of other decisions can be made before you've said *one word* -- all based on the phone number from which you're calling, with all the issues of privacy and accuracy that accompany such a scenario.

And remember--this is happening *right now*. These services exist today; they can be subscribed to immediately. Your area does not need to have local CID for your number to be transmitted via 800 or 900 calls--in fact, about 90+% of the phones in the U.S. are already transmitting their numbers on 800 and 900 calls. As more areas achieve "equal access" long distance carrier status, that number will eventually reach 100%. Local CID blocking will probably *not* block the delivery of your number via 800/900 calls under the current rules, though the definitive status of such calls remains unclear.

We need federal legislation to address these issues, and we need it now. These concerns can not be dealt with effectively on a local or state basis. It's up to those of us who are aware of the dangers inherent in these systems to make our concerns known and push for appropriate improvements in the Privacy Act and other related legislation.

Please feel free to contact me if you'd like further information about any of these topics.

--Lauren--

Search RISKS using swish-e

THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

ACM Committee on Computers and Public Policy, Peter G. Neumann, moderator

Volume 11: Issue 89

Thursday 13 June 1991

Contents

Re: Formalism vs. Experimentation (RISKS-11.86 [,87,88])

Nancy Leveson <nancy@murphy.ICS.UCI.EDU>
Wed, 12 Jun 91 11:57:13 -0700

I am dismayed by the focus in this discussion on making everything into dichotomies: women cannot think logically or do mathematics, men can. Women work well in cooperative problem solving, men don't. Software should be developed using logic only, software should not be developed using logic.

First, I have never heard of Danielle Bernstein or of Kean College. Karen Frenkel is an editor on the staff of the CACM, and, as far as I know, she is not a computer scientist or mathematician. I don't understand why everyone in this discussion has taken these two people's comments as somehow being informed and knowledgeable. Perhaps it is because they fit the common stereotype -- the one that has resulted in women having so much trouble breaking into scientific fields. I personally do not believe that women are less capable at mathematics and logic than men -- but our society teaches them at a young age that it is not feminine to be good at these things. It is not very surprising to me that girls start to do poorly in these classes just about the time they reach puberty and start becoming interested in boys. I remember lying about being a

math major because when I told boys this, they would give me a funny look, screwing up their faces and saying "you must be a brain" (which sounded very much to me like "you must be a freak"). NOBODY wants to be known as a freak, male or female. Boys in our society adjust their behavior to avoid doing things that make them appear feminine.

Because of the stereotypes, women who are interested in math and logic are discouraged and told that they should do something else because they will never be good at it. Whenever one of the stupid studies that say women are not good in math is published in the popular press, the number of girls enrolled in advanced math classes plummets. When I taught high school math, I found both teachers and parents discouraging girls from taking advanced math. They are told to concentrate on subjects that "girls are good at." I used to get so frustrated when parents of some of my best students (female) would tell them they should major in English or another "female" subject. If the boys were having trouble in math, the parents would immediate help them or hire a tutor. If the girls were having problems, they were told that girls weren't supposed to be good in math and not to worry about it. Maria Klawe told me a story about recently visiting a high school chemistry class. It was the first day of the term and the teacher was going through the table of contents of the textbook and describing what they would be learning. Of one chapter he said, "This chapter is very mathematical so the girls won't do well on this part of the class." Real encouraging -- the way to get people to do well is for an authority figure to tell them before they start that they won't succeed :-).

Second, although I believe in applying formal methods to software engineering, I have never seen any person produce a million line piece of code by sitting back and thinking logically about it. Djkstra does not deal with large programs. The developers must work cooperatively together in producing that software (including reviews, etc.) to build a reasonable product. Trying to dichotomize the skills required here is wrong. It takes both an ability for logical thinking AND the ability to experiment and work together cooperatively. Instead of taking something said in the CACM as gospel, look around you. Are the female programmers you see less able than the men? The women I find in industry are wonderful. Perhaps they have to be to get past the stereotypes and other barriers that this discussion and the messages that have been sent to Risks about this have shown are out there.

Now, to be really provocative, there is some evidence that women are better at using "both sides of their brains" than are men (who tend to be analytical but not good at other skills). Perhaps that means that women will actually be better than men at developing complex software products :-). If you are male and get irate at this statement because I have just stereotyped all males, imagine how women feel who get this all the time.

nancy leveson

Re: Formalism vs. Experimentation (Jones, RISKS-11.88)

Steven Philipson <stevenp@kodak.pa.dec.com>
Wed, 12 Jun 91 14:36:38 -0700

I found your article in RISKS interesting, but there is a point on which I'd

like to comment.

> ... Or would you prefer a world in which we worship bridge-builders and live
> in fear and awe of their constructions? Of course not.

It seems to me that we do live in the world of your latter case. Civil engineers _are_ a minority of the population, and their work is not understood by the majority. Engineering is indistinguishable from magic for many. Most people blindy trust the engineer's work because it is both highly reliable and pervasive in our environment. A person in our society would find it very difficult to avoid contact with all technologies he or she doesn't understand.

There is another minority profession that is just as opaque to layman but is feared by some. Most people have no understanding of how aircraft fly, and have mixed feelings about pilots as being something of a cross between magician and daredevil. Many people are afraid of flying but fly anyway as their are few, if any, reasonable alternatives for their transportation needs.

It is my opinion that it would be extremely bad for us to change our system such that it would become possible for people with lesser ability or restricted training to assume major responsibility in technologically demanding fields. Public safety demands competence, irrespective of the majority's ability to understand or perform the work itself. This may not require us to stand in awe of all professionals, but we must at least appreciate that not everyone has what it takes.

Steve Philipson

Re: Formalism vs. Experimentation (Pomeranz, RISKS-11.87)

Ed Nilges <egnilges@phoenix.princeton.edu>
12 Jun 91 21:45:45 GMT

>... However, if I were that student I wouldn't even bother.

Huh? What is a university about, save getting a student from point A to point B? Why is the "necessary violence" of teaching discriminatory?

And in Computer Science there is no "conversational German." It's all technical. Bernstein feels it would be less sexist to have the students who wish to learn high-level languages and packages. However, Computer Science is not about low-level language and you can discuss effective algorithms in the highest-level language.

>... The Russian women in Ed's classes are those few women who are able to
> "hack it" in the rigorously mathematical and abstract Russian system.

Actually, there are probably MORE women working as scientists and engineers within Soviet technical institutes and universities, proportional to the population, than in American universities: and it can cogently be argued that the lower on-the-job sex discrimination experienced by Soviet women (balanced, unfortunately, by a "second shift" worse than that of their American counterparts) is a result of a more demanding, and more formal, education in

mathematics.

INFORMALITY can create much discrimination as dropping formal (and hence visible) criteria results in there being unspoken discrimination based on class, race and gender. Mathematics has historically been a path out of invisibility for low-status males (one is reminded of G. H. Hardy's discovery of the brilliant, but completely unknown, Indian mathematician Ranumujan). It has not, historically, performed the same function for women, but that is because of extra-mathematical discrimination...the source of which is very often the less-than-competent teacher of mathematics with his own, undealt-with, issues around math anxiety. One thinks of the women who were able to end-run the prejudices around mathematics by entering "the most difficult part of applied mathematics" (Dijkstra): Ada Augusta and Grace Hopper.

>It may well be that more formal training turns some people into better
>programmers. ...

I'm sorry, I have never seen how anything less than SOME sort of formalism (from automata theory to decision tables) has ever resulted in any progress in the field of programming.

>All education would benefit from massive dose of new and different thinking...

Here's one example of "new and different" thinking in education. Students in a poor Brooklyn district are being allowed to watch "kiddie slasher" movies in their assembly period, including "Child's Play 2." I suggest that this racist pandering to the absolute worst in students is the logical end-point of these attempts to sugar-coat and deflate the curriculum in the name of fairness. Better the brutal frankness of affirmative action than this.

Re: The RISKS of political correctness in computer science

Michael Tobis <tobis@meteor.wisc.edu>
Thu, 13 Jun 91 04:24:30 GMT

Hal Pomerantz, it appears to me, has completely missed the point of Ed Nilges' comments. It is more than "unfortunate" that the word "sexist" is used in an argument about the emphasis which formal and rigorous thought should have in computer education. It is symptomatic of a very significant risk to academic thought which, rather incredibly, is leaking out of the liberal arts and soft sciences into a critique of rigorous thinking itself.

In a nutshell, the problem is not the extent to which formal automata theory, software engineering, verification, etc. should be presented in an undergraduate program. The problem is that the issue is being attacked _on the grounds_ of its social/political appropriateness, rather than its utility.

I have recently become aware of the extent to which the more ambitious (generally female baby-boomer academic) proponents of "deconstruction" intend to carry their philosophy. I was, in conversation with one such, discussing the (well-known to RISKS readers) propensity of the press to garble matters with a

scientific content.

I mentioned a recent article in the New Republic on the future of energy, in which hydrogen was mentioned as a possible energy source, pointing out its plentiful "supply" in the world's oceans. (This is a common confusion with the attractiveness of hydrogen as a _fuel_ for vehicles. Most readers will understand that the second law of thermodynamics prevents the use of hydrogen extracted from water as an energy _source_, since combustion restores it to a component of water.)

I remarked that the part of the article that had most irritated me was the admission that there were "technical problems" with the use of hydrogen as an energy source, with a qualifier to the effect that "scientists are always saying things are impossible and then finding out how to do them in the long run". (another common misconception)

The female baby boomer academic in question responded that this was indeed the case, and that "you scientists are so attached to your orthodoxies". Yes, the law of entropy, folks, is not an enigma, not a strange but inevitable feature of the fabric of the universe, nor an excellent approximation to reality whose limits have yet to be discovered. It is a dogma, if the deconstructionists are to be believed. What is more (here in the interests of preserving our friendship the conversation had to be dropped) it is no more or less true than "any other myth".

My guess is that had the conversation continued, the second law would be denounced as sexist, since it had been promulgated almost exclusively by wealthy or at least bourgeois white males. I have since discovered that there is a literature of the "deconstruction" of science, which generally shows little understanding of the pursuit of knowledge through rigourous thought, and claims to deny the _existence_ of truth in an extravagantly radical way.

I looked up "physics" in the index of one "deconstruction of science" book, since skimming the book showed so little attention to what is usually considered to be the scientific enterprise. Sure enough, there was one such reference. From memory, it said something like "The principal effect of the beginnings of physics was to blur the boundaries between the aristocracy and the serfs, since aristocrats found themselves doing manual labor." This was the first reference to physics in the book. An effect, perhaps. The _principal_ effect???

There are many people who 1) are in positions of some power and influence at universities 2) believe that there is no "truth" other than a matter of "preference" and 3) that all discourse, whatever its explicit content, is implicitly about the relations between the privileged and the oppressed. That such people are the ones enforcing "political correctness" is not surprising.

The connection to the typical subject matter of this group is somewhat remote. Mr. Nilges' comments are only an example of the broad problem, which should not be underestimated, particularly by those of us with a broad sympathy with most of the aims of feminism. I think the aspect that the readership of RISKS should be concerned about is the amazing ignorance of what it is we scientific/technological types do, among intelligent literate people, that allows it to be construed as just another branch of politics.

I hope, with their moderators' permission, to continue this discussion in soc.feminism .

Michael Tobis tobis@meteor.wisc.edu

Re: Formalism versus Experimentation

<Bob_Frankston@world.std.com>
June 12, 1991 7:35 pm EDT

There are two unrelated discussions here.

The first starts with the proposition that computer programming requires a certain skill set and considers the social impact arising from that premise. An interesting topic but not limited to the risks of technology except as one of the (primary?) forces of social change.

We should also examine the proposition itself. One way programming (by any of its varied names and approaches) differs from other engineering disciplines is that it is very malleable and even self-redefining. The original higher level programming languages, automatic programming (Fortran), were intended to allow mathematicians to get direct access to the computer. Later SPSS gave psychologists statistics to revel in.

With PCs (Personal Computer, not Political Correctness and not just IBM PCs) the goal is to empower the "end user" to control the systems. In effect, program the systems in a way that makes sense to that user. Of course a term like "end user" becomes inappropriate when others benefit from the automation (scripting, programming, whatever term you'd like).

To go back to Geraint Jones' bridge building analogy, some of us produce bridge building kits. Others, having faith that the kits will assure the bridges will not fall down, concentrate on the aesthetic or political or whatever aspects are appropriate.

The fundamental fallacy in a "pure logic" approach to programming is that it doesn't scale and deal with complexity. Chemical engineering is not just quantum mechanics with a few more numbers.

Formalism and Experimentalism

<anasaz!qip!john@asuvax.eas.asu.edu>
Wed, 12 Jun 91 22:29:31 -0700

I want to offer a viewpoint on formalism in computer education from the commercial world. I have worked as a programmer, designer and manager for 25 years. After a while in the profession, I went back to school and studied formal methods along with the rest of the computer science curriculum, so I have some insight on both sides of this this.

I find the assertion that formal proofs and other formalisms should be required subjects for programmers and system designers to be ludicrous. Anyone who has worked on a real-world, complex system knows that formal proofs are rarely possible. In fact, it is hard to even find a statement of work or a specification that is complete - much less provable.

Likewise, there are few people who end up writing compilers for a living, yet computer science curricula require courses in formal grammars. Why? It may weed out a number of good system designers who are not mathematicians, but will only be used by a very few students.

In hiring programmers and designers, I have found some correlation between basic computer science education and the ability to perform good work. I have found almost none between mathematical ability (as distinct from logical reasoning ability) and programming or design skills.

I concede that there are a few cases where formal methods are required. for example: research, robotics, super-critical real world control systems (in those few cases where they can be simplified and specified), VMM kernels, database systems internals and compilers.

I would argue, however, that the vast majority of those in the profession will never need or have an opportunity to employ those methods. It is an economic and human waste to require this material of everyone in the profession.

Re: The impact of formalism on Computer Science education

David Murphy <dvjm@dcs.glasgow.ac.uk>
Thu, 13 Jun 91 11:05:56 BST

I'd like to add my tuppence to the current religious wars in RISKS on Formalism in CS education. It's hard to know where CS is going, as it has only been around as a discipline for half a century or so; let us instead, then, translate the debate to an older science -- Physics.

The anti-formalists say: women tend to prefer experimentation and teamwork to solitary abstract thought. Hence we should cut the theory out of Physics to widen its franchise; there are plenty of people who `could' be professors of physics without knowing any theory if only we would let them.

The formalists say: Physics is an inherently mathematics discipline; a good understanding of it requires abstract mathematical thought.

Seen in these terms, the debate becomes less polarised; Physics is inherently mathematical -- you can remove some of the mathematics, but not without removing some of the Physics. It is also inherently experimental -- theoreticians need experimenters and vice versa. It is my belief that CS will eventually mature into this kind of subject; experimenters build things, using previously developed theory. Their constructions either call for a new theory (infrequently -- paradigm changes are rare in a mature subject) or support the old one. Just as no engineer would think of building anything but the simplest bridge without using the theory of statics, so no software engineer will think

about building anything but the simplest program without using the theory of program development. That doesn't mean that all software engineers will need to understand categorical logic, but it does mean that they will all want to use the products of theory; because they can build better, safer programs that way.

Re: Political Correctness in Computer Science

Paul Andrew Olson <PAOlson@DOCKMASTER.NCSC.MIL>
Thu, 13 Jun 91 09:38 EDT

Re Ed Nilges posting on PC vs. formal training,

I became a Computer Science major at Columbia University only just after it became the popular thing to be. Classes that had held 25 people ballooned to 125 in a single semester. The number of available terminals did not keep pace with the demand, so I found myself in much the same position as Mr. Nilges' Russian students. Since computer time was available only late, on weekends, after an indeterminate waiting period (I hate waiting), I learned early to rigorously design, code, hand-simulate, and re-code. I found this way I could type in and finish my assignments in relatively few compiles, rather than having to come back repeatedly, as my fellows were doing. I readily admit it was hard work, but it was harder work if I didn't do it. It is an already-old but true cliche that 'the sooner you begin coding, the longer programming will take'. Dijkstra is to be commended for trying to get the curriculum to reflect this.

