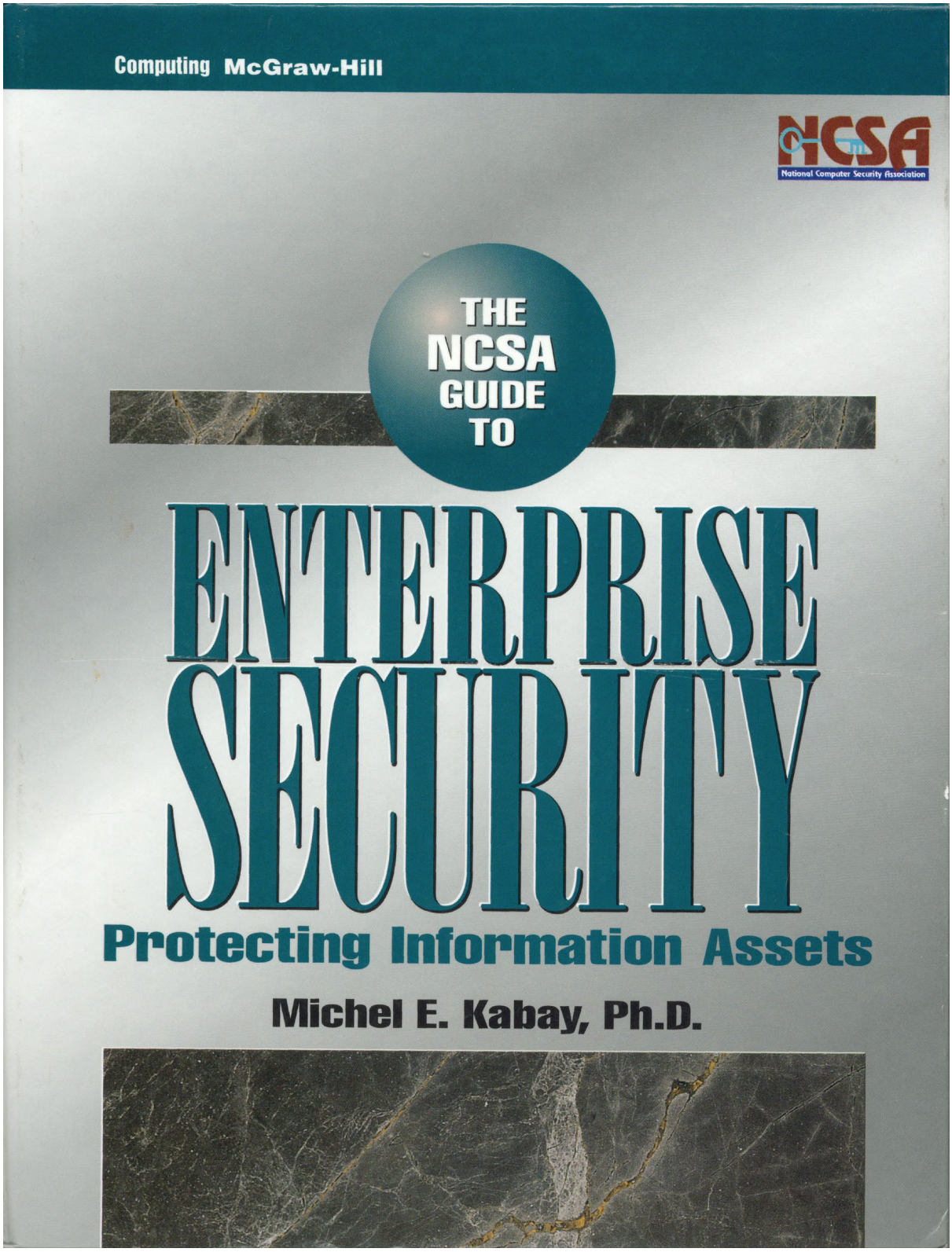

Copyright © 1995 M. E. Kabay. All rights reserved.

LAST MODIFIED: October 3, 1995

NCSA Guide to Enterprise Security

Table of Contents

Copyright © 1995 M. E. Kabay. All rights reserved.

Note: This is the original MS used for the textbook published in 1996. It differs from the published version in minor details.

Chapter 1: Introduction—protecting your information assets

Information is recognized as a strategic asset in today's competitive world. Threats to enterprise information systems must be met by appropriate responses. This text teaches the concepts, vocabulary and practice of information technology security for people immersed in the day-to-day tasks of managing information systems and also for students beginning their study of information security. The focus is on *enterprise* systems security, as distinct from the techniques required for specific platforms. There are many security texts available for learning the syntax required to define password length on a particular version of a local area network; this text explains why one should bother and how to convince managers and employees to care about the issue.

The **National Computer Security Association** serves as a clearing house for information about information systems security (infosec). This text is one of a series of *NCSA Guides* covering infosec topics. It serves participants in the NCSA *Information Technology Security* course and is suitable for practitioners involved in the management and application of information technology as well as college and university courses introducing information security to students at the undergraduate level and in business administration programs.

Objectives:

After studying this chapter, the reader should be able to
1. define the key concerns of enterprise systems security.
2. set information security in an historical context.
3. define the mission of the information security practitioner.
4. present industry statistics on the prevalence of computer and telecommunications crime.
5. describe methods for assessing vulnerability and risk.

What is enterprise systems security?

Enterprise systems are the computers and networks on which society increasingly depends for information management, process control, and direct control of equipment. The consequences of damage to or loss of information affects every sector of society. Not only commerce, education, and business are at risk; the political process itself may be attacked as computerized voting systems become more widespread.

We face an uphill battle whenever we try to convince management of the need for appropriate information systems security measures. Security is seen as a kind of insurance — it's necessary but boring. Insurance is thought of as an expense rather than as an investment. In contrast, this

Copyright © 1995 M. E. Kabay. All rights reserved.

text is based on the premise that enterprise systems security protects against disaster instead of simply paying for recovery.

There is a growing consensus: information security matters. In 1988, the Defense Advanced Research Projects Agency (DARPA) asked the Computer Science and Technology Board (renamed the Computer Science and Telecommunications Board of the NRC in 1990) for a study of computer and communications security issues affecting U.S. government and industry. The NRC's System Security Study Committee published its results in a readable and informative book, *Computers at Risk: Safe Computing in the Information Age.*

The Committee included experts with impeccable credentials, including executives from major computer vendors such as HP, DEC and IBM; from high-technology companies such as Shearson, Lehman, Hutton Inc. and Rockwell International; universities such as Harvard and MIT; and think tanks like the RAND Corporation.

A public misconception is the supposed divergence in focus of the military and of commerce: the military is usually described as concerned with external threats and the problem of disclosure, whereas businesses are said to worry more about insider threats to data integrity. On the contrary, the military and commerce need to protect data in similar ways. The differences arise primarily from (1) the sophistication and resources available to governments that try to crack foreign military systems; (2) the relatively strong military emphasis on prevention compared with commercial need for proof that can be used in legal proceedings; and (3) the availability to the military of deep background checks on personnel contrasted with the limits imposed on the invasion of privacy in the commercial sector.

Some of the more interesting general points raised by the NRC Committee include:

- because of the rapid and discontinuous pace of innovation in the computer field, 'with respect to computer security, the past is not a good predictor of the future;'

- embedded systems (those where the microprocessor is not accessible to reprogramming by the user; e.g., medical imaging systems) open us to greater risks from inadequate quality assurance (e.g., a software bug in a Therac 25 linear accelerator killed three patients by irradiating them with more than 100 times the intended radiation dosage);

- networking makes it possible to harm many more systems: 'Interconnection gives an almost ecological flavor to security; it creates dependencies that can harm as well as benefit the community....'

The Committee proposed six major recommendations, summarized as follows:

1) Push for implementation of generally accepted system security principles:

   - quality assurance standards that include security considerations;

   - access control for operations as well as data [e.g., any of the menu systems which preclude access to the operating system];

Copyright © 1995 M. E. Kabay. All rights reserved.

- unambiguous user identification (ID) and authentication [e.g., personal profiles and hand-held password generators]

- protection of executable code [e.g., flags to show that certain object modules are 'production' or 'installed' and thus apply strict access control that would prevent unauthorized modification — as found in configuration control systems]

- security logging [e.g., logging failed file-open attempts and logon password violations];

- assigning a security administrator to each enterprise;

- data encryption;

- operational support tools for verifying the state and effectiveness of security measures [e.g., audit tools];

- independent audits of system security by people not directly involved in programming or system management of the audited system;

- hazard analysis evaluating threats to safety from different malfunctions and breaches of security [e.g., consequences of tampering with patient data in hospitals].

2) Take specific short-term actions now:

- Develop security policies for your organization before there's a problem;

- Form and train computer emergency response teams before a crisis to respond to security violations or attacks;

- Use the Orange Book's (TCSEC, from the National Computer Security Center's Rainbow series) C2 and B1 criteria to define guidelines on security;

- Improve software systems development by applying better quality-assurance methods;

- Contribute to voluntary industry groups developing modern security standards and implement those standards in commercial software;

- Make effective security the default in software and hardware (make the user explicitly disable security instead of having to enable it).

3) Learn and teach about security:

- Build a repository of incident data;

Copyright © 1995 M. E. Kabay. All rights reserved.

- Foster education in engineering secure systems, both by encouraging universities to provide post-graduate training in security and urging industry to include security training as part of software engineering projects;

- Teach beginners about security and ethics in computer usage and programming [e.g., the NCSA is working on a research and development project to study beliefs, attitudes and behavior about ethical issues in computing in grade- and high-schools, colleges, and universities].

4) Clarify export control criteria and set up a forum for arbitration [hardware and software vendors have been complaining for years that the arbitrary imposition of severe export restrictions hampers American competitiveness in overseas markets without materially helping national security].

5) Fund and pursue needed research in such areas as

- security modularity: the effects on security of combining modules with known security properties;

- security policy models: more subtle requirements like integrity and availability are still not easily represented by control structures;

- cost estimation: there should be better ways of measuring the costs and benefits of security mechanisms in particular applications;

- new technology: networking, in particular, leads to greater complexity (e.g., how to connect 'mutually suspicious organizations');

- quality assurance for security: how to measure effectiveness;

- modeling tools: standards for graphical representations of security relationships analogous to the diagrams used in functional decomposition and object-oriented methodologies for program design;

- automated procedures: audit and monitoring tools for the data center management team;

- nonrepudiation: combining the need for detailed records of user actions with the values of privacy;

- resource control: how to ensure that proprietary software and data are used legitimately (e.g., preventing more than the licensed number of users from accessing a system, preventing software theft);

- security perimeters: how to reconcile the desire for network interconnection with limitations due to security requirements ('If, for example, a network permits mail but not directory services... less mail may be sent because no capability exists to look up the address of a recipient').

Copyright © 1995 M. E. Kabay. All rights reserved.

Chapter 2 of the NRC report, 'Concepts of Information Security,' is a 25-page primer on information systems security that could be handed to any manager who needs to be filled in on why you propose to spend so much money protecting the computer systems. The authors cover the fundamental aspects of information security (confidentiality, integrity and availability); management controls (individual accountability, auditing and separation of duties); risks (probabilities of attack or damage) and vulnerabilities (weak points); and privacy issues. In Appendix 2.2, the authors report an informal survey in April 1989 of 30 private companies in a variety of fields. The consensus among those polled included the following basic standards for information systems security (show these to your upper management if necessary):

- unique IDs, block access after a maximum number of incorrect logon attempts, show last successful access at logon time, make passwords and IDs expire;
- disallow embedded passwords during logon, make passwords invisible during entry, force minimum length (6), store passwords encrypted, scan proposed passwords to eliminate easy words;
- permit strict control over file access;
- detect and interdict viruses, certify software as virus-free, provide data encryption, overwrite deleted files to prevent recovery, force tight binding of production data to production programs;
- automated time-out for inactive sessions, unique identification of terminals/workstations during logon;
- network security monitoring, modem-locking, callback, automatic data encryption during transmission;
- audit trails including security violations;
- generally applicable security standards that could be used by vendors and users to evaluate different equipment and software for specific environments.

History

We live in a society so permeated with information technology that we forget that computation, tallying, and communication were once the domains of tiny elites. Entire civilizations rose and fell with a fraction of the information processing power we take for granted. Getting news from one end of the Roman empire to the other could take weeks; simple multiplication using Roman numbering required specialized training. However, despite the complexity of modern information processing, very little in modern information systems security would have been incomprehensible to an educated person from hundreds or even thousands of years ago.

Enterprise systems security is primarily a question of human behavior. The specifics of protecting specific equipment and programs are details of implementation. If people don't care

Copyright © 1995 M. E. Kabay. All rights reserved.

about security, even the most sophisticated and expensive security mechanisms will be wasted. The Post-It(R) sticky note is probably a greater threat to security in your organization than the teenaged cracker lusting to crack your access codes.

Throughout history, people have protected information against unwanted disclosure. Documents have been locked away — an early form of access control. Julius Caesar is said to have encoded secret documents by translating each letter to the one a fixed distance ahead in the alphabet — a monoalphabetic cipher. Writers and inventors created secret languages to protect themselves against persecution and theft.

Computing machinery has changed in form and power over the millennia. Concerns over security have changed as a result. About 5000 years ago, the Babylonian abacus was the pocket calculator of the time; security centered around protecting the device from theft and destruction.

In 1614, John Napier invented logarithms. For centuries, scientists and engineers depended on logarithmic tables for multiplications, divisions, powers and roots. Errors in these tables could cause severe failures. Security centered around accuracy.

William Oughtred's slide rule was as revolutionary in its day as the abacus and the pocket calculator were in their times. Physical protection and quality control during production were critical security concerns.

Physical security was paramount through the ages of the digital adding machine of Blaise Pascal (1642), Wilhelm Leibnitz' hand-cranked calculator (1673), the Jacquard Loom (1804) with its punched cards and Herman Hollerith's punch-card tabulator and sorter (1890). Owners of these expensive machines were primarily concerned with protecting them against damage and malfunction.