The astute will notice that I am arguing for more Formalism, based on Experience:-)

I believe Nilges is also correct regarding the RISKs of political correctness. In academia today, accusations of being racist, sexist, elitist, etc. are freely tossed about, expressly for political ends. For an excellent reference on this phenomenon, read "Illiberal Education" by D'Nesh D'Souza. D'Souza is Indian by birth, so University presidents and professors felt comfortable admitting to him how disciplenary action, mob rule, and sophistry are used to suppress free speech, limit academic freedom, and politicize the curriculum. The news is bad, and the RISKs go a lot farther than computer science.

Re: Formalism versus Experimentation

Ian Brown <creare!inb@dartvax.dartmouth.edu>
Thu 13 Jun 1991 10:02:48 EDT

Eric Postpischil writes in RISKS 11.88:

> [assuming women prefer experimentation/teamwork], is not the proper question to ask "Which method of teaching women is best for their learning?" rather than "Which method of teaching women most addresses women's preferences?". That is, even if we assume experimentation and teamwork is best for women, this does not necessarily mean teaching with experimentation and teamwork will

> produce better women computer scientists than would teaching with formalism.

While the question is probably reasonable, I think that you will find that a significant number of people (both men and women) will learn better (not only prefer) using experimentation and teamwork. Using myself as a case in point; I have only taken a couple of courses (one of which I completed, an introduction to AI) in Computer Science. The way I learned most of my programming skills (and I think that most people would say that I am, at least, a competent programmer) was through hands-on work.

I think the real risk here is that people are going under the assumption that there is *one* best way to teach, whether the subject be Computer Science, or anything else. The problem with this is that different people learn in different ways; you are trying to force a square peg into a round hole - you may succeed, but the fit will not be very good.

The goal should be to produce as many good programmers as we can; don't exclude someone or force them to be less efficient by selecting a single method of teaching.

Re: 11.86 -- Political Correctness (cont'd)

Michael Barnett <mbarnett@cs.utexas.edu>
Thu, 13 Jun 91 09:48:49 CDT

In RISKS-11.86, Ed Nilges discussed Karen Frankel's article in the Nov. 1990 CACM. I also was bothered by the comments of Danielle Bernstein. Although there are some faculty members here at the University of Texas at Austin that try to teach in a more rigorous manner, the undergraduate curriculum here is based mainly on programming. From my perspective as a graduate student and teaching assistant, it is precisely this approach which puts the women students at a disadvantage. Generally it seems it is the male students who have more experience playing with computers and benefit from the "kick it 'till it prints out the right answer" mentality. A more Dijkstra-esque approach in the curriculum would provide a "level playing field", an environment equally new to both genders.

I have been told by female students that they are often intimidated by the men when working in the sort of group projects advocated by Bernstein. Being less comfortable with rushing into coding and the consequent late-night debugging sessions our students have been taught as the essence of computing (sigh), they are often pushed to the periphery of the group activities.

Having said this, I would not like this thread to become part of an attack on those who criticize computing and science in general for providing an inhospitable environment towards groups that have been excluded. For a general critique of the current movement against "political correctness", I recommend Alexander Cockburn's article in The Nation, May 27, 1991.

Michael Barnett (mbarnett@cs.utexas.edu)

Search RISKS using swish-e

Report problems with the web pages to the maintainer

Search RISKS using swish-e

THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

ACM Committee on Computers and Public Policy, Peter G. Neumann, moderator

Volume 11: Issue 90

Thursday 13 June 1991

Contents

Formal-dehyde and Exper-topinion

"Peter G. Neumann" <neumann@csl.sri.com>
Thu, 13 Jun 91 13:43:30 PDT

OK, gang, it seemed to be a reasonable bet that Ed Nilges' message in RISKS-11.86 would start a lively discussion. But it was rather less constructive than I had hoped, and many of you missed the bigger picture. Well, now we are starting to run off into all sorts of tangential directions. Thus, I hope that this issue and some other contributions that must be deferred to RISKS-11.91 because I try to hold issues smaller than the 32Kbytes (which is the limit for some of your mail systems) will be last of it for a while -- unless something incisive comes in from Edsger Dijkstra or Karen Frankel or Danielle Bernstein... And if you feel you must reply to this issue, please wait until you see RISKS-11.91, with a few more items on this subject. But let's stick to the basic issues, not to second- and third- and even fourth-order incrementals. Those tend to get tiresome quickly for most readers, and your moderator runs the risk of swinging from more-inclusive mode to more-exclusive mode... Thanks. P.

Re: Formalism versus Experimentation

Nancy Leveson <nancy@murphy.ICS.UCI.EDU>
Thu, 13 Jun 91 10:09:40 -0700

For some reason that I don't understand, an early draft of my message to Risks was sent instead of the one I spent two hours polishing (sigh). You'll have to take my word that it was great :-). Here is the final paragraph that was totally missing in the version printed:

I am most appalled at the implication in many of the messages that have appeared in Risks that in order to get more women into computer science, standards must be lowered. That is, they imply that the main reason why women are not participating is because they are not capable of logical and mathematical thinking and getting more women means that worse (and riskier) software will be produced. The reason for the low number of women in our field stems more from this type of prejudice than from any lesser ability. I have written about the extra barriers and difficulty that women face in becoming computer scientists. If you are interested, an article that appeared in the Newsletter of the Computing Research Association can be obtained via anonymous ftp from ics.uci.edu -- the article is in pub/nancy/snowbird (print using troff -ms). In this same directory, by the way, you will find a long (but incomplete) list of women PhD.s in Computer Science or Computer Engineering who are professors in Ph.D.-granting universities or in industrial research.

Women and computer science education

Paula M. Ferguson <paula@lta.lta.com>
Thu, 13 Jun 1991 14:16:04 -0400

I find it telling that all of the dialogue on this subject has been between men. Maybe that speaks to the fact that there aren't very many of us women in the field of computer science.

[Don't forget Nancy Leveson's item in RISKS-11.88!]

I have some strong ideas about this subject, having spent my senior year writing a thesis about issues of women and computer science education. Before you decide to dismiss my position as the ranting of a feminist, let me tell you a little bit about my background. I graduated last year from MIT with a B.S in computer science, so I'm not talking about this issue on an abstract level, but rather from personal experience as a woman in a computer science program. I did quite well in my "formal" programming courses and I am now working for a small software development company.

I think that it is fairly obvious that there is something about computer science that discourages women from entering the field. One place to look for discouraging forces is in the realm of computer science education. While the percentage of women at MIT is around 35%, the percentage of women in computer science is 22%. What is more interesting is that the enrollment of women in the introductory computer science course is around 30%. This class is the

first class that someone who is thinking of majoring in computer science would take. Is there something that about the course that causes women to decide not to major in computer science? I think so. This topic was the subject of my thesis, but I'm not going to go into it here, except to say that it has a lot to do with the course's emphasis on abstract, logical reasoning. I was a lab assistant for the course for two years, so my conclusions are based on extensive observation of students taking the course.

I am not advocating the elimination of training in formal logic from the computer science curriculum. I think that computer scientists need a background in this area. Structured programming is necessary for large programming projects, to manage complexity, reduce the potential for errors, and help in all of the other ways that it does. However, I don't think that training in formal mathematics and logic should be the only training for computer scientists. It also should not be the first subject in a computer science program. The field of computer science is much more than just structured programming. There is room for a lot more creativity than is allowed by formal logic. After taking the introductory computer science course at MIT, I decided not to major in computer science because I didn't enjoy formal programming. I thought that structured programming was all that people with computer science degrees did. After a year and a half of electrical engineering courses, I changed my major to computer science and discovered that there is a lot more to the field than I originally thought.

One problem with the almost universal focus on logic and abstract reasoning in computer science education is that it affects all levels of computer education. Programming courses in high school demand that students use structured methods. Even courses in Logo for grade school kids emphasize procedures and abstraction. It hardly seems necessary to start training kids how to write "correct" programs at that age. One of the reasons that there are so few women in college computer science programs is not that they are turned off to computers in college, but that they are turned off to computers at a much earlier age.

There is a lot of evidence from psychology and sociology that supports the idea that women and men have different cognitive styles. Our society and its educational system values abstract, logical thinking, which is typically the male domain. Women's styles of thinking are seen as inferior. I haven't read Frankel's article in CACM so I don't know if Ed Nilges' paraphrasing is accurate:

> mathematics on logic.) Nye, and apparently Bernstein, believe that solitary
> abstract thinking is a typically male activity and to force women to engage in
> it is sexist.

Forcing women to think abstractly isn't sexist. If Bernstein calls it sexist, it is unfortunate. However, setting up a system that values the male style of thinking and devalues the female style is sexist. These values create a roadblock that women have to overcome to succeed in the male-defined and dominated world of computer science. Faced with these barriers, all but the most determined women will give up at some point, either in grade school, in college, or at the professional level.

There is little room for creativity in a world that is ruled by formal logic.

A number of areas of computer science have have benefitted greatly from creativity that probably never would have happened within the constraints of abstract thinking. Two areas that come to mind are artificial intelligence and user-interface design. The argument, raised by Eric Postpischil, that women need to be taught in the way that is best for them, not in a way that they are comfortable with, assumes that "best" can be defined universally. Teaching everyone formal logic may teach people how to write more "correct" programs with fewer bugs, but it won't help anyone write innovative programs. If creative people are discouraged by the formal, abstract nature of computer science, it will only be to the detriment of the field in the end.

Eric Florack asks:

> even-handedness amongst the sexes, I question your conclusions.. Do we attempt
> to change laws of chemestry and electricity because of a particular group of
> students' inability to learn the laws as they are? IE: do we attempt to change
> reality to aid some people's ability to deal with it effectively? Why, then do
> you conclude that to learn computer logic, one need not learn logic, first? Is
> it simply because of one 'minority' or another's inability to deal with that
progression?

First of all, computer science isn't a science like chemistry, it is an engineering discipline. There are no "laws" of computer science. And secondly, if scientists had always blindly obeyed the laws as they knew them, we wouldn't have things like the theory of relativity, quantum mechanics, or chaos theory.

Eric goes on to say:

> It is the retreat from the more formal, (and yes, harsher) learning
> environments, the 'massive dose of new ideas' that have placed this country
> into the educational crisis it's in today, where nearly 50% of high school
> students cannot read effectively. In the 'marginalized groups' as you put it,
> these percentages are even higher... we expect less of them, so they produce
> less. What you suggest is more of the same.

I disagree completely. Educational techniques have changed very little in the past century while the world has changed considerably. The educational crisis is the result of this disparity. Kids don't feel like their teachers are teaching them anything worth learning, so they don't learn. Until education is made relevant to kids' lives, the crisis won't go away. 'Marginalized groups' suffer the most from this problem. Until education is truly multicultural, these groups will continue to be marginal. When kids get the message that they are not valued, they are going to act accordingly.

In the same way, most women are going to avoid computer science until the computer world begins to value their style of thinking and the contribution that they could make. And some women in the field will continue to feel isolated by their difference.

Paula M. Ferguson, Lewis, Trachtenberg & Associates (LTA) +1 617 225 0366

Formalism vs. Experimentation (RISKS-11.86 [,87,88])

Mary Shafer <shafer@skipper.dfrf.nasa.gov>
Thu, 13 Jun 91 12:31:58 PDT

Based on the co-ops and young engineers/programmers that I've worked with, the current methods of teaching programming don't work, whether based on formalism or problem solving philosophies.

Being able to write little programs, no matter how elegantly, is no introduction to reality, which seems to consist most frequently of modifying sections of existing (and frequently ugly) code.

Debugging is also a topic that should be dealt with in more depth.

Mary Shafer ames!skipper.dfrf.nasa.gov!shafer
NASA Ames Dryden Flight Research Facility, Edwards, CA

---

re: Formalism, new twists

Leslie DeGroff <DEGROFF@INTELLICORP.COM>
Wed, 12 Jun 91 17:09:19 PDT

Reading the replies and having watched some previous...What and How to teach computer science discussions, I have a couple bits that might be worthy of attention as we contemplate. Fundamental before we even get to the politics of men/women is the question of what gets taught, why and how is it used... from late 70's till recently there seemed an unfillable demand in America for programmers (and related software skills, software engineers, documenters that understood software, analysts...) This void sucked up almost anyone who could and wanted to do this kind of work...spectrum from starting with a single computer course to PHD's of many flavors.... Coming to today, the demand seems to be slackening but not so much so that we can set up the academic training system so that only .1 percent of the mathematically gifted can past... A useful analogy for education and professional life is that of an adjustable filter, besides shaping people it filters. As a filter, some people get rejected, thats how it works, but the adjustability of the academic part of it is loosly coupled to job market requirements. I say loosely coupled because some CS education programs with quite high formal contents are relatively weak on critical job related skills like test design, requirement and user oriented design that are needed to build real world systems. To make an exaggerated example, the formal analysis of a computation problem will not help if the engineer puts in no input checking to insure that the input is a number. (sorry to say, I've seen that bad, defended as performance requirements)
Similar loose coupling is common in all engineering fields, there are risks in at least two directions, the curiculum gets so formal and remote as to not be useful to the profession or it gets watered down and too many graduates are release unable to perform the work. This and many other curriculum and accreditation discussion are a necessary part of the eternal vigilance of professions and so should be frequently discussed.
Personally I think the roots of the argument are such that the solution is that nobody wins... I don't believe that the formalists want or imagine

computer science in the US to be 95% mathematics with no computers or that the other side wants no logic or mathematics, they are discussing in an exaggerated way the balance point.

Changing directions from whats the arg and why nobody should win, I'd like to pick up the thread about various styles as stereotyped by nationality; there do seem to be important differences in working style fostered by different cultures and education systems and in my experience this is stronger than sexual differences... The hardworking diligent precise asian, the theoretical indian, the hacker american are dangerous stereotypes with some base of observable truth, and out in industry they have strengths and weaknesses, it seems that with in a curriculum for computer science overburdened as it is that there is a need the project management, working as teams foci and this useful set of skills if present in several of the programming language and software engineering courses of a program would make them easier and more attractive to certain personality types with certain slightly different skills than the current approaches. I would not leave this in the realm of man/woman, in the company I work for it's marketing/technical and technical/management/production operations were the problems of approach become crisis.

Re: Formalism versus Experimentation (Brown, RISKS-11.89)

Mart Molle <mart@csri.toronto.edu>
Thu, 13 Jun 91 14:10:23 EDT

>The goal should be to produce as many good programmers as we can; don't
>exclude someone or force them to be less efficient by selecting a single
>method of teaching.

This is the wrong goal! Taken to an extreme, we may as well give typewriters to monkeys and try to pick out the literary works. It would be a mistake to try to increase the production of good programmers (or bridge builders, or Chevys...) by adopting new methods of training if those other methods increase the risk of producing bad programs (or unsafe bridges, or defective Chevys). Although I know a number of excellent, self-taught programmers, on the whole I have found that people with formal training tend to write more reliable and maintainable programs.

Mart L. Molle

Re: Formalism versus Experimentation (Franston, RISKS-11.89)

Rick Smith <smith@SCTC.COM>
Thu, 13 Jun 91 13:11:20 CDT

>To go back to Geraint Jones' bridge building analogy, some of us produce
>bridge building kits. Others, having faith that the kits will assure the
>bridges will not fall down, concentrate on the aesthetic or political or
>whatever aspects are appropriate.

I thought that the point of the bridge-building analogy was that there's no such thing as a "bridge building kit." Sure, you can buy prebuilt trusses and

assemble them, but the assembly is supervised or at least reviewed after completion by a civil engineer. The construction of reliable software needs the attention of a professional. You don't guarantee the correctness of your solution just by using a "kit" in the form of some higher level language.

In the same vein, using SPSS doesn't guarantee the correctness of one's statistical efforts. The user needs to apply formal techniques to assure the validity of the sample population and that the statistical techniques being used are appropriate for analyzing the sample.

Well, actually I do know of a class of things called "bridge building kits" but they are generally sold in toy stores. I think this has an apt analogy with software development, too. The unpracticed eye really can't tell the difference between prototype software that tries to simulate a problem solution and software that really implements a problem solution. Bridge building with Lego blocks can be a complex and even satisfying endeavor, but it's just not the same as building one to carry real traffic.

Rick Smith, SCTC, Arden Hills, Minnesota.