During the decades from 1930 to 1950, computing machinery was expensive and rare. Each model was unique: Vannevar Bush's Differential Analyzer (1930); George Philbrick's analog computer, Polyphemus; Bell Laboratories' Complex Number Calculator (1940); the Rockefeller Differential Analyzer (1942); Colossus (1943), with its 2000 vacuum tubes. The Harvard Mark I (1944), was fifty-one feet long and had a speed of 3 adds per second; it was used for 16 years to calculate ballistics tables for the U.S. Navy. ENIAC (1946) filled a room. In the early 1950s, it was commonly assumed that computers would never be widespread; after all, who but governments and a few large corporations could afford something as expensive as UNIVAC?

By the 1960s, the ‘glass house’ was the norm. Large computers were placed in glass-walled enclosures where proud executives could show them to visitors. Security still focussed on the physical parameters. Giant processors required adequate cooling, including cold water flowing through the equipment and air conditioners for the rooms filled with tape drives. Electrical power quality rose in importance; computer centre managers installed isolation transformers and uninterruptible power supplies. Cipher locks became the norm for controlling access to the hardware.

As data processing shifted towards information processing in the 1970s, data centre managers invested in logical access controls. The widespread use of multiple-user operating systems naturally led to concern over privacy and protection of each user's information. For example, the

Copyright © 1995 M. E. Kabay. All rights reserved.

MULTICS project at MIT in the mid 1960s included multi-level security that would allow Top Secret, Secret, Confidential and Unclassified data to reside safely on the same computer. UNIX is an offshoot of MULTICS; by the mid 1970s, it included powerful mechanisms for protecting files, memory structures, and system resources. Other proprietary operating systems (e.g., those for IBM mainframes and Digital Equipment Corporation's and Hewlett-Packard's midrange systems) also include extensive security mechanisms for file and system protection.

Remote computing started with the American Mathematical Society's meeting at Dartmouth College. On September 11, George R. Stibitz used a teletype link from Hanover, New Hampshire to the Complex Number Calculator at Bell Labs' offices in New York City to transmit problems and receive answers. Dartmouth College was also a pioneer in public time-sharing, with its student- and faculty written Dartmouth Time-Sharing System (DTSS) operating system for General Electric and Honeywell computers. By 1967, DTSS was supporting dozens of remote terminals, some of them linked by phone lines using modems. With the growth of networking came concerns over unauthorized listening (eavesdropping) and undetected modifications of the data stream.

The first microcomputers widely used in business were the IBM PCs, introduced in 1981. The introduction of the PC complicated security for managers who had become accustomed to centralized controls. Users and departments sometimes became rogue computer centers, functioning with non-standard hardware, software and procedures. Naive users knew nothing about backups and passwords; they left their systems open to intrusion without even thinking about corporate information. Disaster plans failed to include microcomputers, even though an increasing share of corporate information actually resided on little hard and floppy disks.

As distributed computing environments spread through the 1980s, new security challenges faced the growing number of local information systems managers. Local area networks were notoriously unstable, with periodic destruction of individual records, files or entire disk volumes. Untrained staff were assigned to do backups — and never thought to verify that their tapes and cartridges were actually readable. Concerns over privacy grew as governments, third-party data vendors and employers collected and shared information about more and more of the population. Computer foul-ups caused ever-greater consequences for organizations and individuals.

Now, in the mid 1990s, the developed world depends on information technology to a degree unimagined ever a few years ago. Cellular phones depend on computers to switch their signals from station to station. Automobiles can't run without microprocessors. Air traffic, ground transport, medical care, science, the military, consumer goods — all depend on information technology. Factories communicate automatically using EDI (electronic data interchange) so that suppliers can deliver materials and parts minutes before they are needed by the client. The use of computers and telecommunications links for communications has spawned a new sphere of human intercourse: cyberspace.

Cyberspace includes all the intangible communications that many of us depend on daily: from voice messaging systems through electronic bulletin boards, CompuServe and the Internet, digital telephony and virtual reality. Because of the storage and transmission of information about ourselves, we all extend at least partly into cyberspace. An error in a government computer can cause untold headaches for the victims of mistaken identity. An error in a commercial credit bureau can ruin an innocent person's chances of buying a car.

Copyright © 1995 M. E. Kabay. All rights reserved.

In contrast with earlier times, computer expertise is no longer rare. Some children begin using computers as early as three years of age. One computer expert in Los Angeles was writing programs at eight and had his first contract with a major computer manufacturer as a consultant at the age of thirteen. He was hired for his deep knowledge of the operating system for million-dollar computers. By the age of sixteen, he was a millionaire because of a utility program he wrote that was sold to thousands of customers at $5000 a copy.

Cyberspace has its villains, too. Disturbed, poorly socialized youths turn the world of electronic communications into the equivalent of the trash-strewn school yard. Childish criminal hackers — including children — enter poorly-protected systems and leave electronic graffiti in their wake. Misguided programmers amuse themselves by writing self-replicating programs called viruses which cause havoc on infected systems. Government agents invade privacy, interfere with citizens' rights to private communication and store intimate details of the lives of innocent and guilty alike.

Organized crime is implicated in a growing number of attacks on computer systems. In response, the FBI created a special unit, the Computer Analysis and Response Team (CART) in February 1994. CART consists of computer specialists devoted to the identification and preservation of computer data needed as evidence in criminal prosecutions.

Another area of concern is the growing use of the Internet and of value-added services such as CompuServe and America Online. Criminals have already taken advantage of the relative anonymity of cyberspace communications to engage in fraud.

The mission

The classic definition of information security is drawn from IBM Corporate Policy Number 130, as quoted in Carl B. Jackson's 1992 paper, ‘The need for security’ (see chapter notes).

> *Data security ... [involves] the protection of information from unauthorized or accidental modification, destruction and disclosure.’*

Another classic triad names confidentiality, integrity and availability. Donn B. Parker (affectionately known as the ‘Bald Eagle of Security’), a respected author, teacher and thinker in the security field and a principal in the SRI high-tech consultancy , has added to these possession, authenticity and utility.

Definitions

Protection means reducing the likelihood and severity of damage. Another way of putting this is that information security strives to reduce risks. It is not possible in practice to provide perfect prevention of security violations. Common sense suggests that the degree of protection must match the value of the data.

Copyright © 1995 M. E. Kabay. All rights reserved.

Information is protected by caring for its form, content and storage medium.

Unauthorized means forbidden or undocumented. The very concept of authorization implies classification: there must be some definition of which data are to be protected and at what level.

Accidents account for a major proportion of data damage. Accidents are due mostly to ignorance or to carelessness. Management must either hire well trained, knowledgeable staff or provide appropriate on-the-job training. In either case, part of the task facing all managers is to create, maintain and enhance motivation to do a good job. These basic management issues profoundly affect enterprise security.

Modification means changes of any kind. The ultimate modification is *destruction.* However, you can usually spot destruction fairly easily. With adequate backups copies, data can be restored quickly. A more serious problem is small but significant changes in data. The work required to find the changes is often a greater problem than the changes themselves. Computer viruses that wipe a hard disk identify themselves at once and can be removed quickly. Viruses that make small random changes can persist for months, ruin the integrity of backups, and end up costing the victim more than the virulent disk destroyers.

Disclosure means allowing unauthorized people to see or use data. Again, this word implies the need for a system of data classification. Who can see which data and when?

Confidentiality is a wider concept than disclosure. For example, certain files may be confidential; the data owner may impose operating system controls to restrict access to the data in the files. Nevertheless, it may be possible for an unauthorized person to see the names of these files or find out how often they are accessed. Changing a file's security status may be a breach of confidentiality. Copying data from a secure file to an unsecured file is a breach of confidentiality.

Possession means control over information. When thieves copy proprietary software without authorization, they are breaching the owner's possession of the software.

Integrity refers to internal consistency. A database is termed structurally corrupt when its internal pointers or indexes no longer correspond to the actual records they point to. For example, if the next record in a group is in position 123 but the index pointer refers to position 234, the structure lacks integrity. Surreptitiously using a disk editor to bypass security and alter pointers in such a data structure would impair integrity even if all the data records were left intact. Logical corruption occurs when data are inconsistent with each other or with system constraints. For example, if the summary field in an order header contains a total of $5,678 for all items purchased but the actual sum of the costs is $6,789 then the data structure is logically corrupt; it lacks integrity.

Authenticity refers to correspondence between data and what the data represent. For example, if a field is supposed to contain the number of parking violations cited by a specific police officer, then the field should not contain an outdated record of parking violations or the number of arrests by that officer. Another example of impaired authenticity is electronic mail sent with a false name. The only breach of security in such a case is loss of authenticity.

Copyright © 1995 M. E. Kabay. All rights reserved.

Availability means that data can be gotten to; they are accessible in a timely fashion, convenient, handy. If a server crashes, the data on its disks are no longer available; but if a mirror disk is at hand, the data may still be available.

Utility refers to the usefulness of data for specific purposes. Even if the information is still intact, it may have been transformed into a less useful form. Parker gives as an example the unauthorized conversion of monetary values in a database; seeing employees' salaries in foreign currency reduces the utility of the data. One of my colleagues was called in to help a firm whose source code had all been encrypted by a departing programmer. The programmer claimed to have done so to protect his ex-employer's security, but unfortunately claimed to have forgotten the encryption key. In a formal sense, the data were authentic, accurate and available — they just were not useful.

Threats to security

Enterprise systems are faced with two kinds of threat: people and disasters. People include managers, employees, service personnel, temporary workers, suppliers, clients, thieves, liars and frauds. Disasters include fire, flood, earthquake, civil disturbance and war.

The problem of ascertainment

The difficulty in describing the risk of facing these threats is that we lack proper statistical information about how often different types of damage occur. In statistical work, this difficulty is known as the problem of ascertainment. Most organizations are reluctant to admit, let alone publicize, successful attacks on their information systems. Would you be comfortable putting your money in a local bank after it revealed a million-dollar fraud? Would you use a law firm whose client records had been used for blackmail?

The second part of the ascertainment problem is that even if people were reporting all the computer crimes and accidents they knew about, we would still not know about the crimes and accidents that have not yet been discovered.

You should therefore doubt the accuracy of all statistics about the incidence of damage and threats to information systems.

Having said all that, we still have to explain to managers and others why we want to spend their money on security. The following graph shows rough guesses about the causes of damage to information systems. Think of it as a guide to the industry consensus.

<<insert Figure 1-1>>

As you can see, the most significant cause of damage is ignorance and carelessness. Fire is a serious threat; water damage often accompanies fires because of fire-suppression systems and fire fighters. Unhappy and dishonest employees account for most of the rest of the damage, with

Copyright © 1995 M. E. Kabay. All rights reserved.

viruses a distant last (and currently only for microcomputers). Outsiders are thought to account for no more than a sixth or so of all damage to information systems.

As usual, Donn Parker has a provocative and original view of these estimates. In a 1990 paper, he argued that, among other points,

- We don't know how much these attacks cost or many there are;
- We don't know what proportion of human threats are caused by outsiders;
- Most computer criminals are not so much greedy as unhappy or desperate;
- Computer viruses are still a negligible threat;
- Information stored in computer systems is safer than voice and print;
- Electronic eavesdropping is discussed by security experts because it is interesting, not because it happens;
- Computerization decreases business crime;
- Business security should emphasize the need-to-withhold, not the need-to-know.

Threats from insiders

Despite our qualms about ascertainment, there are nevertheless surveys which give us some idea of the situation. In 1984, for example, the American Bar Association Report of Computer Crime suggested that about 78% of all offenders in computer crimes were insiders who usually had authorized access to the systems they damaged or abused.

Disgruntled employees are the third most costly threat to information systems (after fire and water). This finding supports the view that management supervision and sensitivity to mood and morale are crucial foundations for effective security.

Unionization is an interesting question. In my own practice, I was asked by a manufacturing firm to serve as an expert witness in a planned court case. The employer wanted to oppose unionization of its computer operations staff. They felt that unionized employees would pose a threat were there ever a strike by the rest of the employees. The funds set aside for the legal battle were more than $100,000 (in 1986). I asked, ‘How do we know that unionization is bad for security?’ Accordingly, the company commissioned me to search the published literature for references to unionization and security.

There were 39 articles from the previous decade which dealt with the issue. Thirty-seven argued that, far from decreasing security, unionization could actually improve computer room security. Unionized employees were more willing than non-union staff to follow detailed, written security procedures. Detailed access control audit trails based on electronic card readers were more

Copyright © 1995 M. E. Kabay. All rights reserved.

acceptable than to some non-union staff. The company saved its $100,000, much to the displeasure of its lawyers.

Threats from outsiders

Outsiders are still an over-rated threat, but that threat may increase. Amateur criminal hackers are a minor problem, despite overblown media reporting. However, organized crime has a serious interest in personal information and computerized access to the monetary system. In addition, today's highly-competitive international market makes industrial espionage attractive to unscrupulous clients and lucrative to information thieves.

Computer criminals run some of the world's most highly secured systems: underground bulletin board systems (BBSs). Unlike the majority of BBSs, which are run by and for innocent cyberspace enthusiasts, criminal BBSs store and provide dangerous information about interesting victims — especially large, high-tech companies and financial institutions. In private areas restricted to those who have provided illegally-obtained information, these BBSs supply browsers with dial-up port telephone numbers, stolen telephone credit card numbers and bank credit card details. Some companies monitor these BBSs to keep track of their own vulnerabilities. For example, a school commission in Montreal found its dialup numbers and logon procedures in a local BBS.

Statistics

In a 1992 survey, USA Research, Inc. estimated about 700,000 cracker attacks per year in the United States. They calculated that there was a 1 to 2% probability that a given computer system would be attacked in any given year, and that the total damage (in lost productivity or sales) caused by criminal hackers was about $150 million in 1991.