Formalism versus Experimentation

Michael L Muth <rzw3484@dcrs.dla.mil>
Thu Jun 13 13:03:27 1991

I have read with interest, and considerable dismay, the recent discussion generated by Danielle Bernstein's comments on Dijkstra's call for reform in computer science education. Dismay because most (but not all) of the postings reflect an underlying assumption that women are innately incapable of mastering logic and mathematics. It seems that even Bernstein makes this assumption.

Aw, come on folks! The only reason men seem to out-perform women in these areas is that we are conditioned to it. The conditioning begins in grade school. Teachers assume that boys will be better at math than girls. Girls are dissuaded from pursuing higher math, logic, and technical subjects. Both teachers and parents are to blame here. Since women still comprise the larger group of educators, this seems to indicate that women themselves are doing their part to perpetuate the problem.

My daughter received a pretty fair dose of this conditioning. As a result, she struggled with math. I embarked on a protracted de-programming effort. Largely because she is now free of this nonsense, she is on track to take the Calculus AP exam during her Junior year in High School.

Relaxing computer science curricula will not fix this problem (We would only be addressing the symptoms). On the other hand, I would not want to rely on software written by a less rigorously trained programmer. Let's fix the problem, not the symptoms.

****

Let me shift to a closely related problem I see (which has also been reflected in this ongoing discussion). Why do we assume programming has to be some kind of solitary (lonely?) activity? Why do our schools teach programming as an INDIVIDUAL activity? (A local university not only does not teach team effort but FAILS or EXPELS students who work together!)

Failure to teach software design and development (SDD) as a team activity already costs all of us. Major software projects are usually (and should be) team projects. But, because team members have been conditioned to solitary effort, these projects suffer from personality and software integration problems. Students hear of "ego-less programming" but never practice it. How much have firms like Lotus, Ashton-Tate, and Microsoft suffered from this problem? How much of your tax dollar is spent on protracted debugging and retesting of government projects? As a former government QA specialist for computer software, I can tell you that the cost to taxpayers is more than it should be.

Why can't our universities require successful completion of a team programming class for a CS degree. Graduate students would participate as team and project leaders while undergraduates would make up the teams. Student grades would be based upon individual, team and project accomplishments. After a few days discussion of team programming and possibly some team building exercises, the instructor would hand the students a specification and stand back. The class would be expected to develop the software and provide draft documentation.

Mike Muth -- mmuth@dcrs.dla.mil

Re: Formalism vs. Experimentation (RISKS-11.86 [,87,88])

Brinton Cooper <abc@BRL.MIL>
Thu, 13 Jun 91 14:20:24 EDT

The RISKs of this discussion are:

1. that it will degenerate into quibbling over the respective attributes and capabilities of men and women and

2. that some of our readers will actually begin to believe that women are more (or less) logical than men and less (or more) effective in working in groups.

It is incredibly unfortunate that sexist issues ever saw the light of day in CACM., RISKS, or any other credible forum. We have serious issues confronting us and need the talents of any men, women, and others who can contribute to the solutions. Research is inconclusive as to whether (elementary age) boys learn math better than girls. We certainly have no scientific basis to argue whether women are more or less effective as computer designers.

I don't know whether we should have more or less rigor in CS education. I believe, however, that whatever the answer, we must assume that it applies equally to men and women.

_Brint

Re: Formalism versus Experimentation (RISKS-11.88)

Ed Nilges <egnilges@phoenix.princeton.edu>
13 Jun 91 18:53:33 GMT

Tim Shimeall asks:

>Isn't there a need to differentiate programmers by background and
>ability, particularly in development of life-critical systems?

But a two-tier (or even n-tier) class structure in programming could be as sexist, classist and racist as excluding out-groups in the first place. Even more, as people are lured into the field, given sub-standard training, and then face a lifetime of frustration and glass ceilings.

Furthermore, differentiation of programming problems into Serious and Not Serious is a rhetorical trick that conceals as well as reveals. Business problems are commonly regarded by computer science students and professors as Not Serious Enough, yet Dijkstra and others have commented on the difficulty of these problems: as Dijkstra writes,

> "The problems of business administration in general and data base management in particular are much too difficult for people that think in IBMerese, compounded with sloppy English."

Also, software reuse implies that a programmer may be working on code she thinks not mission-critical, only to have the code be picked up in a mission-critical system at a later time (is a compiler not life-critical? what if I use it to compile something that is life-critical?)

Jean-Francois writes (and I apologize for not being able to spell his name with proper accents):

>The discussion revolves around straightening the three following inconsistent
>propositions:
>
>1 Abstract logic is necessary to the computer industry
>2 Logic is not compatible with women

> Good heavens, nobody is making this claim...sounds like something Jean-Louis Gassee would say on a bad day. For one thing, it's a type conflict of the first order.

>Most of them have *at best* a knowledge of conversational english, yet they
>have to access to hard technical literature. Those who are not proficient
>enough or cannot adapt are definitely weeded out. You can find this perfectly

>normal or unacceptable depending on how much you think cultural imperialism is
>relevant to computer education.

Cultural imperialism is VERY relevant. Algol lost out to Fortran in part because of imperialism: Algol was superior to Fortran but the United States could not concede that the Europeans had the lead in programming languages.

But I think you'd concede readily enough that it would be a DISSERVICE to French people and other non-English speakers to avoid requirements that they learn English as part of the preparation for a technical career. But this is exactly what Ms. Bernstein wants CS departments to do for women.

Political Correctness: DON'T PANIC!

Glen Ditchfield <gjditchfield@watmsg.waterloo.edu>
Thu, 13 Jun 91 15:33:46 -0400

I think that many of the people discussing this topic are reacting to other people's interpretations of Bernstein's ideas, rather than to what the CACM article of November 1990 actually says. For instance,

> Ed Nilges: "Bernstein, according to Frankel, feels that Dijkstra is being sexist!"
> Hal Pomeranz: "It is unfortunate that Bernstein slings the word 'sexist'..."
> Michael Tobis: "It is more than 'unfortunate' that the word 'sexist' is used .... The problem is that the issue is being attacked _on the grounds_ of its social/political appropriateness ..."

My bet is that if we all went back and read the CACM article, the discussion would be shorter and calmer, and our Moderator would be happier.

Frenkel discusses Bernstein's ideas in six paragraphs of an eleven page article. No one ever calls Dijkstra "sexist"; Bernstein believes that Dijkstra's curriculum would cause disproportionate numbers of women to drop out, but that is not the same as an accusation of sexism. Bernstein does not call for the removal of formalism from computer science curriculums; she just wants an introductory CS course, based on the use of software packages as problem-solving tools, that would help to get women hooked early.

Frenkel's interpretation of Bernstein's opinion of Dijkstra's proposal comes down to two sentences:

> Bernstein disagrees with this approach because it would discourage those who want to "see, tinker, experiment, and interact" with computers in order to understand principles. And so, she says, Dijkstra's approach would cause computer science majors to further dwindle.

To me, "those who want to 'see, tinker, experiment, and interact'" sounds a lot like "hackers", who are stereotypically male. And note that the last sentence does not say _women_ CS majors. Given earlier statistics and later comments in the article, I think she is worried about the total number of CS majors.

Of course, all of the above is just my reading of the article. Please read it and form your own opinions.

Glen Ditchfield gjditchfield@violet.uwaterloo.ca Office: DC 2517 x3437
Dept. of Computer Science, U of Waterloo, Waterloo, Ontario, Canada, N2L 3G1

Search RISKS using swish-e

THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

ACM Committee on Computers and Public Policy, Peter G. Neumann, moderator

Volume 11: Issue 91

Thursday 13 June 1991

Contents

Another answering machine risk?

Dave Brower, UNIX Group, [415] 748-3418 <daveb@ingres.com>
Thu, 13 Jun 91 08:38:32 PDT

[From the 6/13/91 SF Chronicle]

> LEAVE A MESAGE AT THE TONE: Either a disgruntled employee or a disgusted fan somehow changed the telephone message at the Minnesota Viking's offices recently. Instead of the regular message, callers hears this: ``Thank you for calling the most rotten, stinking team in the history of man. that's right, you have reached the Minnesota Vikings.''

The possibilities of hacking answering machines/voice mail have been beaten to death in RISKS several times before. This one may be a good exemplary tale to spread around showing the pitfalls of undersecured systems.

Dave Brower

Fraud aided by insider

Steve Smaha <Smaha@DOCKMASTER.NCSC.MIL>
Thu, 13 Jun 91 17:08 EDT

From the 13 Jun 91 Austin American-Statesman, staff report:

"Son testifies against father in insurance case"

The son of a Houston insurance fraud defendant told jurors Wednesday that he installed a command in a computer system that would delete traces of an investment plan created by his father. Bud Skillern, 56, former financial consultant to the insolvent American Teachers Life Insurance Co., has pleaded innocent to accusations that he stole funds from an investment plan involving the firm.

Tuesday, witnesses outlined Skillern's plan, which used ATL to sell $100,000 single-premium annuities. [...]

Prosecutors spent Tuesday questioning witnesses to try to show that Skillern's method of having buyers acquire the annuities through promissory notes - simple IOUs - is highly questionable, because annuities normally are bought with cash.

On Wednesday, Skillern's son, 24-year-old Michael Don Skillern, testified that he was in charge of programming computers at ATL to make calculations required by the investment plan. The son told jurors that he built a command into the program that would delete all traces of the plan in the computer system. "The idea was that if (State Board of Insurance) examiners came into American Teachers Life, it would not look good for General Mercantile to be doing business out of American Teachers (office). So I installed an erase feature," said the younger Skillern. He also said that General Mercantile Finance Corp. - a company owned by his father - was supposed to lend money to the annuity buyers. [...]

In the grand jury indictment of Bud Skillern, it is alleged that Skillern sold the $100,000 annuities to Premier [Bank of Dallas] after he assured the bank officials that ATL had been fully paid for the annuities. [...]

Failure to Manage Risks Can Reduce Claim

Patrick Wolfe <pwolfe@kailand.kai.com>
Thu, 13 Jun 1991 13:00:00 CDT

The following paragraphs are extracted from the article "Contingency Planning - The Failure to Manage Risks Can Reduce Claim" by J.T. Westermeier which appears

in "Computer Law Strategist" Volume VIII, Number 1 - May 1991, published by Leader Publications, New York, NY. Considering the performance of our local electric utility company, I found the limitation on liability interesting.

The recent ruling by the Minnesota Court of Appeals in "Computer Tool & Engineering Inc. v. Northern States Power Co.", underscores the importance of managing effectively the problems that may arise in the operation of a computer system and represents an important lesson in contingency planning and risk management.

Computer Tool & Engineering Inc. had its computer system damaged seriously as a result of a power surge. To recover for those damages, the company brought a lawsuit against two parties, its electric utility company, Northern States Power Co. and its telephone company, the United Telephone Company of Minnesota. The telephone company's liability arose from its conduct when it was engaged in placing underground telephone cables. During the installation of the telephone lines, the telephone company severed a primary feeder cable and a secondary cable of the power company, which caused a power surge to travel through the power company's cable, damaging Computer Tool's computer equipment.

The Court of Appeals affirmed the trial court's ruling denying any liability by the power company on the grounds that the limitation on liability granted to the power company in its rate tariff protected it against damages resulting from interruptions in power.

At the jury trial of the negligence claims against the telephone company for the damages resulting from it's cutting the power company's cables, under Minnesota's comparative fault statute, the jury assessed 85 percent of the fault to the telephone company for severing the cables in question, and 15 percent against Computer Tool for failing to install surge protection equipment. The evidence at trial showed that Computer Tool had experienced power surges in the past, and, that it did not use surge protection equipment even though it knew such equipment was available at a relatively low cost.

"If the probability of an injury-causing event be called "P"; the injury "L"; and the burden of adequate precautions "B"; liability depends upon whether B is less than L multiplied by P; i.e., whether B<PL."

Because this B<PL formulation serves as a tool for analyzing risks, it was applied in essence in the Computer Tool case, and can be applied to computer system risks other than power surges.

Liability can be imposed where management knew or should have known what to do, but failed to act, as in Computer Tool.

Patrick Wolfe (pwolfe@kai.com, uunet!kailand!pwolfe)
System Programmer, Kuck & Associates

"Risks of getting caught" (Wright , RISKS-11.87)

<Anonymous>
Thu, 13 Jun 91 11:52:52 xxx

Ed Wright writes that he is "often intrigued by people apparently worrying about the risk of 'getting caught.'"

Ed, because of the ways that laws are made in the society in which we live, there are ethical behaviors which an individual may choose that, for whatever reasons, happen to be illegal.

It is sometimes in the interest of individuals who engage in these ethical behaviors (1) to fix those laws, and (2) in the meantime, to prevent authorities from becoming aware of those activities.

The issue being raised is the government tracking and control of activities which, ethically, are the choice of the individual. It is unethical for the government to interfere with or control that particular class of activity (ethical but illegal), yet they attempt to do so nonetheless.

I think that the concern brought to RISKS was the effect of new technologies on the government's ability to carry out such unethical behavior. When a new technology makes such unethical government behavior easier, faster, or more cost-effective, it should be no surprise that educated people would worry about the increased risk of "getting caught."

Fiction is truer than fact? (Re: RISKS-11.88)

Grant Hogarth <cgh@frame.com>
Wed, 12 Jun 91 12:53:36 PDT

Two (admittedly fictional) texts which touch on issues discussed in Risks 11.88:

Peter G. Neumann (neumann@csl.sri.com) talks about a pre-programmed [or common-mode embedded hardware] systematic failure point.

> In his book _The Stone Dogs_, SM Sterling uses exactly this device (implemented, as I recall, by a viral mechanism), as a weapon to simultaneously disable all of the "bad guys" computing systems. (A similar technique, based in biology, is used by the baddies against the "good guys".)

Lauren Weinstein (lauren@vortex.com) discusses the interlinking of databases and caller ID.

> There is a short story by Robert A. Heinlein titled "We Also Walk Dogs" (Anthologized, I believe, in _Waldo and Co._) that shows a "positive" use of such a database by a commercial company. It's a little idealistic, but does demonstrate some of the issue raised by his article.

Fear of Censorship

"Peter G. Neumann" <neumann@csl.sri.com>

Wed, 12 Jun 91 14:42:30 PDT

An article contained two incidents that I do not recall previously appearing in RISKS. Excerpts follow.

FINANCIAL UPDATE Data base users fear censorship
By Frank Green, Copley News Service, 12 June 1991?

[...] Consider these recent showdowns on the fiber-optic web:

* Internet, a computer network connecting thousands of scientists and researchers worldwide, kicked two users off the system after they transmitted digital images of Playboy centerfolds, as well as some hard-core pornography. [well, Internet is not a system...]

* A dozen customers on the Prodigy network, owned by Sears and IBM, were kicked off the system by the company for a few weeks after they complained on-line about a planned increase in user fees.

* Bowing to 30,000 consumer complaints, Lotus Development Corp. and Equifax Inc. in January jettisoned a computer program with data on 120 million American households. The program contained the names, addresses, marital status and estimated income of consumers. [old stuff]

RIGHTS IN CYBERSPACE

These cases raise intriguing legal and constitutional questions:

* Did Prodigy and Internet violate computer users' First Amendment rights to freedom of speech?

* Can the National Security Agency legally intercept computer messages transmitted in the United States and beyond?

* Does a computer user in Austin, Texas, have the right to "talk" to a friend in Tel Aviv about Iraqi missiles landing in Israel, thus breaching both U.S. and Israeli security?

"Constitutional protections have not been adequately extended to digital media and digital technologies," said Mike Godwin, staff counsel of the Washington-based Electronics Frontier Foundation, a new lobbying group.

Harvard law professor Laurence Tribe has gone so far as to propose a 27th amendment, shielding travelers on the computer highways from government or corporate invasions of their privacy while guaranteeing their freedom of speech. [old stuff for RISKS]

Others, however, consider this unnecessary. "All the protections we need currently exist," said Marc Rotenberg, director of Computer Professionals for Social Responsibility, a Washington-based lobbying group that boasts 2,500 members. In his eyes, the principle at stake in the computer age is the unrestricted flow of information and the presumption that any government efforts to restrict it is impermissible. That doesn't mean that the government shouldn't have a policing role, Rotenberg said. Criminal activity conducted over computer networks such as the trafficking of stolen telephone-access codes would justify government intervention. So would threats to public safety, such

as the unleashing of a computer virus in the Pentagon's computer system.
"Trouble is, the law is always 10 to 20 years behind the technology, "
Rotenberg said. "Many mistakes are made, at great cost to people, before it
catches up." [...]