Another area of growing abuse is phone fraud. Criminals steal phone services and resell them for enormous profits. James Snyder, Special Counsel for Investigations at MCI Telecommunications Corporation, addressed the Tele-Communications Association (TCA) 1992 Annual Conference in San Diego in September 1992. He warned that organized crime has found selling stolen phone services to be highly profitable and low in risk. Stolen access codes are being sold to other criminals for prices ranging from $3,000 to $10,000. According to Detective Don Delaney of the New York State Police, some thieves are earning more than $1M annually through call resell operations.

Lawrence Gessini, Director of the International Communications Association, addressed a special hearing of the Federal Communications Commission (FCC) in October 1992. His members reported theft of phone services amounting to $73.5 million over three years. The losses occurred in 550 cracker attacks on Customer Premise Equipment (CPE), including Private Branch Exchanges (PBXs), electronic Voice Mail Systems (VMSs), and Automated Call Distributors (ACDs).

Copyright © 1995 M. E. Kabay. All rights reserved.

In a recent DROIS report, Ira Herzoff estimates telecommunications losses an order of magnitude higher: $3M a day and annual losses in the $1B to $2B range.

Information systems managers must either work closely with managers responsible for telecommunications equipment or must consolidate voice processing with data processing into an integrated enterprise information systems directorate. It is no longer possible to consider information security without including voice systems.

Information warfare

Threats to information systems have largely been from accidents, as discussed above. However, for some organizations, the threats may change. The rise of global competition suggests that we are entering an age of *information warfare.*

Historical perspective

Throughout the history of conflict, technology has provided both weapon and target. When warriors mounted horses, their steeds provided both threat and vulnerability to opponents. To harm a single mounted man, one could attack his horse. To imperil a nation of horsemen, one could poison the herds. Armored knights fell to crossbows, but a more subtle attack was to destroy the foundries.

The defining technology of civilization as we enter the twenty-first century is the computer. Computers are pervasive, necessary and vulnerable to attack. Computers are linked to each other through networks; one cannot pick up a daily newspaper without reading about the data superhighway that will supposedly bring cyberspace into our living rooms and allegedly bring anything from good grades to the end of civilization.

Cultures that depend on information systems are vulnerable to information warfare. Information warfare consists of deliberate attacks on data confidentiality and possession, integrity and authenticity, and availability and utility. Information warfare can harm individuals, corporations and other private organizations, government departments and agencies, nation-states and supranational bodies. Information warfare is the extension of war into and through cyberspace. Military planners have recognized their dependence on information technology; some forces now speak of C4I: Command, Control, Communications, Computers and Intelligence. Protecting the technology of war against attack is an obvious extension of the military mind set; smart bombs require smart defenses. However, there is still no general agreement within the military establishments of the planet on the importance of protecting civilian as well as military information infrastructure. As for civil defense, there is a long way to go in including the information infrastructure as a necessary component of protection and recovery operations. Federal government departments are at least required to pay attention to the Government Security Policy, which mandates attention to security and business resumption planning (BRP); however, the task has barely begun in most departments. Provincial and municipal governments are at different stages of awareness and implementation of security and BRP. Finally, in the civilian arena, there are still many organizations which assume that disasters — let alone deliberate attack — will never strike.

Copyright © 1995 M. E. Kabay. All rights reserved.

Given the degree of dependence on information systems, it is essential to erect legal, organizational, and cultural defenses against information warfare.

Conceptual framework

Winn Schwartau has defined three levels of information warfare:

- Level one: interpersonal damage. Damage to individuals in recent cases includes impersonation in cyberspace (e.g., false attribution of damaging communications), appropriation of credit records (for fraud and theft), harassment (e.g., interruption of phone services) and loss of privacy (e.g., theft of medical records).

- Level two: intercorporate damage. Attacks on the financial and operational interests of corporations, government departments, universities and so on. Such attacks include industrial espionage, theft of services or money, and sabotage.

- Level three: international and inter-trading block damage. Destabilization of entire economies and societies. The techniques of information warfare levels one and two could be applied in a systematic way by terrorists, extortionists, or foreign governments.

The possibility that organizations will be the target of deliberate attack profoundly alters the process of *risk assessment,* which is the subject of the next section of this chapter.

Risk assessment

Most adults realize that insurance is a balance between costs and risks. We decide that the cost and inconvenience of replacing the oil in our car is minor compared with the consequences of dirty or insufficient oil. We pay insurance companies to protect our investments in houses and cars. Cellists insure their hands but not their lips; flautists insure their lips but not their hands. We have to know how much an asset is worth to us and then estimate the risks to that asset before we can make rational decisions about how much effort to expend in protecting the asset.

As in daily life, so in enterprise security. You cannot reasonably develop security policies and procedures without having a clear idea of the systems you want to protect and how valuable they are to you. In addition, you have to determine — or more usually, guess — the probability that your assets will be threatened.

Critical and sensitive data

There are two dimensions by which you have to measure the value of your information assets.

Copyright © 1995 M. E. Kabay. All rights reserved.

Critical information must be available and correct for your operations to continue at acceptable levels of efficiency and effectiveness. For example, in a hospital, clinical data provided at the bedside to treating physicians and nursing staff are critical: unavailability or inaccuracy may threaten people's health and even their lives. On the other hand, the hospital's internal newsletter, although valuable, is not critical.

Data have different degrees of criticality. Time, for instance, can make data less critical. Last week's backups are not as critical as yesterday's backups. Accounting data from five years ago may be important in case of an audit, but they are not as critical as this year's financial figures.

Sensitive information must be protected against unwarranted disclosure. A simple way of thinking about sensitivity is to ask whether you would be comfortable seeing specific information

- Only in a private memorandum to your boss;
- In a memo to your peers;
- In a memo only to the people you supervise;
- In a company internal newsletter;
- In the stockholders' annual report;
- On the evening television news.

Continuing our hospital example, a patient's age is less sensitive or confidential than the results of a test for Human Immunodeficiency Virus (HIV). Both data are more sensitive than an in-patient's room number in the hospital.

Quantitative risk analysis

Risk analysis is the process of developing a risk assessment. The assessment is a report showing assets, vulnerabilities, likelihood of damage, estimates of the costs of recovery, summaries of possible protection and costs, and estimated probable savings from better protection.

There are two broad classes of methodology for risk analysis: quantitative modeling and qualitative estimating. Quantitative risk analysis developed first, in the 1970s. It uses numerical estimates of cost and probability to generate models of expected loss and expected savings. There are many software packages available to aid users in developing such models, most have different assumptions and algorithms and produce risk assessments that differ in their details.

Qualitative risk analysis developed because of criticism that the quantitative methods were based on illusory precision. Qualitative methods explicitly use subjective judgement scales; e.g., severity ratings expressed as ranks from 1 to 10. The arguments over methodology obscure the fundamental uncertainty of all risk estimates. As Charles Pfleeger has pointed out in his

Copyright © 1995 M. E. Kabay. All rights reserved.

university text on information systems security, 'The precision of numbers is a red herring. Risk analysis is best used as a planning tool.' He emphasizes that all risk assessments should be used to point out areas of greatest concern; haggling over precise numbers is a waste of time.

Systematic risk analysis begins with a tabulation of enterprise assets. Although you can restrict this tabulation to information systems only, many analysts extend the process to cover global assets. In many organizations, this tabulation may be the first opportunity to develop a view of how much you depend on your information systems. Information systems assets include equipment, programs, data, documentation, supplies and staff. Investment in acquisition, development and maintenance of information systems have been studied by the staff of Computerworld for many years; the annual Premier 100 reports published in September list information systems expenditures as percentages of total revenue. Dun & Bradstreet Corporation, for example, was estimated in 1992 to have spent over 16% of its gross revenue on information technology. On average, the best users of computer systems spend 1% to 5% of their annual revenue on their information systems.

For each asset, you must brainstorm to imagine as many risks as you can. Look at physical damage, errors, criminal behavior by employees and other insiders, and breaches of security by outsiders. List the potential effects of compromising confidentiality, data integrity and system availability. Imagine the effects of unavailability for an hour, a day, a week. For example, a factory that uses computerized bar-code readers to keep track of production may continue operating for an hour or two if the bar-code reader system fails. However, it may shut down completely if the systems are unavailable for a day or more. Think of a university whose registration system depends on computer databases. Errors or accidents that delay registration for more than a week may cause serious problems for students and staff. Failure of a clinical information system for longer than minutes could put patients at risk of injury or death; it could also put doctors at risk of malpractice suits and the hospital administrators at risk of prosecution for negligence.

The preliminary study may lead to better awareness of security issues among your staff. One of the most important contributions of risk analysis to better security is that every employee can contribute insights. The people best positioned to evaluate risks and consequences are those who use the tools under evaluation.

Another advantage of undertaking such a study is that it is the basis not only of improved security policies and procedures, but it also serves as the first step in disaster prevention, mitigation and recovery planning.

The hardest part of quantitative risk analysis is estimating probabilities. Actuarial data compiled by insurance companies can help you estimate risks; however, all such general figures must be taken as guides, not eternal truths. The probability of loss is strongly influenced by your own situation. For example, the risk of water damage may be (say) 1% per year in general — but if your buildings are located near a badly-constructed dam, your probability is higher than average by an unknown amount.

Recently, spreadsheet add-in packages have appeared to help model risk using appropriate probability distributions. These tools allow risk managers to apply Monte Carlo simulation

Copyright © 1995 M. E. Kabay. All rights reserved.

techniques, in which the probability of complex events is estimated by repeated sampling of more elementary components linked in a causal chain.

Some risk analysis packages include extensive databases of actuarial data and expert knowledge about different industries. You can install modules dealing with banking, manufacturing, insurance, federal and state governments, physical security, microcomputers, telecommunications, computer applications, and disaster recovery. Costs of such packages range from less than $100 per copy into the $20,000 range. The more expensive packages use artificial intelligence techniques, including fuzzy logic, to model your risks, costs of counter measures, and annualized savings. The sophistication of reports is also correlated with cost; the more costly packages provide several levels of reporting (e.g., executive summary and decision support with graphics and tabular details in the technical analyses). Because the field continues to evolve, you should consult reviews in DROIS and in the technical press before choosing a specific package.

Qualitative risk analysis

Many of the risk analysis packages include qualitative measures. However valuable, these models nonetheless provide less support for the monetary estimates that managers have come to expect from their information systems staff. It is ironic that many people would rather have bad estimates expressed as dollar figures than better estimates couched in qualitative terms.

Risk analysis in the age of information warfare

Threat and risk assessment has traditionally dealt with the probability of Acts of God. Fire, flood, earthquake, even burglary can be looked at as involving random events. However, in today′s competitive and unethical environment, the likelihood of being attacked is an unknown and unknowable function of an organization′s attractiveness and preparedness. The most successful and least secure organizations will be victim. Faced with a choice between an unkempt hovel and a palatial residence, a thief will try to rob the more lucrative target. But suppose a thief sees two palatial residences: one has Doberperson Pinchpersons (politically correct guard dogs) roaming the space inside a 3 meter fence, infrared motion detectors and a direct link to a security company; the other has locks on the doors. There′s not much doubt about the selected victim.

In my courses, I like to explain the principle of appropriate defense with a story. Two hikers are walking happily along a trail in Alberta when they come upon a huge grizzly bear. Turning tail, they being running down the trail. One huffs to the other, “This is (pant, gasp) crazy. We can′t outrun a grizzly bear! They can run 30 km an hour and climb trees!@ The other gasps, “I don′t have to outrun the grizzly bear (pant, pant). I just have to outrun *you.”*

To pursue the analogy, unprepared organizations may be in the position of hikers unaware that they are covered in honey when there are bears on the path. Risk assessment in the age of information warfare must include self-examination from the point of view of a competitor. Organizations must recognize when they are attractive to predators and must then make themselves unattractive targets for espionage and sabotage.

Copyright © 1995 M. E. Kabay. All rights reserved.

Summary

The pervasive use of information technology in the developed world has brought with it a widening need for security. Information security includes concerns for protecting information assets from unauthorized or accidental modification and disclosure. Security includes the need for preserving confidentiality, integrity, availability, utility and authenticity. Because of under-reporting of computer crime, we should mistrust statistics about attacks and accidents that damage information. The consensus is that the most serious risks to information systems come from authorized personnel who are either inadequately trained, inattentive, angry or dishonest. Criminal hackers and viruses are significant but over-rated threats. Information security policy development must begin with a thoroughgoing analysis of sensitivity and criticality. Risk analysis software can bring artificial intelligence and industry expertise to bear on the production of detailed risk assessments. Human factors make risk analysis more difficult in the age of information warfare.

Copyright © 1995 M. E. Kabay. All rights reserved.

CHAPTER NOTES

These notes represent details of where to look for more information. Since this text is not intended as a scholarly review of the field, but rather as a guide for practitioners, I have not interrupted the flow of your reading by inserting numbered footnotes or endnotes. The notation v(n):p (as in PC-Computing, 3(8):122) means volume v, number n, page p (thus volume 3, number 8, page 122 and following). As much as possible, I have restricted the choice to readings from 1990-1995.

1. System Security Study Committee, Computer Science and Telecommunications Board, Commission on Physical Sciences, Mathematics, and Applications, National Research Council (1991). *Computers at Risk: Safe Computing in the Information Age.* National Academy Press (2101 Constitution Ave NW, Washington, DC 20418). ISBN 0-309-04388-3 (paper). xv + 303 pp. Bibliography, appendices. Also available from the National Computer Security Association (NCSA).

2. National Computer Security Center (NCSC). The "Rainbow Series" includes (among other titles):

   Orange Trusted Computer System Evaluation Criteria

   Red Trusted Network Interpretation
   Light Green Password Management Guide

   Dark Green Glossary of Computer Security Terms

   Dark Blue Magnetic Remanence Security Guidelines

   Yellow Guidance for Applying the Department of Defense Trusted Computer System Evaluation Criteria in Specific Environments

3. One of the most important services available for the information systems security professional is *Datapro Reports on Information Security* (DROIS). These reports, updated monthly, are an invaluable source of up-to-date information. Three large binders contain over a thousand pages of clear, detailed reports from journals, conferences and books. Many reports are especially written for DROIS and are unavailable elsewhere. You can reach Datapro Research Group at 1-800-928-2776 in the US and 1-416-298-1177 in Canada. Headquarters: 600 Delran Parkway, Box 1066, Delran, NJ 08075. DROIS is now available on CD-ROM.