Caller ID -- The risks are already here. (Re: Weinstein, RISKS-11.88)

Jim Purtilo <purtilo@cs.UMD.EDU>
Wed, 12 Jun 91 14:29:50 -0400

Indeed they are. This technology has now *really* hit me where it hurts. One
of the better pizza joints near campus has decided not to deliver to campus any
more, save to "known good customers". They know they do not want to deliver to
you based upon the phone number you call from. I suppose the chief risk here
is in reduced quality of my software due to its production during a period of
low blood sugar.

Fortunately, the phone number for Vic Basili's secretary is on the "good" list,
since she has done most of the ordering for the "software engineering lunch
bunch" over the years. So even though I can't order a pepperoni 'za from my
office, I can get it any time I can sneak down the hall to Claire's office and
call from there ...

Jim

---

re: Caller Id -- The Risks are already here!

John (J.G.) Mainwaring <CRM312A@bnr.ca>
12 Jun 91 19:11:00 EDT

I found Lauren Weinstein's posting quite stirring. At least, it seems to be
stirring the pot a bit.

A call to an 800 number is in fact a collect call. A person (or company) has
at least a plausible argument that they should know who is calling, and have
the right to refuse calls from whomever they please. Most 800 numbers are
owned by businesses, which can be expected to make decisions on business
grounds. If their decisions are wrong, they will offend customers (or
potential customers), and their business may suffer. If they are the sort of
business that deserves to succeed, they will avoid bad policy or recognize it
and fix it.

If you really want to talk to someone who has an 800 number, and you don't like
the way they deal with the 800 number, you can always get their real telephone
number from directory assistance and pay for the call yourself.

It seems to me that the main risk created by Caller ID on 800 numbers is a
common risk created by new technology, namely the unlimited ability of some
people to make stupid or insensitive use of it. Still, they're mostly the same
people who were rude or insensitive before the new technology came along. We
can always hope that at least some of the companies using ANI on 800 numbers
will think of pleasant ways to use it, just as some companies have always been

more pleasant to deal with than others.

Re: Fighting phone hackers in SoCal (RISKS-11.87)

Ralph 'Hairy' Moonen <rmoonen@hvlpa.att.com>
Wed, 12 Jun 91 09:48 MDT

[account of female Clifford Stoll deleted]
->A non-negotiable condition of Bigley's out-of-court settlement provided that
->the guilty party relinquish his (or, infrequently, her) computer and modem.
->Thrifty Tel donates the confiscated weapons [computers] to law enforcement
->agencies.

Who the hell gives someone the right to blackmail alleged criminals into giving them their computers? (Did the article really say "weapons"??) I could understand a settlement being made on the terms of "pay up or face charges". This is actually quite normal. But to also include a term "...and I'll have your computer & modem too, please" is downright blackmail!!

However sure Bigley may be that she has proof that a certain individual commited a crime, she does not have the right to confiscate computer equipment. People are innocent untill *proven guilty by a court of law*... or not anymore? If the alleged criminal indeed has commited a crime, (s)he may well be tempted to go for the offer. In that case, the settlement should involve the paying of the financial losses that the company has suffered, AND NOT MORE.

Imagine someone stealing an apple (Thrifty only offered the settlement to *small* time crackers), and getting cought. The shop owner now says: "Pay for the apple, and I won't call the police" (acceptable) "... oh, and by the way, gimme your new leather jacket & wallet also, and we'll forget the whole thing" This in my opinion is unacceptable.

--Ralph Moonen

Re: Fighting phone hackers in SoCal

John R. Levine <johnl@iecc.cambridge.ma.us>
12 Jun 91 11:40:32 EDT (Wed)

John Higdon recently sent the Telecom digest a summary of a radio talk show in LA on which he appeared along with the head of Thrifty Tel. Thrifty is a most unusual phone company. They offer flat rate long distance service to any point in the USA for a fixed monthly charge. Their tariffs include a special multi-thousand dollar "hacker rate" that applies to anyone who uses their facilities other than through legitimate means. Their access is almost entirely through the obsolescent 950-XXXX access numbers, and their code numbers are apparently much shorter than anyone else's. It was clear from the presentation made by Thrifty's head that she is much more interested in punishing illegitimate phone use than in preventing it, since she had no interest at all in going to longer and harder to guess access codes nor in switching to the nearly hack-proof 10XXX equal access dialing. Her main

thrust was that these hackers have broken the law and should be punished.

Their dedication to obeying the law apparently does not deter them from completing intra-LATA calls via their 950 numbers, in violation of their own tariffs and of state law (as do most other long distance companies.) There are also reports which may or may not be true that Thrifty puts their access codes on pirate BBSes to encourage and entrap potential illegitimate users.

The risk here is a familiar one -- the tension between technical and political means of enforcing legitimate use of technology. I expect that few readers of Risks think that the legal prohibitions against listening to cellular telephone broadcasts keep many snoops from listening in. Similarly, you don't have to condone phone phreaking to think that a company that makes their facilities unusually easy to break into deserves what they get.

John Levine, johnl@iecc.cambridge.ma.us, {spdcc|ima|world}!iecc!johnl

---

Re: Formalism vs. Experimentation (RISKS-11.89)

Ed Nilges <egnilges@phoenix.princeton.edu>
13 Jun 91 19:41:58 GMT

> Dijkstra does not deal with large programs. [Leveson]

Actually, he does deal with large programs. The entire reason for his original CACM letter was the fact that while toy programs could be produced using go to and adhoc methods, some theory (such as the theory that any possible program could be written satisfactorily without go to) is needed to "scale up."

And I don't believe that YOU believe the first sentence in the above paragraph. What works in place of some person (or group) sitting back and thinking logically? Prayer? Transcendental meditation?

>I looked up "physics" in the index of one "deconstruction of science" [Tobis]

Michael, the very reason why spent 14 bucks on Andrea Nye's book Words and Power is because I am fascinated by such "deconstructions" of science. This does not mean, however, that I hew to any "politically correct" line that (for example) women's needs should always have precedence over the requirements of the field. Nonetheless, I found much to profit by in Nye's book, and I think that the notion that physics has some sort of genesis in a gentleman's need to distinguish his activity from that of the herd a fascinating and illuminating notion. This may be confusing: however, it is also a highly CRITICAL reading of critical theory and a theory which cannot stand self-application is undeserving of honor.

I find it interesting, have read my critical theory, that status and class anxieties blind people in programming to the realities of that field. Programming is like writing was to Plato in that it may empower the formerly silent, and this produces anxiety even in the formerly silent. Thus the need to differentiate Serious and Mission Critical software from Not Serious and Not Critical software, even when writers with the intelligence of Dijkstra have

pointed out the inability to computer science majors to write a simple match-merge problem for business (presumably a Not Serious application.)

It should also be noted that deconstruction, like Algol, is a European import and as such what you were subjected to may have been the product of the American mis-reading of deconstruction, based on the decline in standards at our universities that began in the Sixties. Derrida himself, one of the luminaries of the French school, has commented on how Americans misread him when he writes about notions like "free play" and the differing "semantic networks" around "jeu" versus "play".

>With PCs (Personal Computer, not Political Correctness ...) [Frankston]

...or puissance/connaissance, Foucault's power/knowledge represented by computer power...

>The fundamental fallacy in a "pure logic" approach to programming is that it
>doesn't scale and deal with complexity. Chemical engineering is not just
>quantum mechanics with a few more numbers.

> Computer programmers hate the idea of having to use formal methods. Formal methods have the air about them of being kept after school, since they essentially use the same symbolic notions as programming. However, training in formal methods enables you to use them informally...to produce, say, a cogent argument in natural language concerning a piece of code.

>I find the assertion that formal proofs and other formalisms should be
>required subjects for programmers and system designers to be ludicrous.
[anasaz!qip!john]

Richard Slomka wrote a book years ago, "No-Nonsense Management" which said that although you'll never get perfect numbers this is no excuse for not continually trying to improve your numbers. Training in formal methods produces programmers better able to produce INFORMAL (natural language) proofs and arguments about their code.

>Likewise, there are few people who end up writing compilers for a living, yet
>computer science curricula require courses in formal grammars. Why? [...]

Training in the development of compilers is excellent preparation for developing front-ends to business programs, and I am also reminded of the recent comp.risks article mentioning a reinsurance system that could not handle recursive cycles. As a consultant and programmer in that aforementioned real-world, I have encountered a number of disasters that could have been avoided if the original designers had been CS-literate:

* A Cobol program for telecom switch billing that had to simulate the switch in order to reconstruct calls from basic events such as off-hook. The original designers did not know anything about finite-state automata, around which the actual switch was built. The resultant program was for this reason a collection of pious hopes connected by

gotos which I rewrote in a few weeks...using finite state automata.

* A bill of materials processing program that, like the reinsurance program, did not use stacks and as such did not handle self-embedding parts (part A needs part B needs part C)

* IBM's "arbitrary character" hack in XEDIT, an editor for the mainframe VM/CMS operating system, which is "simpler than" regular expressions...and which is essentially unpredictable in common instances.

Formalism vs Experimentalism

A. Padgett Peterson <padgett%tccslr.dnet@uvs1.orl.mmc.com>
Thu, 13 Jun 91 16:01:56 -0400

1) Am not sure what purpose sexism has in this argument, my staff is evenly divided & I haven't seen any correlation - all of my people have equally odd and complementary abilities.

2) Both F & E have a place in good software design as does art, formalism is necessary to "define the envelope" and experimentalism is necessary to fill it.

But art is necessary in determining that it can be done in the first place: it takes a peculiar sort of attitude to take "it can't be done" as a challenge rather than a fact & I choose my people for attitude, ignorance is curable.

When I use maxterms & minterms to establish a logical path from inputs to outputs, formalism tells me how many steps are necessary and hints at the best path and experimentalism will often find innovative paths to sucess, (of course having learned FORTRAN II as my milk language and having used EQUVALENCE & reverse dimensioned arrays in the past to accomplish goals probably does not make me a good model for the innocent), but neither is of much use for creating the model - that takes art.

As do many things, this reminds me of a quotation attributed to W. A. Mozart (if incorrect, I am certain that the RISKS readers will correct me). A student asked how both/he/it/she (covers all bases alphabetically) could learn to write an opera. When told that it took a combination of schooling, study, & practise that totaled over twenty years, the response was: "But Herr (do not think this is in question) Mozart, you wrote your first opera when you were sixteen !?". Wolfie replied: "Ah yes, but I did not have to ask."

Padgett

Report problems with the web pages to the maintainer

Search RISKS using swish-e

THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

ACM Committee on Computers and Public Policy, Peter G. Neumann, moderator

Volume 11: Issue 92

Monday 17 June 1991

Contents

RISKS DISK'S WHISKS TSKS!

"Peter G. Neumann" <neumann@csl.sri.com>
Mon, 17 Jun 91 13:58:33 PDT

Speaking of things not working as expected (see the next three messages), the active RISKS disk on CSL was down from late Thursday until mid-Monday. [The repairman said finally today rather calmly, "The disk motor fell out."]

The mail server (Hercules) remained up. Nevertheless, all sorts of incoming mail was rejected. If you got BARFmail, please RETRY. Thanks. PGN

The Patriot system and the Dharan Scud: Time Warp

"Peter G. Neumann" <neumann@csl.sri.com>
Mon, 17 Jun 91 13:56:25 PDT

The 10 June 1991 issue of Aviation Week and Space Technology (p.25-26) has another increment on the Dhahran Scud attack. In the four-day siege ending on 25 Feb 91, one of the two batteries was down for radar repairs. The other had endured a clock drift of .36 seconds, which was enough to prevent the radar from tracking the Scud. It seems that the spec called for 22 hours of continuous operation, with the tacit assumption that the system would be shut down each day, maintained, and possibly moved to another location. 100 hours was obviously well beyond spec...

A two-cable telephone interruption: Washington D.C.

<smb@ulysses.att.com>
Fri, 14 Jun 91 16:07:09 EDT

A fiber cable cut, in Annandale, Virginia, knocked out the Associated Press's audio feed for their radio news service. They do have a backup routing system, which switches transmissions to a second cable if the first one fails. However, according to a spokesperson for the AP, ``Somehow, they both ended up being hit by this incident.''

--Steve Bellovin

A two-cable telephone interruption: Washington D.C.

"Peter G. Neumann" <neumann@csl.sri.com>
Sun, 16 Jun 91 14:23:13 PDT

About 80,000 telephone circuits were accidentally knocked out when a contractor severed two fiber-optic cables in a suburb of Washington, D.C. UPI, AP, the Pentagon, residential, and business phones were cut off for a few hours in the morning of 14 June 91, along with some cellular phone relay stations. [Source: San Francisco Chronicle, 15 June 81, p.A5] The outage lasted from 9:30am until 3:30pm.

<<<<<<<<<<<<<<<><><><><><><><><>

TWO cables in one swell foop! So, as in the 1986 cutoff of New England from the rest of the ARPAnet because one cable held all supposedly-independent 7 circuits, the primary and the backup were knocked out -- this time despite the precaution of running them through separate cables. Murphy and his twin brother were both at work.

This episode occurred just in time to add another datapoint for my talk at COMPASS '91 on 26 June at NIST in Gaithersburg MD, presenting my annual `risk award' paper, this year's title being

"The Computer-Related Risk of the Year: Weak Links and Correlated Events",

considering a bunch of outages resulting from single-point failures and other cases in which apparently independent events resulted in disasters. The phone cases discussed include the AT&T long-distance problem on Jan 15 1990, the NY-area cable on 4 Jan 91, and the White Plains ARPAnet 7-link outage 12 Dec 86. The multiple-event cases are also drawn from the RISKS archives.

If you are interested in COMPASS '91 (information, proceedings, etc.), please contact Dolores Wallace at NIST. Try wallace@swe.ncsl.nist.gov or mayhaps DWallace@nist.gov if their "standardization" works...

Oh, by the way, RISKS will slow down for this week and next. I'll put out an issue only now and then. PGN

Abusenet (a feeling of deja vu?...)

Pete Mellor <pm@cs.city.ac.uk>
Mon, 17 Jun 91 15:39:20 PDT

An item appeared in yesterday's Mail on Sunday which sent a shiver down my spine. (I don't have the article to hand, so I am summarising from memory.)

Apparently, innocent British kids are being corrupted by a tidal wave of filth from the other side of the Atlantic. This is being beamed right into their homes via satellite, and all they have to do is flick a switch on their computers to receive explicit hard-core porno pictures which they can display on screen. The authorities are powerless, since the source is outside the UK, and even the existing laws governing posting of indecent material do not apply.

This dire state of affairs has come to the attention of a certain Emma Nicholson, MP (she of the proposed draconian laws against hackers: see RISKS passim), who thinks that someone ought to do something about it.

Expect some half-baked attempt to introduce legislation to control UK access to Internet! :-(

Peter Mellor, Centre for Software Reliability, City University, Northampton Sq.,London EC1V 0HB +44(0)71-253-4399 Ext. 4162/3/1 p.mellor@uk.ac.city(JANET)

IRS Tax Systems Modernization

<rlw@ida.org>
Mon, 17 Jun 91 13:16:54 E+1

The IRS is heavily involved in a Tax Systems Modernization (TSM) program. The following (part of the public record) is from the IRS Commissioner's testimony to congress about the program.

Chart 2 Projected Benefits From TSM

Eliminate 6-7 million unnecessary contacts with taxpayers each year that are now required to correct name, address, social security number or account information.

Eliminates 95 percent of the computer-generated enforcement notices that our current systems mail out after a taxpayer has properly responded to a prior notice.

Resolve during the first call 80 percent of all taxpayer questions that are raised by telephone.

Assure that in 95 percent of all cases, a taxpayer can resolve an IRS-related matter by dealing with a single IRS employee, and can do so within specified time frames (ranging from minutes to months, depending upon the nature of that matter).

Generate all account-related correspondence to a specific taxpayer, not a generic "taxpayer".

In all cases, provide IRS front-line employees (and taxpayers) with current, complete and accurate account information.

Provide copies of tax returns to IRS employees and taxpayers within one day rather than the current 45-day target. (A goal we presently are unable to meet one-third of the time.)

Reduce case processing times by 20-15 percent.

Reduce taxpayer, practitioner and IRS caused processing errors by 70-90 percent for electronically filed returns; increase number of taxpayers using electronic filing from 4 milion (1990) to more than 25 million by the mid-1990s.

Maintain and enhance the privacy and confidentiality of tax returns and taxpayer information.

Generate the information necessary to move from after-the-fact, case-by-case enforcement activities activities to comprehensive strategies designed to enhance voluntary compliance, while minimizing the burden on taxpayers and reducing costs to the government.

Generate annual savings of $500-700 million (by reducing systems maintenance costs, reducing staffing in paper intensive processing activities, and eliminating the costs of storing and retrieving paper documents).

EC draft directive on telecomms privacy

Martyn Thomas <mct@praxis.co.uk>
Fri, 14 Jun 91 10:34:13 BST

The European Commission (CEC) has issued a draft directive on privacy of telecommunications. The idea is to bring the EC natins' laws into harmony,

so that the service and privacy are the same throughout the EC. The draft directive is COM(90) 314 final - SYN 288.

Some parts may be interesting for comparison with US practices:

Article 8: The telecommunications organisation [t.o.] must provide adequate, state-of-the-art protection of personal data against unauthorised access and use. In case of particular risk of a breach of the security of the network, for example in the field mobile radio telephony [sic], the t.o. must inform the subscribers concerning such risk and offer them an end-to-end encryption service.

Article 12: [paraphrased]. callers must be able to disable CID per-call, and per-line. Called subscribers must be able to disable incoming display of IDs per call or per line, and must be able to restrict incoming calls to those which transmit IDs. Overrides must be available for tracing nuisance calls and for emergency services, and these must work community-wide.

Article 17: [paraphrased] Subscribers must be able to request that unsolicited advertising calls are blocked, and the t.o. must take the necessary steps to prevent such calls.

Article 19: "The provisions of this directive relating to the telephone service shall be applied to other public digital telecommunications services to the extent that these services present similar risks for the privacy of the user".

Martyn Thomas, Praxis plc, 20 Manvers Street, Bath BA1 1PX UK.
Tel: +44-225-444700. Email: mct@praxis.co.uk

EC draft directive on data protection

Martyn Thomas <mct@praxis.co.uk>
Fri, 14 Jun 91 11:15:37 BST

The Commission of the European Community (CEC) has issued a proposal for a Directive on data protection [COM(90) 314 final - SYN 287.]

It is very detailed and prescriptive. The broad principles are similar to the UK Data Protection Act (which I assume is well-enough known to save me hours of typing!) with two notable extensions:

The "data-subject" has to have given informed consent to any processing which goes beyond "correspondence purposes" (subject to exceptions for public authorities and other processing specifically authorised by law).

The protection is NOT limited to computer files - it covers all manual files as well.

Article 17 is interesting:

"The Member States shall prohibit the automatic processing of data revealing

ethnic or racial origin, political opinions, religious or philosophical beliefs
or trade union membership, and of data concerning health or sexual life,
without the express and written consent, freely given, of the data subject. [
... ...] Data concerning criminal convictions may only be held in public
sector files."

Martyn Thomas, Praxis plc, 20 Manvers Street, Bath BA1 1PX UK.
Tel: +44-225-444700. Email: mct@praxis.co.uk

Algol vs. Fortran (Nilges, RISKS-11.90)

<smb@ulysses.att.com>
Thu, 13 Jun 91 20:33:31 EDT

> Algol lost out to Fortran in part because of imperialism:
> Algol was superior to Fortran but the United States could not
> concede that the Europeans had the lead in programming languages.

This claim, though (mercifully) tangential from the main thread, is actually
quite relevant if viewed differently. Is Algol really superior? By what
metric?

Fortran was carefully crafted to be as efficient as assembler language.
Witness, for example, the restrictions on subscript form -- they were imposed
so that a comparatively-simple compiler -- and today's optimizers didn't exist
-- could generate excellent code. Algol, on the other hand, had constructs
like call by name, and required a stack for efficient implementation.

Today, with the hindsight of 30-odd years, it's easy to see that Algol is
better. But the criteria by which we make that judgement didn't even exist
then -- all there was was the clash of efficiency versus an (obvious) elegance.
And even if those making the choice had known of our concerns, it's far from
obvious what they would have decided -- machine cycles were not seen as a
luxury.

Sure, cultural NIH played a part. But don't discount the effect of people
aiming for different -- and equally valid -- targets. (I leave the connection
as an exercise for the reader.)

--Steve Bellovin

The best is not good enough -- why Algol lost out to Fortran

Martin Minow 14-Jun-1991 0949 <minow@ranger.enet.dec.com>
Fri, 14 Jun 91 06:57:36 PDT

I must respectfully disagree with the claim in Risks 11.90 that Algol lost out
to Fortran because of an American rejection of a superio -- but non-American --
language. There are several other reasons, some of them actually Risks
related:

-- Algol-60 lacked a usable input-output method, especially one appropriate

for the offline tab-equipment (punch cards and line printers) in common use in America in the '50's and early '60's. This was an intentional omission in Algol-60, as many of the computers it was first (in Europe) were one-of-a-kind research computers that used 5-channel paper tape and teletype printers. Magtape was generally unavailable.
-- No Algol-60 compiler was available on an IBM-709 series machine until, roughly, 1966. (Well, there was the Algol-58 MAD, but it was a university development that ran on a non-standard executive.) By 1965, however, Fortran was being taught to engineers as an engineering tool (one of my programming courses was in the agriculture department), the IBM 360 was about to replace the 709-series. and PL/I was not yet available.
-- IBM *marketed* Fortran to engineers: I learned it from a tiny manual called, as I recall, "An Introduction to Engineering Analysis by Computer" that taught Fortran by example, and used "real" engineering problems for its examples (structural engineers did not see the relevance of the eight queens problem).

The above claims are from my own experience: I learned Algol (from Dijkstra's book) before Fortran, gave some minor assistance to the Alcor-Illinois Algol-60 compiler team, and programmed for several years exclusively in Algol-60 on an European 1st-generation computer using a compiler that I believe was written by Dijkstra -- and a very good compiler it was, too.

Martin Minow minow@ranger.enet.dec.com

Caller ID and 800 numbers (Mainwaring, RISKS-11.91)

Lauren Weinstein <lauren@vortex.com>
Mon, 17 Jun 91 12:01:41 PDT

John (J.G.) Mainwaring, in response to my recent statements on caller ID (CID), suggests that since 800 calls are essentially a "collect call", that caller number information is appropriate to provide to the callee.

He states:

"A call to an 800 number is in fact a collect call. A person (or company) has at least a plausible argument that they should know who is calling, and have the right to refuse calls from whomever they please."

He also suggests that callers could avoid perceived problems by finding the number of the company via directory assistance and not using the 800 number. Outside of the fact that this would require the caller to pay for the call, it can be difficult, and often impossible, to gather enough information from a quick commercial or even a print ad to dig out the actual name of the parent firm who would be listed and to know where they are listed. Then you end up paying for the directory assistance call, and, assuming you get a number, find yourself talking to a receptionist at corporate headquarters, rather than the sales or info people who answer the 800 number and might be located somewhere else entirely!

I would agree that 800 calls, being of a "callee pays" nature, are deserving of special consideration (however, this does not apply to non-800 calls, which are the primary focus of the now appearing general purpose CID systems). One of the problems, however, as has been mentioned here before, is that CID does not tell who is calling, it tells the number of phone from whom the caller is calling!

When someone calls you collect, are you told the number they are calling from? No, you are told *who* is calling. As I mentioned in my original article, people make calls from different numbers at different times! Nor should one be required to provide their number in order to "identify" themselves. Telling someone who you are (if they have a "need to know") is one matter--giving them your (possibly unlisted) phone number is something entirely different.

While at least one telco is experimenting with a name delivery service in conjunction with CID, this as far as I know is providing the name associated with the phone number account, not a name as provided by the person who is actually making the call (who may have nothing to do with the name on the account). This forum has previously seen discussion of proposals that would allow the caller to individually specify what name would be sent to the callee as an identification on a call from any phone. There is no evidence that the telcos are interested in such systems or that they are moving in that direction. Such systems would of course have various RISKs associated with them as well, and I would consider it important that callers still be able to choose not sending any identification at all if they so desire.

Decisions made on the basis of caller telephone numbers will often be incorrect. Even worse, callers may not even realize why they were treated the way they were, since they won't usually know how much (possibly erroneous and often invasive) information was gathered based on their phone number before their call was answered. The ANI magazine I mentioned previously suggested using calling number as a means to determine what language operator to use when answering incoming calls, since, it states, "people who speak different languages tend to live in geographic clumps". While this is one of the less onerous applications of this technology, it gives some insight into the rather bizarre thinking going on among some of the proponents of these systems.

Regarding the specific issues of 800 numbers, the legitimate concerns of the firms paying for these numbers can be preserved in other ways. Presumably it could be made possible for them to block calls from particular numbers, without knowing what those numbers are, just as in standard CID systems. There are of course RISKs associated with this, given that you are dealing with a phone number, not the person who might be, for example, making harrassing calls to your firm. You could end up blocking a number that happened to be used for some troublesome calls at one time but that later might represent a potential customer. And people do change their phone numbers!

An even better technique would be for the telcos and long distance (LD) carriers to be required to respond to an 800 subscriber's request for dealing with harrassing or troublesome calls. This could be done by the telco or carrier looking at the call pattern information for the subscriber (at their request) to determine the caller numbers, or through the use of a Call Trace system like that which exists as an

alternative to CID for conventional calls. In either case, the subscriber themselves would not need to know the caller's phone number.

To make it easier for the 800 subscriber to detect abusive calling patterns but avoid the problems associated with full number delivery, it might be reasonable to provide the 800 subscriber with the caller's area code and prefix only, when the caller has specified CID blocking. This would only apply for 800 calls--for all other calls a CID block would result in no number information being provided.

Area code and prefix would provide enough data to pick out harrassing or other troublesome 800 call patterns. In conjunction with rules that required the telco or LD carrier to cooperate in such cases to use their full number information that they have for the callers to deal with taking action against such callers, this could solve the problems without revealing the full caller number to the 800 service subscriber. The lack of full number would make most of the more obnoxious applications of CID/ANI delivery on 800 numbers impossible.

Of course, the telcos and LD carriers would prefer not to be involved in this process. They'd prefer that the caller and callee just slug it out completely amongst themselves. Their main concern is that if full calling number information is not available to the entity being called, a massive potential revenue stream from business applications that would make (mostly realtime) use of these numbers would be rendered impractical.

--Lauren--

Search RISKS using swish-e

THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

ACM Committee on Computers and Public Policy, Peter G. Neumann, moderator

Volume 11: Issue 93

Monday 17 June 1991

Contents

Formalism and women

<SIMONS@IBM.COM>
Fri, 14 Jun 91 10:08:25 PDT

I have found the discussion on formalism and women quite disturbing. For starters, I suggest that we attempt to minimize or completely eliminate the use of two loaded phrases: 'Politically Correct' and 'sexist'. They push people's buttons and result in heated, but not necessarily rational, discussions. Instead of using loaded words, let's specify whatever it is that bothers us. This might lead to a calm discussion and possibly even a deeper understanding of the issues.

I am strongly opposed to efforts at university campuses to penalize people for what they say, no matter how offensive. But I phrase my opposition in terms of the first amendment and freedom of speech. It has nothing to do with Political Correctness or lack thereof. The current movement to label ideas or programs as P.C. is a chilling reminder of McCarthyism, which also involved mindless branding of people and ideas. Consider the following, written by Ed Nilges:

>This does not mean, however, that I hew to any "politically correct" line
>that (for example) women's needs should always have precedence over the
>requirements of the field.

Dear Ed, I am a feminist, and almost all the female computer scientists I know would consider themselves feminists. Neither I, nor any woman or man I know, would suggest that women's needs should always have precedence over the requirements of the field. In fact, every woman I know would be very upset if anyone were to propose such a thing. Do you know any women computer scientists? If so, has any of them, or anyone else you know, ever made such a suggestion?

The comment below was written by Michael Tobis:

>I have recently become aware of the extent to which the more ambitious
>(generally female baby-boomer academic) proponents of "deconstruction"
>intend to carry their philosophy. I was, in conversation with one such,
>discussing the (well-known to RISKS readers) propensity of the press to
>garble matters with a scientific content.

>The female baby boomer academic in question responded that this was indeed the
>case, and that "you scientists are so attached to your orthodoxies". Yes, the
>law of entropy, folks, is not an enigma, not a strange but inevitable feature
>of the fabric of the universe, nor an excellent approximation to reality whose
>limits have yet to be discovered. It is a dogma, if the deconstructionists are
>to be believed. What is more (here in the interests of preserving our
>friendship the conversation had to be dropped) it is no more or less true than
>"any other myth".

>My guess is that had the conversation continued, the second law would be
>denounced as sexist, since it had been promulgated almost exclusively by
>wealthy or at least bourgeois white males.

Michael, I realize that you had not intended to offend anyone, but I was made very uncomfortable by your remark. It might help to understand my discomfort if you substitute the word `Jew' for `female baby boomer'. That doesn't sound ok, does it? It also doesn't sound ok to `guess' what the woman would have said, or to imply that her comments are in any way a function of her being female, or that proponents of `deconstruction' tend to be female. (I've never heard that word mentioned by any of my friends, male or female, and I expect I know more women than you do).

I am a theoretician, and I would like to see more, not less, rigor in our field. I also want to see more women and blacks in our field. I am convinced that we can introduce more rigor AND develop teaching approaches that do not alienate women or minorities.

Barbara

---

women and programming

Alex Martelli <alex@am.sublink.org>

14 Jun 91 22:22:26 MDT (Fri)

I am rather astonished at the `women/programming/logic' thread. I believe a *MAJORITY* of graduates in mathematics in Italy are women! The firm I work for, a software house specializing in non-electronic engineering CAD applications, has roughly a 50-50 split in the software production division personnel between men and women. This is despite the fact that a VERY large majority of mechanical and civil engineering graduates in Itali are men, and of course we need staff with such degrees for expertise in the application domains; this is balanced by our need for advanced mathematical techniques, for such applications as solid modeling, and computational geometry in general - for this, we mostly look for mathematicians, and most mathematicians (around here) are women!

I have definitely seen discrimination against women in the computer area - I regret, for example, the fact that a huge majority of computing *enthusiasts* in Bologna are men - but here I'm talking about the kind of guys who spend nights and weekends hacking on PCs, chat on Fidonet, and meet at night in clubs and osterias to spend even more time on their favourite subject... most of them wouldn't know formal techniques from baked zucchini! So, whatever is discouraging women from joining in such pursuits, it most surely is not any emphasis whatever on formal logic.

The general man/woman stereotype around here is probably that men are supposed to be more apt at "practical" matters (thus tend to go for degrees in engineering more often than maths), while women are supposed to be more "theoretical" (thus, the reverse). I deeply mistrust any such stereotype, and I find it just wonderfully laughable to learn that the US stereotype is supposed to be JUST THE REVERSE! Tacke no wooden nickels from bigots of either side...

Criteria and Science

Christopher Maeda <cmaeda@EXXON-VALDEZ.FT.CS.CMU.EDU>
Fri, 14 Jun 91 01:37:49 EDT

In all the cross talk on Formalism, Experimentation, etc. I think we have lost track of the heart of the matter. Michael Tobis said it best, at least in the last few issues of Risks:

> In a nutshell, the problem is not the extent to which formal automata theory, software engineering, verification, etc. should be presented in an undergraduate program. The problem is that the issue is being attacked _on the grounds_ of its social/political appropriateness, rather than its utility.

Let us remember that Computer Science aspires to be a Science. As such, a thing's utility (for "doing" Science) is the only criterion that we, as Scientists, can use to judge a thing's value. The risks of doing otherwise in a society so dependent on the fruits of science are immense. I don't want to be drawn into the vortex of who's way of thinking is better and whether there is any correlation with gender. Suffice to say that there are undoubtedly many

ways of thinking but all are not necessarily useful for doing Science. Note that what is useful for Science often has no relation to what is useful for the rest of society.