4. There is a continuing debate in the technical community about whether it's too late to salvage the word *hacker* now that the popular press has demonized it. As a 15 year old learning assembler in 1965, I would have qualified as a *hacker* in the honorable sense of the word. We techno-nerds would never have sunk so low as to be *criminal hackers.* One of the terms being tossed around the Internet to describe criminal hackers include *cockroach,* which suggests the contempt in which these creeps are held by honest people.

Copyright © 1995 M. E. Kabay. All rights reserved.

Personally, I feel that the cockroach has a long history on the planet and that its name should not be so besmirched.

5. Many of the references in this and subsequent chapters were found through the *Computer Database Plus* offered by Ziff Communications Company through the CompuServe value-added network. This bibliographic database includes over 530,000 references to the computer trade press. More than two-thirds are *full text* articles. Costs are modest: $0.25/minute connect time, $2.50 for each full-text article downloaded, $1.50 for articles that have no abstract, and $1.00 per abstract.

   The breakdown of articles indexed by date is as follows:

   1994: 76,557
   1993 73,680
   1992: 83,148
   1991: 78,705
   1990: 68,979
   1989: 62,029
   1988: 47,405
   1987: 33,580

   Selection criteria permit Boolean operators (AND, OR, NOT) in several fields including:
   Key Words (words in article titles, subject headings, company or product names)
   Subject Headings (including lookup and menu functions)
   Company Names
   Product Names
   Publication Names (including a list of all publications and their addresses)
   Publication Dates (1987 to present)
   Article Types (e.g., opinion, tutorial, buyers' guide)
   Words in Article Text.

   Lookups rarely take more than a few seconds. The number of hits is shown and a menu of article titles of possible interest is available for inspection. Specific articles can then be read or downloaded.

   Everyone who joins the National Computer Security Association receives a free CompuServe membership kit and can participate in the NCSA security section.

6 Excellent overviews of computer crime and security (listed from most recent to oldest):

Flaherty, F. (1994). Cyberspace swindles: old scams, new twists. *New York Times* 143(July 16, 1994):25

Kelly, S. (1995). Highway to Hell? *Computer Weekly* (March 2, 1995):30

Coffee, P. (1994). Developers must guard against fraud, snoopers. *PC Week* 11(30):1

Newsome, C. (1994). Data security threat as crime increases. *PC User* (246):14

Copyright © 1995 M. E. Kabay. All rights reserved.

Jackson, C. B. (1992). The need for security. DROIS report #IS09-100-101. This report contains a wealth of valuable insight and details of practical implementation.

Herzoff, I. (1992). Voice network fraud. DROIS report #IS35-200-101. Mr Herzoff provides the address of the Communications Fraud Control Association / 2033 M Street NW / Washington, DC 20036; tel. 202-296-3225.

Snyder, J. F. (1992). Toll fraud today. *Proceedings* of the 1992 Annual Conference, Tele-Communications Association; San Diego, 21-25 Sept. P. 415.

USA Research, Inc. (1992). *IPA Computer Virus and Hacker Study.* 4 volumes, 300 pp. USA Research, Inc. / Technology Company Information Reports / 4380 SW Macadam Avenue / Portland, OR 97201-6406 / Tel. 503-274-6200 / Fax 503-274-6265.

NCSA (1991). *Computer Virus Prevalence Study.* Available from the National Computer Security Association.

Parker, D. B. (1991). Restating the foundation of information security. Paper presented at the 14th National Computer Security Conference in Washington, D.C. (October 1991). Reprinted as DROIS report #IS09-125-101. This paper lays out Parker's thoroughgoing revision of the classic goals of information security.

Parker, D. B. (1990). Seventeen information security myths debunked. *ISSA Access* 3(1):43. Reprinted as 'Information myths explained,' in DROIS report #IS09-150-101.

Manning, R., D. Pearlman, & D. Steinberg (1990). To catch a hacker. *PC-Computing* 3(8):122.

7 Risk analysis software

Classe, A. (1994). Hazard warning. *Computer Weekly* (Nov 17, 1994):56

Waring, B. (1994). Crystal Ball 3.0: Excel add-in provides intelligent risk analysis. *MacUser* 10(10):64

Duncan, R. J. (1992). Risk analysis software: overview. DROIS #IS21-001-101. This report includes detailed comparisons of 13 packages, including general information about the product and its sales, host requirements, source code, operation, risk analysis features, report generations, support and prices.

Ozier, W. (1992). Issues in quantitative versus qualitative risk analysis. DROIS #IS20-250-101. Will Ozier summarizes the metrics available for both approaches to risk analysis.

Pfleeger, C. P. (1991). Security in Computing. Prentice-Hall (Englewood Cliffs, NJ). ISBN 0-13-798943-1. Chapter 13, pp. 457-470, includes several examples of quantitative risk analysis.

Copyright © 1995 M. E. Kabay. All rights reserved.

8 On information warfare:

Kabay, M. E. (1995). M. E. Kabay on Information Warfare. *Computerworld* 29(12):48 (insert)

Schwartau, W. (1994). *Information Warfare: Chaos on the Electronic Superhighway.* Thunder's Mouth Press, New York. ISBN 1-56025-080-1. 432. Index.

9 The NCSA Forum on CompuServe [now defunct] provides an excellent opportunity for professional discussion of information security issues with security experts and other managers and users of computer systems. As of May 1995, there were over 29,000 participants in the Forum.

Sections include

1	About NCSA	Information about the Association; NCSA events
2	Ethics/Privacy	Protecting personal information in cyberspace; policy issues such as censorship, anonymity
3	News/Case Studies	Security events, computer crimes, fraud using computers
4	Anti-Virus Support	News of recent outbreaks, support in diagnosis of virus attacks and damage repair
5	Disaster Recovery	Disaster prevention, mitigation, and recovery planning; postings from Internet newsgroups dealing with natural disasters; discussions of quality assurance failures in software and hardware
6	Encryption	Technical, policy, and regulatory issues involving encryption; support for PGP users; front-ends for encryption packages
7	PL/MAC/LAN	Access control policies and techniques; logging; software license compliance; network monitoring
8	UNIX/Internet	Firewalls, bug reports, fixes
9	Telco Security	Toll fraud, voice mail, fax security
10	Crime/Law/Policy	Legal initiatives, statutes; corporate policies
11	Electronic Commerce	Electronic data interchange, funds transfers
12	Host/Single Signon	Large system security; RACF, ACF/2
13	Product Info/PR	Infosec product descriptions, press releases
15	Auditing	Systems auditing, log files, quality assurance.
16	Certification/Training	Professionalization, education, teaching
17	BBS/Sysop	Security for bulletin board system operators
18	UNCLASSIFIED	Friendly area for casual discussions
19	Book Reviews	The latest security books
20	Special Topics	Recently set aside for Pentium Bug; available for other hot topics as required
21	Electronic Seminar	Interactive seminars on security
22	Security Management	American Society for Industrial Security (ASIS) area

Copyright © 1995 M. E. Kabay. All rights reserved.