It is unfortunate that women are underrepresented in Computer Science but it is hard to propose solutions (at least for me, personally) when you are unsure of the causes. These are also the types of problems that I was trying to avoid when I went into Computer Science in the first place :-).

Finally, the deconstructors of science seem to have gotten most of their ideas from Kuhn's _The Structure of Scientific Revolutions_ but with a political slant. I don't see how people get surprised when they hear that scientists don't really know or search for Truth. That's what philosophers do.

Re: Formalism vs. Experimentation (RISKS-11.89 et passim)

Pete Mellor <pm@cs.city.ac.uk>
Mon, 17 Jun 91 15:11:08 PDT

To avoid the argument becoming too one-sided (i.e., one side of the Atlantic! :-), I thought I'd chip in with my three-ha'p'orth:-

That women *are* discouraged from analytical subjects such as Maths and Physics is undeniable. The following anecdote from my schooldays illustrates this beautifully:-

At my co-ed grammar school (high school for "academic" kids who managed to pass the dreaded 11-plus exam), it was decided by the powers that be that it was not possible to teach both Biology and Physics to O-level (exam at around age 16). At the end of the second year, we were gathered together in front of the headmaster, who informed us that we had to choose between the two options. In view of the natural distribution of abilities, we were informed, it had been decided that all girls would take Biology, and all boys would take Physics, from the third year on. Anyone who objected had to produce a letter from their parents within three days.

Result: two girls, one a very bright mathematician, the other her best friend to keep her company, did Physics; one boy, a keen entomolygist, did Biology.

This, of course, was in my schooldays, i.e., 100 years ago, and things must be better now. So why does my daughter, in her first year at high school (girls only, so I *hope* without the element of boy/girl comparison), never mention Mathematics without an automatic expression of disgust? When I point out that Maths is a fascinating and creative subject, I get a reaction of the "Oh, yeah? Who does the old fossil think he's kidding?" type.

The problem seems to lie with the subculture of that strange alien tribe "teenage girls", and from her conversation, I gather that social acceptability depends upon having Jason Donovan occupying both right and left hemispheres of the cerebral cortex. Her greatest ambition at the moment is to be a hairdresser.

My problem is to guide her into a career where she will earn enough to support me in my retirement. Given the state of funding of British universities, this will have to be a career which shows a quick return, so perhaps I had better steer her towards photographic, rather than mathematical, modelling. :-)

BTW, it wasn't much fun being a boy who was good at Maths, either. The US comedian Emo Philipson is doing well over here right now. On the radio last Saturday morning he said "I wanted to be a nerd when I was at school, but I didn't have the math requirement!".

I did and I was, Emo! :-)

Peter Mellor, Centre for Software Reliability, City University, Northampton Sq.,London EC1V 0HB +44(0)71-253-4399 Ext. 4162/3/1 p.mellor@uk.ac.city (JANET)

Re: The impact of formalism on Computer Science education

"Robert J. Reschly Jr." <reschly@BRL.MIL>
Thu, 13 Jun 91 22:48:51 EDT

I am sympathetic to the notion of equality when it is based on equivalent ability. No one seems to contest the notion that different segments of the population have differing abilities -- I am emphatically *not* implying they are necessarily innate; they may as easily be instilled -- which impact their suitability for a particular pursuit. To argue that varying suitability is not relevant is sheer folly.

It then comes down to making an often very difficult assessment as to whether the difference is innate or instilled. Instilled differences should be rooted out and corrected, remedially and proactively, but it may be too late in some cases to correct the damage already done. Attempts to compensate for uncorrectable differences can also be made, but in certain situations the added risk may not be justifiable.

Consider for a minute the fact that, even though I had (and still mostly have) excellent reflexes and hand/eye coordination when I went into the service, my 20/400 (uncorrected) vision ensured I would never set foot in the cockpit of a military aircraft. The fact that my acuity is 20/15 (corrected) has no bearing as far as the military is concerned, and I doubt many people inside or outside of the military would question that evaluation.

I would argue that producing correct programs is still difficult enough to warrant similar evaluations. The trick lays in determining the nature of any differences and fixing those which can be addressed.

U.S. Army Ballistic Research Lab. / Systems Eng. & Concepts Analysis Div. Networking & Systems Dev. Team / Aberdeen Proving Grounds, MD 21005-5066 (301) 278-6808 UUCP: ...!{{cmcl2,nlm-mcs,husc6}!adm,smoke}!reschly

---

Women, Computing, & Men

lance.norskog <lance@motcsd.csd.mot.com>
13 Jun 91 21:27:32 GMT

Men talking about "the female mind" is sooooooooo enlightening.

My personal take is that men, much more than women, are fascinated by the act of rearranging machinery. Male programmers prefer software tools which allow them to fiddle endlessly and achieve nothing, because all the really matters is changing the machine. This emphasis on spending vast amounts of time on low-level programming with little end result is, in my experience, why most women exposed to software engineering have little desire to do it for a living.

The biggest consequence of this is that our software engineering environments are dominated by facilities for the pointless and endless rearrangement of bits. After 15 years of watching my development machines speed up 1000fold and my development tools stand still, I have decided that this fascination with fiddling is the single most important factor in the glacially slow progress of software engineering over the past 40 years.

The RISK is not letting women build the software that controls our safety, it is letting men do it.

Lance Christopher Norskog

Read "The Psychology of Computer Programming" by Joseph Weizenbaum. It's all explained there.

Re: The impact of formalism on Computer Science education

paj <paj@gec-mrc.co.uk>
14 Jun 1991 11:00:05-BST

I read with interest Hal Pomeranz's contribution to this debate in RISKS-11.87. Hal fears (along with Karen Frankel, author of the CACM article which sparked this debate) that the emphasis of a solitary `thinking' approach to computer science rather than a hands-on teamwork approach will discourage women from taking up computing as a profession.

I agree with Hal that the superiority of `abstract' over `hands-on' (to label the two approaches rather inaccurately) has not been demonstrated. However, if such a thing is demonstrated, surely it should be taught regardless of whether there are differences between the average abilities of men and women in dealing with this approach. The point of equal opportunities is to allow women (and men of course, although that is not usually a problem) to fulfil their potential, to the benefit of themselves and society. If it should turn out that an apptitude at the `abstract' approach is necessary to be a good programmer and that women do not have this apptitude (which has not been demonstrated to my satisfaction either) then we are driven to the conclusion that in general men make better programmers than women and the lack of women in computing is therefore a Good Thing. Of course, the exceptional women who can

deal with the `abstract' approach should be encouraged to enter computing.

It seems to me that Frankel and Hal are being sexist themselves, in asserting that there is an area of human endeavor in which men are intrinsically better than women (abstract thought). They then compound this error with special pleading for the educational system to use a non-optimal teaching method in order that this failing does not show up in the statistics. The end result of this would be a lower standard of computer programming in the world.

---

political correctness - to PANIC or not to PANIC

Michael Tobis <tobis@meteor.wisc.edu>
Fri, 14 Jun 91 17:52:23 GMT

In response to Mr. Ditchfield's criticism, I must admit that it is true that I haven't yet read the original CACM article, and that my belief that the word "sexist" was used in this particular discussion is second-hand, through Mr. Nilges. My excuse for not reading the article is that I was in some haste to call the attention of the RISKS community to the existence of a significant community of people who consider the importance of science to be purely relative, culturally determined, and political.

It is entirely possible that I owe Ms. Bernstein, at the other end of a long chain of citations, an apology. Nevertheless, the attack on issues of remarkable intellectual purity on the basis of political correctness does exist, and I am pleased to have called the attention of a fairly large population to it. Although it is a small proportion of the world's population that takes political correctness to these extremes, it is an extremely important one, as many undergraduates' first exposure to intellectual pursuits these days (certainly in North America, perhaps elsewhere) is a vigourous condemnation of rationality, the principles of evidence and discourse, and ultimately intellectual honesty. [...]

Michael Tobis tobis@meteor.wisc.edu

Re: Political correctness (Nilges, RISKS-11.86)

Richard A. O'Keefe <ok@goanna.cs.rmit.OZ.AU>
15 Jun 91 08:22:12 GMT

> Bernstein, according to Frankel, feels that Dijkstra is being sexist! ...

Several people have responded to this, but none of them seems to have made the point that the alleged conflict between "solitary abstract thinking" and "teamwork" is totally bogus.

One of the clearest thinkers I've read, Popper, stresses the need for critical *discussion*. Good software construction requires tossing ideas around, deep thinking about the ideas, and critical examination of those ideas. It is worth noting that many of Dijkstra's articles refer to problems which came up in

group discussions, and to solutions which have undergone repeated criticism and consequent improvement. Let me stress that: what Dijkstra himself does, and what his students do, and what he and they have taught by example as well as precept is not

"solitary abstract thinking"

but "logical reasoning as an important component of a rational-critical discipline". Dijkstra has written joint books/papers with Feijen, Scholten, var Gasteren (just to name co-authorships I can remember off the top of my head); he is clearly an exponent of COLLABORATIVE abstract thinking.

Nor are abstract thinking and experimentation incompatible. I haven't much experience teaching Computer Science yet, but what I have noticed is that good students seem to do _both_ and poor students seem to do _neither_. Experimentation gives you something to think abstractly _about_, while abstract thinking is required to design informative experiments. (Something like "what shall I try next? Hmm, I haven't tried throwing the sword at the troll. Maybe that'll get me across the bridge." requires abstract thinking about what you have already tried.)

As for political correctness, the claim that women aren't good at thinking logically smells to me like the old stereotypes dressed up in new clothes. I've met too many good women statisticians and programmers to believe it. From reading many articles by British women scientists, I have a strong suspicion that equal pay and equal respect are a better answer to the question "how to get more women doing X" than pandering to imaginary weaknesses.

Finally, if I may quote Dijkstra himself:

> "Too often, we see a failure to distinguish sufficiently clearly between the intrinsic problems of computer science and the difficulties resulting from the shortcomings of our various educational systems."

Formalism and Experimentation

<WHMurray@DOCKMASTER.NCSC.MIL>
Fri, 14 Jun 91 09:25 EDT

> Why do our schools teach programming as an INDIVIDUAL activity? ...

Why, indeed! Because we put our schools in a double bind; we ask that they both teach and grant credentials. As a consequence, the issue is not what work gets done, nor even what was learned. Instead it is who did the work. "Who gets the credit," as an issue, is so deeply ingrained in the American academic system as to be incapacitating.

Most recent graduates of our system do not want to work on teams. Indeed, they will refuse to do so. They want to go off in a corner and write code by themselves. (My experience was that it often took years to incorporate one so trained into an organization where they could be productive.) Teamwork has been stigmatized by our educational system; instead of encouraging and exploiting it, they call it "cheating."

Learning should be for our children the same kind of joyful experience that it is for us, the elite survivors of this cruel hoax. We have made it into a contest with few winners and lots of losers. No wonder our dropout rate is so high.

We have the recent sorry spectacle of one our most prestigious institutions assigning work that could only be accomplished in teams, should only be attempted in teams, and then getting upset when the students discovered the trick. Unfortunately for us and for the students, the situation was treated not as a discovery, but as ethical and moral terpitude. Shame! I hope that the students involved in this sorry mess understand what was done to them.

If our children are to have a place in the world, they must learn to value, not despise, teamwork. If they are to do so, we must separate the teaching and credential granting functions in our educational system. Unfortunately, some of our schools are so poor at teaching, that without the credentials to grant, they will have to close their doors.

William Hugh Murray, 21 Locust Avenue, Suite 2D, New Canaan, Connecticut 06840
203 966 4769, WHMurray at DOCKMASTER.NCSC.MIL

Rerebuttal on computer education

<Eric_Florack.Wbst311@xerox.com>
Fri, 14 Jun 1991 08:00:49 PDT

Paula Ferguson, in 11.90:

-=-=-
First of all, computer science isn't a science like chemistry, it is an engineering discipline. There are no "laws" of computer science.
=-=-

OK... Let me ask you: What is one of the reasons why everyone feels that C is the darling of programming languages? Why are we not programming in BASIC, for example? Simple: The higher level of logical structure used by C gives you a more powerful tool.

Granted: There are no 'laws' per se', when it comes to computer science, other than the ones we create, since computers are more about thought than about physical reality. But I would point out that it is their logical ability that makes them useful to us. Logic is the one basic atribute that we can pin on the computer; it only thinks in choices of ones and zeros.

I'm by no means suggesting that we leave creativity behind; Indeed, it's needed to program well.... but creativity needs a base of practical knowledge from which to operate. A musician must learn to play their chosen instrument, and have the tech ability down pat before the level of creativity can become apparent. In any field of endevor, that base must be established first. In computers, that base is logic, and the ability to think logically.

You say:
-=-=
Educational techniques have changed very little
in the past century while the world has changed considerably. The
educational crisis is the result of this disparity. Kids don't feel like
their teachers are teaching them anything worth learning, so they don't
learn. Until education is made relevant to kids' lives, the crisis
won't go away.
=-=-

I would suggest to you that the failure here lies not in making the material
relevant to the student, by changing that material to fit the student's
preferrence.. it already /is/ relevant. The failure lies, for the most part, in
the teacher's inability to / convince the student / that the material is
relevant.
(The question of it's being purely the teacher's fault goes outside the realm
of this discussion, but for my part I don't think it is.) I would further
suggest that this is the major failing in the area of female students and
computing. IE: if female students are told from the womb that mechanical and
logical studies are not relevant (You're a girl, you don't have to learn
that...) they'll oblige... and in the long term have a larger barrier to
overcome.

This is true of anyone, not just those outside the established mainstream.
As Nancy Levison points out, (forgive me if I've mis-spelled your name, Nancy)
the idea that minority groups can't make it through the existing system without
some kind of slanting towards them, is insulting, demeaning, and is the root
cause, not the solution, to the ever widening gap between mainstream and
so-called minority students. (Since females make up 51% of our population I
question calling women a minority...)

(Insert your favorite downtrodden here) will continue to under-perform as long
as that's what's expected of them. I ,for one ,value their 'style of thinking,
and the contribution they can make' as you put it, but suggest that the basics
/must/ be instilled before these can be used to their best advantage.

To tie this back to the original angle: The RISK here is the loss of many good
programmers if we don't take this path.

Search RISKS using swish-e

THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

ACM Committee on Computers and Public Policy, Peter G. Neumann, moderator

Volume 11: Issue 94

Tuesday 18 June 1991

Contents

V-22 Osprey crashes on first flight

Martyn Thomas <mct@praxis.co.uk>
Tue, 18 Jun 91 12:43:18 BST

The fifth prototype Bell-Boeing V-22 Osprey tilt-rotor aircraft crashed one minute into its maiden flight on June 1st, according to Flight International (19-25 June, p 16). The pilots reported control problems, with the aircraft feeling tail heavy and rolling from side to side.

The other four V-22s have 567 flight hours in 463 flights. The maiden flight of number 5 was postponed last week after tools were found to be missing, but only a drill-bit was found under the fuselage floor.

Flight-control software problems in another V-22 were traced to a faulty switch.

Martyn Thomas, Praxis plc, 20 Manvers Street, Bath BA1 1PX UK.
Tel: +44-225-444700. Email: mct@praxis.co.uk

Re: The Patriot system and the Dharan Scud: Time Warp (RISKS-11.92)

<HORN%HYDRA@sdi.polaroid.com>
Tue, 18 Jun 91 13:48 EST

A slight correction, the specification for Patriot was 14 hours of operation. The 22 hour figure was the actual operational time for systems that did detect the Scud but were out of range. The origin of the 14 hour spec was the original intended use of Patriot in defense of mobile forces where it was expected that the systems would relocate several times per day, so the assumption was not tacit. It was a deliberate considered decision, balancing procurement and operational costs against the operational needs.

For those who don't understand how a 0.36 second (or 1 ppm) error can cause this problem, you have to examine how a machine tracks a target. At initial acquisition time you have a single location, but no speed or direction. So you put a ``box'' around the location and look again a very short time later. Based upon the article, the timing error resulted in a mislocated box. A slower target (like an airplane) would still have been within the box. A Mach 6 missile was outside the box. So the computer did not associate the second echo with the first echo.

This incident is a good illustration of the problem with the overemphasis of formal proofs. They are only as good as the specification being proved. I cannot find the reference, but I recall that more than half of the problems found in current delivered systems can be traced to incorrect specification.

The issue of proper specification is important to all industries, not just software. It is time to start listening to the ideas that are being spread in other industries. A good starting point for a literature search is to read the works of Deming, Juran, Taguchi, and Ishahawa. Then look under keywords like ``Total Quality'' and ``Quality Function Deployment'' and expand from what you find there.

Total Quality distinguishes three kinds of requirements:

- Expressed, those that the user actually states e.g. ``I want a hotel room tomorrow night''. These are the traditional totality of software requirements.

- Expected, those that are expected but not expressed e.g. that the hotel room has a bed. With Patriot, the expected but not expressed requirement was that so long as the other hardware remained functional past its specified endurance the software would also remain functional.

- Unexpected delights, those that are neither consciously wanted nor missed when absent, like a spectacular view from the room window.

The goal of requirements setting is to understand and learn all three. Many of

the techniques used exploit different formalisms to learn what people need. They are based on the assumption that formalism is a tool to be used to clarify communications. Different or contradictory formalisms should be used so that diverse personalities can all understand proposed requirements and make their own comments and corrections.

Some of the diversities that need to be supported are:

left-brain vs right-brain personalities

actor vs object vs observer perspectives

verbal (written word/ formula) vs aural (spoken/ lecture) vs visual (pictures) vs tactile (touch) oriented personalities.

You need to provide clear presentations that are oriented towards all of the above. One of the most difficult for computer systems requirements is the tactile personalities. Many people, especially those in the machinery field, need something that they can touch and feel. They may have been trained to understand pictures that represent objects, but you can see their eyes light up and their brain engage when you hand them a physical thing to understand. The traditional software documents are very poor communication tools with tactile people. This is a very real risk when more and more machinery involves software components. The people with the best understanding of machinery are the ones for whom we provide the worst communications and understanding.

I suppose that this is vaguely related to the ongoing Formalism debate. I do know from both experience and the literature that men and women fall into all of the above categories.

Rob Horn horn%hydra@polaroid.com

[Rob, Thanks for the correction on the 14 vs 22 hours; what you describe is exactly as it was stated in the AW&ST article. I goofed.

A comment to stave off objections from the formalists: bad specs are not an "illustration of the problem with the overemphasis of formal proofs." They are an illustration of the problem with bad specs, which can effect system behavior -- irrespective of whether formal methods are used! PGN]

AT&T & voice recognition

<rmoonen@hvlpa.att.com>
Tue, 18 Jun 91 13:22 MDT

USA today had an article about a new AT&T product involving voice recognition. This product would enable a shop-holder to call a number, read aloud his merchant number, the credit card number, and the purchase price, and the customer would be billed.

I mean, how much more RISK'ier can you get?

--Ralph Moonen

More RISKS of stolen credit cards

Tsutomu Shimomura <tsutomu@NO-SENSE.LANL.GOV>
Mon, 17 Jun 91 19:46:23 -0600

About 18 months ago, I had my wallet stolen. Upon cancelling my credit cards and receiving replacements, I was somewhat surprised to discover that one them looked very familiar. It had an account number which was one greater than the one I'd just reported stolen (38XX-XXXXXX-XX11 instead of 38XX-XXXXXX-XX03; the final digit is a checksum, uniquely determined by the preceding digits). As it would be bad for a credit card thief to be able to trivially predict the account numbers of replacement cards, I had written this off to coincidence.

This card was lost last week, and I just received the replacement. The account number follows in the obvious pattern: 38XX-XXXXXX-XX29.

It is still possible that this sequence is coincidental, but it would seem most unlikely given the number of possible account numbers.

I hope the RISKS are recognized by the issuing bank (a large U.S. bank) before they are recognized by the credit card thieves.

---TS

Ethics, Drug Testing, and Hacking

Sanford Sherizen <0003965782@mcimail.com>
Tue, 18 Jun 91 14:46 GMT

I sometimes read the comics. Only during off hours, hidden behind a computer book, and in places where no adults can see me. The Boston Globe on Thursday, June 13, had a Dilbert comic strip that showed us how to balance some competing risks.

MAN TALKING TO HIS DOG. "It's an ethical dilemma...I support my company's goal of discouraging drug use, but the random drug testing policy is a violation of my constitutional rights. I'll get fired if I refuse the test. What is the ethical thing to do?"

DOG TO MAN. "Hack into their computer and change your boss's test results."

MAN USING THE COMPUTER AND TALKING TO DOG (AND HIMSELF). "Sometimes the straightest path is through the mud."

DOG RESPONDING TO MAN. "Good, rationalize it with an obtuse metaphor."

Out of the mouths of comic strips ...

Sandy

Legion-of-Doom Goes Corporate

"Craig Neidorf" <C483307@UMCVMB.missouri.edu>
Tue, 18 Jun 91 11:32:59 CDT

AFTER YOU'VE BEAT 'EM -- JOIN 'EM (Time Magazine, 24 June 1991, p.13)

After infiltrating some of America's most sensitive computer banks, is there any challenge left for a digital desperado? Only to go legit, say three former members of the notorious hacker group, the LEGION OF DOOM, who have quit the outlaw game to start Comsec Data Security. The Legionnaires claimed an 80% success rate in penetrating computer networks, and now they want to teach private industry to protect itself from the next generation of intruders. "You can't put a price tag on the information we know," says Scott Chasin, a Comsec partner. But they'll try.

(This article features a color photo of the three founding members:
Erik Bloodaxe, Doc Holiday, and Malefactor.)

Communications Privacy Statement

<cdp!mrotenberg@labrea.Stanford.EDU>
Fri, 14 Jun 91 10:25:08 PDT

STATEMENT IN SUPPORT OF COMMUNICATIONS PRIVACY
Washington, DC June 10, 1991

As representatives of leading computer and telecommunications companies, as members of national privacy and civil liberties organizations, as academics and researchers across the country, as computer users, as corporate users of computer networks, and as individuals interested in the protection of privacy and the promotion of liberty, we have joined together for the purpose of recommending that the United States government undertake a new approach to support communications privacy and to promote the availability of privacy-enhancing technologies. We believe that our effort will strengthen economic competitiveness, encourage technological innovation, and ensure that communications privacy will be carried forward into the next decade.

In the past several months we have become aware that the federal government has failed to take advantage of opportunities to promote communications privacy. In some areas, it has considered proposals that would actually be a step backward. The area of cryptography is a prime example.

Cryptography is the process of translating a communication into a code so that it can be understood only by the person who prepares the message and the person who is intended to receive the message. In the communications world, it is the technological equivalent of the seal on an envelope. In the security world, it is like a lock on a door. Cryptography also helps to ensure the authenticity of messages and promotes new forms of business in electronic environments. Cryptography makes possible the secure exchange of information through complex computer networks, and helps to prevent fraud and industrial espionage.

For many years, the United States has sought to restrict the use of encryption technology, expressing concern that such restrictions were necessary for national security purposes. For the most part, computer systems were used by large organizations and military contractors. Computer policy was largely determined by the Department of Defense. Companies that tried to develop new encryption products confronted export control licensing, funding restrictions, and classification review. Little attention was paid to the importance of communications privacy for the general public.

It is clear that our national needs are changing. Computers are ubiquitous. We also rely on communication networks to exchange messages daily. The national telephone system is in fact a large computer network.

We have opportunities to reconsider and redirect our current policy on cryptography. Regrettably, our government has failed to move thus far in a direction that would make the benefits of cryptography available to a wider public.

In late May, representatives of the State Department met in Europe with the leaders of the Committee for Multilateral Export Controls ("COCOM"). At the urging of the National Security Agency, our delegates blocked efforts to relax restrictions on cryptography and telecommunications technology, despite dramatic changes in Eastern Europe. Instead of focusing on specific national security needs, our delegates continued a blanket opposition to secure network communication technologies.

While the State Department opposed efforts to promote technology overseas, the Department of Justice sought to restrict its use in the United States. A proposal was put forward by the Justice Department that would require telecommunications providers and manufacturers to redesign their services and products with weakened security. In effect, the proposal would have made communications networks less well protected so that the government could obtain access to all telephone communications. A Senate Committee Task Force Report on Privacy and Technology established by Senator Patrick Leahy noted that this proposal could undermine communications privacy.

The public opposition to S. 266 was far-reaching. Many individuals wrote to Senator Biden and expressed their concern that cryptographic equipment and standards should not be designed to include a "trapdoor" to facilitate government eavesdropping. Designing in such trapdoors, they noted, is no more appropriate than giving the government the combination to every safe and a master key to every lock.

We are pleased that the provision in S. 266 regarding government surveillance was withdrawn. We look forward to Senator Leahy's hearing on cryptography and communications privacy later this year. At the same time, we are aware that proposals like S. 266 may reemerge and that we will need to continue to oppose such efforts. We also hope that the export control issue will be revisited and the State Department will take advantage of the recent changes in East-West relations and relax the restrictions on cryptography and network communications technology.

We believe that the government should promote communications privacy.

We therefore recommend that the following steps be taken.

First, proposals regarding cryptography should be moved beyond the domain of the intelligence and national security community. Today, we are growing increasingly dependent on computer communications. Policies regarding the appropriate use of cryptography should be subject to public review and public debate.

Second, any proposal to facilitate government eavesdropping should be critically reviewed. Asking manufacturers and service providers to make their services less secure will ultimately undermine efforts to strengthen communications privacy across the country. While these proposals may be based on sound concerns, there are less invasive ways to pursue legitimate government goals.

Third, government agencies with appropriate expertise should work free of NSA influence to promote the availability of cryptography so as to ensure communications privacy for the general public. The National Academy of Science has recently completed two important studies on export controls and computer security. The Academy should now undertake a study specifically on the use of cryptography and communications privacy, and should also evaluate current obstacles to the widespread adoption of cryptographic protection.

Fourth, the export control restrictions for computer network technology and cryptography should be substantially relaxed. The cost of export control restrictions are enormous. Moreover, foreign companies are often able to obtain these products from other sources. And one result of export restrictions is that US manufacturers are less likely to develop privacy-protecting products for the domestic market.

As our country becomes increasingly dependent on computer communications for all forms of business and personal communication, the need to ensure the privacy and security of these messages that travel along the networks grows. Cryptography is the most important technological safeguard for ensuring privacy and security. We believe that the general public should be able to make use of this technology free of government restrictions.

There is a great opportunity today for the United States to play a leadership role in promoting communications privacy. We hope to begin this process by this call for a reevaluation of our national interest in cryptography and privacy.

Mitchell Kapor, Electronic Frontier Foundation
Marc Rotenberg, CPSR
John Gilmore, EFF
D. James Bidzos, RSA
Phil Karn, BellCore
Ron Rivest, MIT
Jerry Berman, ACLU
Whitfield Diffie, Northern Telecom
David Peyton, ADAPSO
Ronald Plesser, Information Industry Association
Dorothy Denning, Georgetown University

David Kahn, author *The Codebreakers*
Ray Ozzie, IRIS Associates
Evan D. Hendricks, US Privacy Council
Priscella M. Regan, George Mason University
Lance J. Hoffman, George Washington University
David Bellin, Pratt University

(affiliations are for identification purposes only)

Dependable Computing: DCCA-3 call for papers

Carl Landwehr <landwehr@itd.nrl.navy.mil>
Tue, 18 Jun 91 13:20:11 -0400

DCCA-3 Call for Papers
3rd IFIP Working Conference on
Dependable Computing for Critical Applications
Can we rely on computers?

Splendid Hotel La Torre, Mondello (Palermo), Sicily, Italy
14-16 September 1992

Organized by
IFIP Working Group 10.4 on Dependable Computing and Fault Tolerance
In cooperation with
IFIP Technical Committee 11 on Security and Protection in Information Processing Systems
IEEE Computer Society Technical Committee on Fault-Tolerant Computing
EWICS Technical Committee 7 on Systems Reliability, Safety and Security
University of Pisa
Istituto di Elaborazione dell'Informazione del CNR, Pisa
Associazione Italiana per l'Informatica ed il Calcolo Automatico

General Chair
L. Simoncini
University of Pisa, Italy
Program co-Chairs
C.E. Landwehr
Naval Research Laboratory, USA
B. Randell
University of Newcastle upon Tyne, UK
Local Arrangements Chair
E. Ricciardi, IEI-CNR, Italy
Program Committee

J.A. Abraham, U of Texas, USA	B. Littlewood, City U, UK
P. Bishop, National Power, UK	T. Lunt, SRI Int'l, USA
A. Costes, LAAS-CNRS, France	J. Meyer, U of Michigan, USA
D. Craigen, ORA Corp., Canada	M. Morganti, Italtel, Italy
K. Dittrich, U of Zurich, Switzerland	S. Natkin, CNAM, France
H. Ihara, Hitachi, Japan	J-J. Quisquater, Philips, Belgium
R.K. Iyer, U of Illinois, USA	R.D. Schlichting, U of Arizona, USA
J.P. Kelly, U of California, USA	F.B. Schneider, Cornell U, USA
R. Kemmerer, U of California, USA	D. Siewiorek, Carnegie-Mellon U, USA

H. Kopetz, Technische U Wien, Austria L. Strigini, IEI-CNR, Italy
J.H. Lala, CS Draper Lab, USA I. Sutherland, ORA Corp, USA
K. Levitt, U of California, USA W.M. Turski, Warsaw U, Poland
Ex Officio
J-C. Laprie, LAAS-CNRS, France
IFIP WG 10.4 Chair

DCCA-3 is held in conjunction with the 12th IFIP World Congress (Madrid, Spain, 7-11 September 1992)

Increasingly, individuals and organizations are becoming critically dependent on sophisticated computing systems. In differing circumstances, this dependency might for example center on the continuity of service received from the computing system, the overall performance level achieved, the real-time response rate provided, the extent to which catastrophic failures are avoided, or confidentiality violations prevented. The notion of dependability, defined as the trustworthiness of computer service such that reliance can justifiably be placed on this service, enables these various concerns to be subsumed within a single conceptual framework with reliability, availability, safety and security, for example, being treated as particular attributes of dependability. This, the third IFIP Working Conference on the topic of Dependable Computing for Critical Applications, aims to continue the very successful tradition created by its predecessors (1989: Santa Barbara, California and 1991: Tucson, Arizona). It will thus provide a venue for the presentation and detailed discussion of research and advanced development relating to theory, techniques and tools for specifying, designing, implementing, assessing, validating, operating and maintaining critical computing systems. Of particular, but not exclusive, interest will again be presentations which address combinations of dependability attributes, e.g. safety and security, through studies of either a theoretical or an applied nature.

Submitting a Paper: Six copies (in English) of original work should be submitted by 31 January 1992, to the Program co-Chair:

Dr. Carl E. Landwehr
Code 5540
Naval Research Laboratory Tel: +(1) 202 767 3381
Washington, DC 20375-5000 Fax: +(1) 202 404 7942
USA E-mail: landwehr@itd.nr.navy.mil

Papers should be limited to 6000 words, full page figures being counted as 300 words. Each paper should include a short abstract and a list of keywords indicating subject classification. Papers will be refereed and the final choice will be made by the Program Committee. Notification of acceptance will be sent by 25 May 1992, and camera-ready copy will be due on 15 July 1992. A digest of papers will be available at the Conference, and hardbound proceedings will be published after the Conference as a volume of the Springer-Verlag series on Dependable Computing and Fault-Tolerant Systems.

Important Dates:
Submission deadline: 31 January 1992
Acceptance notification: 25 May 1992
Camera-ready copy due: 15 July 1992

Search RISKS using swish-e

THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

ACM Committee on Computers and Public Policy, Peter G. Neumann, moderator

Volume 11: Issue 95

Friday 28 June 1991

Contents

BackLogCabinJohnBridgeOutagesEtc.

"Peter G. Neumann" <neumann@csl.sri.com>
Fri, 28 Jun 91 15:29:25 PDT

I was East for a week, culminating in my COMPASS '91 Risk-of-the-Year talk at NIST on failures (both correlated and independent) that resulted in far-reaching problems, including the recent telephone cable cuts and switching problems. On the way back across the Cabin John Bridge toward Dulles Airport on Wednesday (having experienced enormous traffic delays in the opposite direction on Monday night due to construction), I heard the report of the 7-state east-coast phone slowage plus the simultaneous but presumed independent L.A. problem, both attributed to Switching System 7 protocol implementations.

(See below.) From the airport Wednesday, I tried a bunch of calls that would not go through. Having returned home, it is clear that from a RISKS point of view this was a bad time to have been away (there were over 250 messages awaiting me in the RISKS directory alone).

This issue is the first to try to catch up with the backlog in hopes of not generating the exponentially increasing backlog in response. We will as usual favor exciting new business, and go very slow on nth-order incrementals. I will also jack up the relevance razor ('n' Occam Dead?).

Some of the items in this issue will be "old hat" to those of you who are avid media mavens, but they are included anyway for archival purposes... and have been greatly foreshortened by the PGN Abstracting Service.

Programmer Accused of Plotting to Sabotage Missile Project

Peter G. Neumann <neumann@csl.sri.com>
Thu, 27 Jun 91 01:05:04 PDT

In San Diego, the former General Dynamics Corp. computer programmer, Michael John Lauffenburger, was arrested for allegedly planting a ``logic bomb,'' a type of virus that would have destroyed vital rocket project data. Lauffenburger's goal, according to a federal indictment, was to get rehired as a high-priced consultant to fix the damage he created. He quit May 29.

A fellow General Dynamics worker defused the plot by accidentally stumbling onto the logic bomb. Lauffenburger was charged with computer tampering and attempted computer fraud. If convicted, he faces up to 10 years in prison and a $500,000 fine. He pleaded innocent and was released on $10,000 bail.

[Source: Article by Laura Myers, AP Business Writer, 26 June 91]

Phone system becoming inherently less reliable?

Rodney Hoffman <Hoffman.El_Segundo@Xerox.com>
Fri, 28 Jun 1991 08:57:35 PDT

Excerpts from an article headlined PHONE OUTAGES SHOW HAZARDS OF NEW TECHNOLOGY by Jonathan Weber in the 28 June 1991 `Los Angeles Times':

"The massive telephone failures in the Los Angeles and Washington areas earlier this week stemmed from glitches in ... a specialized computer network that shuttles information about calls between telephone company switching offices.... The inherent complexity of an increasingly software-based phone system ... raises the prospect that the public telephone service may be inherently less reliable in the future than it has been in the past. Pacific Bell said Thursday that it had suspended further deployment of ... Signaling System 7 until the exact cause of the problem could be identified. It appeared ... that the [LA and Washington] problems ... were not identical, but both [were] attributed to breakdowns [in the] SS-7 equipment supplied by DSC Communications of Dallas."

[Explanations of expected benefits from the SS-7, including improved efficiency, capacity, speed, security, and new service possibilities such as "the controversial Caller ID."]

"The flip side of all this ... is that if the SS-7 system malfunctions, it begins sending incorrect information all over the network. Ross Ireland, general manager for network services at Pacific Bell, said Wednsday's incident was caused by a signaling system unit in downtown Los Angeles that inexplicably began sending out a flurry of wrong information about problems in the network, and ultimately shut itself down. Then there was a cascade effect, in which the other signaling system units began acting on the incorrect information. Finally, when people tried to make calls and couldn't, they kept trying, which created an abnormally high level of calling traffic and thus further exacerbated the problem.

"Because a phone network is so tightly integrated -- akin to one big computer -- it's very hard to locate and fix problems...."

[See also `Los Angeles Times,' John Kendall and Paul Lieberman, 27 June 1991: "By coincidence, service also was disrupted to 6.7 million telephone customers Wednesday in the District of Columbia, Maryland, Virginia, and parts of West Virginia.... [T]he trouble began in Baltimore during a routine modification of equipment procedure." [sic]]

[Officials at Chesapeake and Potomac said the problems were probably unrelated. Asked if hackers could have caused the problems, Ellen Fitzgerald, a spokeswoman for Chesapeake and Potomac, said she she had been assured that the system could not be penetrated. [!!!] But, she added, ``a few days ago I would have told you that what happened yesterday wouldn't happen.''

Terry Adams, a spokesman at the DSC Communications Corp., which made both systems, said company officials also discounted any connection between the failures. {From the NY Times article, 28 Jun 91. PGN}]

Another software-caused phone network problem

Fernando Pereira <pereira@klee.research.att.com>
Fri, 28 Jun 91 12:03:13 EDT

[...] May we be seeing here a situation in which market pressures to implement a complex new protocol is affecting design and test cycles for switching software?

According to the WSJ, the equipment and software in question are made by DSC Communications Co. The new protocol supports all those new services we hear so much about, such as caller ID, return call, call trace and various new business services. It's interesting to note that the January 1990 disruption in the AT&T network, involving an implementation of the same protocol, involved different (AT&T) hardware (4ESS) and software.

Fernando Pereira, 2D-447, AT&T Bell Laboratories, 600 Mountain Ave,

Murray Hill, NJ 07974 pereira@research.att.com

Mitsubishi sues AT&T for unsecure system

Rodney Hoffman <Hoffman.El_Segundo@Xerox.com>
Thu, 20 Jun 1991 09:49:43 PDT

According to an AP story carried in the 18 June '91 `New York Times', Mitsubishi is suing AT&T over a pbx system that was broken into by hackers who made thousands of illegal calls worldwide.

Mitsubishi contends that AT&T's System 85 Private Branch Exchange is not secure and that AT&T failed to warn Mitsubishi of the potential for unauthorized use. Mitsubishi seeks $10 million in punitive damages and a dismissal of $430,000 billed for 30,000 phone calls which Mitsubishi attributes to unauthorized users.

The pbx system, installed in 1988 and disconnected last year, permitted Mitsubishi employees to make calls on the company lines no matter where they were by using a 6-digit personal password. According to Mitsubishi, AT&T failed to diagnose the problem, and it was New York Telephone which finally told Mitsubishi of the possibility of system crackers.

Andrew Myers of AT&T declined to comment on the suit but said that under federal communications law, "customers are clearly responsible for both authorized and unauthorized service."

Cellular Phone Swindle

"Peter G. Neumann" <Neumann@csl.sri.com>
28 Jun 91 10:20:45 PST

The old sell-illegal-calls-at-a-discount scam has reemerged in Elmhurst, Queens, NY. High-tech mobile phone booths (cars) are very popular there, and draw crowds of people standing in lines to make their calls, often to Colombia or Peru. Each car has a doctored cellular phone chip containing an ID illegally set to some poor sap's valid ID. "The swindle has become so popular that legal cellular phone users in the area can rarely get access to an available phone line." Law-enforcement officials say that many of the calls are made to high-level drug dealers in Colombia. Many of the numbers dialed from Elmhurst match up with Colombian phone numbers that investigators have on file with the Federal Drug Enforcement Administration.

Metro One in Paramus, N.J., one of the two cellular carriers for New York City, estimated that it has lost more than $1 million a month from illegal calls transmitted from Elmhurst. Nationwide, such fraudulent calls cost the cellular phone industry about $700 million in 1990, according to Donald Delaney, an investigator for the NY state police. Industry officials put the figure much lower, at $100 million. [Source: Cars Using Rigged Cellular Phones Sell Illegal Overseas Calls, By Donatella Lorch, N.Y. Times News Service, 28 Jun 91]

Lauda Air crash (from "The European")

Pete Mellor <pm@cs.city.ac.uk>
Wed, 26 Jun 91 21:52:24 PDT

"The European" is a weekly news magazine published and distributed throughout Europe. Last week's issue carried the following article.

Boeing skipped essential test on Lauda crash jet By Mark Zeller, Paris

The Lauda Air 767 that crashed in Thailand last month was granted an airworthiness certificate without vital tests being carried out, the US Federal Aviation Authority has admitted. The FAA's administrator said that the aircraft's thrust reversers - which have been blamed for the crash - were only tested at low air speed with the engine set to idle because Boeing convinced the FAA that safety systems would prevent their accidental deployment in flight.

Examination of the wreckage and the pilot's cockpit voice recorder have [sic] now shown that one of the thrust reversers - used to slow an aircraft after landing - failed to lock in place when the plane was gaining height and accidentally shifted to a high-power setting, causing the plane to turn so rapidly that the tail was torn off the aircraft.

Under the FAA's rules, all jet aircraft which use the thrusters must be tested to ensure that accidental deployment would not cause the plane to crash. But the FAA's administrator, James Busey, in Paris for Le Bourget air show, said last week that the plane had not undergone a realistic in-flight test of the thrust reversers, which were designed and manufactured by Boeing and fitted to Pratt & Whitney engines. He disclosed that Boeing told the FAA that the plane's sophisticated flight control computers made an accidental inflight [sic] deployment of the thrust reversers impossible. The plane, owned by former Austrian racing driver Nikki Lauda, was en route from Bangkok to Vienna when it crashed in a Thai jungle three weeks ago, killing all 233 on board.

P&W confirmed that if the reverse thruster had not locked properly there would have been an indicator light advising the pilots. This warning light was heard [sic] being discussed by the pilots on the cockpit recorder shortly before the crash. Reading instructions from the Boeing manual, they took no action and continued to ascend. Seconds before the crash, the co-pilot shouted that a thrust reverser had been activated.

The tape concludes with a series of warning sirens, alarms, a snapping sound and then a bang. The wreckage of the plane was found in dense jungle in Thailand with one engine's thrust reverser deployed. The tail section was found several kilometres away. Asked about the possibility of an accidental deployment of a thrust reverser, Boeing spokesman Dick Kenny said: "It can't happen."

But a P&W representative, who wished to remain anonymous, said it was possible.

According to the engine-maker, Boeing was only now carrying out exercises to

find out what would happen if the reverse thruster deployed at high power. Boeing has refused to comment on these tests. Before the crash, there had already been at least one incident involving partial in-flight deployment of a thrust reverser on a Boeing 767. There have also been several similar incidents on 747s, but none of these led to a crash.

Peter Mellor, Centre for Software Reliability, City University, Northampton Sq.,London EC1V 0HB +44(0)71-253-4399 Ext. 4162/3/1]

Lauda Air and lithium batteries

Peter G. Neumann <neumann@csl.sri.com>
Sun, 23 Jun 91 11:47:08 PDT

Lauda Air disaster linked to potentially hazardous cargo

London, 23 June 1991 (dpa) - A potentially hazardous cargo may have contributed to the engine thrust reversal which caused a Lauda Air Boeing 767 to crash in Thailand May 26, killing all 223 people aboard, according to a British report Sunday. The Sunday Times, citing aviation safety experts, said the Austrian plane was carrying a shipment of cheap Chinese-made watches in a cargo hold, and that lithium batteries in one or more of the watches could have discharged, resulting in heat and possibly fire. Fire in the cargo hold could have affected computer wiring, causing the plane's port engine to shift into reverse thrust in mid-air. The cockpit's in-flight voice recorder, and inspections of the wreckage, showed that the engine inexplicably went into reverse, creating aerodynamic stresses which pulled the aircraft apart.

The wreckage also showed evidence of burn marks in one cargo hold, a phenomenon which specialists initially were unable to explain but later linked to the watch batteries, the report said.

The Sunday Times said speculation about the potentially dangerous batteries has already prompted several major airlines to slap a ban on such shipments from Hong Kong.

The report claimed that a South African Airways Boeing 747 was carrying a cargo of lithium-battery watches when it crashed into the Indian Ocean on a flight from Taiwan to South African in 1987, killing 159 people. Last year, a Cathay Pacific plane was forced to make an emergency landing after fire broke out in a cargo hold bearing a shipment of watches with lithium batteries, it said.

Videotape of the pilot discussing the crash of UAL 232

Mary Shafer <shafer@skipper.dfrf.nasa.gov>
Tue, 25 Jun 91 15:45:20 PDT

There's been a lot of discussion of the safety of fly-by-wire aircraft, so here's the discussion of an accident that very possibly would have been prevented were the DC-10 fly-by-wire rather than hydraulic.

On July 18, 1989, while in cruise at 37,000 feet, United Airlines Flight 232 suffered an uncontained engine failure of the #2 engine. This ultimately

disabled all three hydraulic systems, thus rendering the aircraft all but uncontrollable. The flight crew were able to guide the aircraft to Sioux City Gateway Airport by using a technique of "differential thrust." Approximately fifty feet above the ground, they lost control, which, when combined with a high descent rate, resulted in a violent crash. Of the 296 people on board, 184 survived. This included the flight crew.

On May 24, 1991, the captain of the airplane, Al Haynes, gave a speech on the crash to a gathering at NASA's Dryden Flight Research Facility. It was primarily concerned with the mechanics of controlling the aircraft, as well as disaster preparedness. The speech was recorded on video tape, and, with the consent of Al Haynes, has been made available to the net community via a somewhat ad hoc distribution system.

In the US:

Eric Thiele (ericth@i88.isc.com) will make you a copy of your own
for $4. Send a check to:

Eric Thiele
2000 Crown Point
Woodridge, IL 60517

Loaner copies will be distributed by a number of people. E-mail to
the person closest to you to get on the list. Don't be too surprised
if there's a little delay; this seems to be very popular.

barney@usc.edu -- Barney Lum -- Southern California
geoff@apple.com -- Geoff Peck -- Northern California
jle@hpfcla.fc.hp.com -- Jerry Eberhard -- Colorado
ericth@i88.isc.com -- Eric Thiele -- Illinois
mahler@usl.edu -- Steve Mahler --Louisiana
james@nueng.coe.northeastern.edu -- James Jones, Jr -- Massachusetts
rjg@umnstat.stat.umn.edu -- Robert Granvin -- Minnesota
gerry@n5jxs.jsc.nasa.gov -- Gerry Creager -- Texas
gjh@galen.med.virginia.edu -- Galen Hekhuis -- Virginia

A transcript has been made by Robert Dorsett (...cs.utexas.edu!cactus.org!rdd,
rdd@cactus.org) and is available by anonymous ftp on rascal.ics.utexas.edu.
It's located in the directory ~ftp/misc/av/safety-folder/SUX. A Macintosh
Microsoft Word-formatted file is in that directory, as well as a text-readable
version. The transcript has also been posted to sci.aeronautics, in two parts.

Australian readers will be able to borrow a copy from Mark Ferraretto
(mferrare@physics.adelaide.edu.au). There is some delay here, as I'm trying to
get it converted to PAL and it's taking some time.

If the demand is very heavy, I'll ask for a couple more volunteers and
get more copies circulating.

Mary Shafer shafer@skipper.dfrf.nasa.gov ames!skipper.dfrf.nasa.gov!shafer
NASA Ames Dryden Flight Research Facility, Edwards, CA

Searching the RISKS archives via WAIS

Garrett Wollman <wollman@emily.UVM.EDU>
Tue, 18 Jun 91 20:41:27 GMT-6:40

The folks at Thinking Machines have provided what is (so far as I can tell) a complete archive of RISKS for access by users of the Wide-Area Information Server technology, on their public-access Connection Machine WAIS server. I have been fiddling with this for a few days now, and I think it's extremely useful. For example, I can ask about "Clifford Stoll Wily Hacker" and it will come back with

```
263 2K  (01/12/89) :   Name this book  -- for a box of cookies!
^^^    ^^     ^^^^^^^^^^ ^^^^^^^^^^^^
Score   Size    Date      Headline
```

among others; I can then retrieve the *individual articles* from the server, save them on the local disk if I want, and much more! The server is only available from 9 to 9 ET, but it works really well, and is amazingly fast--there's more time spent on my end setting up question files and garbage-collecting in Emacs than during the actual search.

Anyway, I thought you might want to mention this in the masthead... The "source description file" is called "risks-digest.src" and is available from quake.think.com:

```
(:source
  :version  3
  :ip-name "cmns.think.com"
  :tcp-port 210
  :database-name "RISK"
  :cost 0.00
  :cost-unit :free
  :maintainer "ephraim@think.com"
  :description
"Connection Machine WAIS server.  Operated between 9AM and 9PM EST.

Risk Digest collection from the arpa-net list, but this is so far an unofficial
archive server.  It contains all issues, but is not updated automatically yet.
" )
```

Garrett A. Wollman - wollman@emily.uvm.edu

Search RISKS using swish-e

Report problems with the web pages to the maintainer