23	PRISM Members Only	Reserved area for subscribers to special NCSA services

<<end of chapter>>

Copyright © 1995 M. E. Kabay. All rights reserved.

LAST MODIFIED: 2002-04-26

NCSA Guide to Enterprise Security (1996)

FILE: 02 Crime.DOC

Chapter 2: Computer crime techniques and counter-measures

After studying this chapter, the reader should be able to

1. Form an informed opinion about the advisability of publishing and discussing computer crime techniques.

2. Recognize, define and illustrate the most common computer crime techniques.

3. Describe and develop appropriate defenses for each threat.

Computer viruses are discussed in Chapter 3.

Why study crimes?

In public discussion of crime techniques, someone always asks whether it's prudent to talk about crime so openly.

The arguments against such discussion fall into two classes. Won't people get ideas? That is, will discussing crime lead to more crime? And won't descriptions of how to commit a crime teach criminals how to be more effective? That is, will discussing crime make crime prevention harder?

Yes, it is possible that describing criminal acts will suggest to people on the borderline of honesty that they could carry out a similar crime. Copycat crimes are a well known consequence of newspaper stories about any unusual crime. The romantic image of crackers in such movies as *War Games* and *Sneakers* may indeed contribute to the delinquency of computer-literate minors.

However, when computer crime techniques are put in perspective, it is hard to believe that the overall effect is to encourage crime. When I teach the three-day *Information Systems Security* course on which this text is based, I repeatedly stress that the criminals who abuse information systems and use computers in their crimes are enemies of society. Embezzlers steal the life savings of innocent victims; thieves and swindlers and extortionists increase the costs of goods and services for everyone; and blackmailers victimize the weak and push them into despair.

After Craig Neidorf was accused in February 1990 of publishing stolen information about BellSouth 911 operations, security specialists engaged in vigorous debate about the issue of publishing computer crime techniques. Long articles in the Communications of the ACM provides extensive discussion by leaders in the field. Some argue that no limitations should be imposed on the publication of any information; others feel that society has a right to restrict the dissemination of dangerous information.

Copyright © 1996, 2004 M. E. Kabay. All rights reserved.

Chapter 9 includes a detailed discussion of the BellSouth case and others.

As you read this book, be on guard against the seductive lure of crime. Some criminal techniques are so clever and so original that it's easy to fall into the trap of admiring the criminals. Remember that the criminals consider themselves better than you and me; they put themselves above the norms of decency and kindness that most of us strive for. Computer criminals are often intelligent, but at a fundamental level they are despicable and defective human beings.

If that mantra doesn't sour your admiration for crooks, nothing will.

The second question concerns the danger of showing criminals weaknesses in security. Security practitioners have struggled with this problem for years. In the first place, much of the discussion to follow centers on carelessness and lack of training, not on criminality. Helping managers and employees tighten up their attention and improve their policies to reduce accidents will not aid criminals.

Another answer has been commonplace in military doctrine since some nameless protohuman decided to fight back against the local top carnivore: security is by its nature a defensive proposition. There are many ways of breaching barriers; the foe need find any one of the weak spots, but the defenders must guard the entire perimeter. Security professionals do the best they can given constraints of time and money, but people determined to overcome the defenses can spend as much time and effort as they wish to locate weak spots.

Another point in defense of teaching is that a course or discussion of counter-measures need not provide solace to the enemy. Discussing forgery techniques, for example, can go as far as mentioning that color copiers and scanners make it easy to counterfeit some currencies and official documents. However, it doesn't take a rocket scientist to realize that imaging technology can be abused. Simply pointing out the problem does not constitute a primer in the techniques, especially when coupled with admonitions to be more skeptical about official-looking documents of all sorts. The balance of risks and benefits seems clearly on the side of benefits.

Giving details sufficient for emulation is another matter, however.

A controversial example of providing too much information revolves around the publication of detailed source or object code for functional viruses. In 1991, someone published a book containing detailed instructions on how to create functional viruses. The book included source code. The publication of this manual caused a furor in the anti-virus product developers' community. Some prominent anti-virus workers proposed to assault the author; others reviled him to his face and on the electronic networks.

I and others feel that it is unnecessary to give such detailed instructions to people interested simply in defending themselves against viruses. Very few people will be able to use detailed information about virus code for constructive purposes. It is enough for most people to rely on shareware and commercial anti-virus products and let experts handle the dangerous code under conditions of tight security and isolation.

After all, no one seriously proposes that anthrax bacilli or polio virus be freely distributed for amateur microbiologists.

Copyright © 1996, 2004 M. E. Kabay. All rights reserved.

In March of 1993, I published a short opinion piece in *Network World* entitled, "Virus Code and the First Amendment." I argued that even if we admit that virus code is speech, it need not be protected by First Amendment rights to free speech. In any case, I proposed, virus code is not speech any more than punched paper tapes for milling machines are speech, and so the whole issue of First Amendment rights for publishers of virus code is irrelevant. Publishing virus code irresponsibly or with malicious intent should be punishable.

This article provoked the most mail I have ever received for a publication. Within days, my electronic mailbox on the Internet was inundated with vigorous discussion, mostly opposing my proposals on (I admit) reasonable grounds. The most striking argument among the 100K bytes of correspondence I received was that hiding knowledge is not an effective defense.

My own position is that I will not provide workshops in how to commit computer crimes. The information I provide in my writings and my teaching helps participants defend themselves but does not materially aid them in honing criminal techniques.

A computer crime glossary

Before plunging into details, it's good to have an overall view of the area you're about to study. Here is a brief glossary of computer crime techniques.

BACK DOOR: secret (undocumented), hard-coded access codes or procedures for accessing information. Some back doors exist in commercially-provided software packages; e.g., consistent passwords for third-party software accounts. Alternatively, back doors can be inserted into an existing program to provide unauthorized access later. Such a modified program is a kind of Trojan Horse.

DATA DIDDLING: modifying data for fun and profit; e.g., modifying grades, changing credit ratings, altering security clearance information, fixing salaries, or circumventing book-keeping and audit regulations.

DATA LEAKAGE: uncontrolled, unauthorized transmission of classified information from a data center or computer system to the outside. Such leakage can be accomplished by physical removal of data storage devices (diskettes, tapes, listings) or by more subtle means.

IMPERSONATION: pretending to be authorized to enter a secure location. Examples include swaggering into a site equipped with what look like tool kits of the manufacturer of computer equipment, or pretending to be a janitor.

LOGIC BOMB: similar to time-bomb, but the "explosion" occurs because of a particular logical condition, such as not having the author's name in the payroll file. Logic bombs are a kind of Trojan Horse.

Copyright © 1996, 2004 M. E. Kabay. All rights reserved.

PIGGYBACKING: entering secure premises by following an authorized person through the security grid; also unauthorized access to information by using a terminal that is already logged on with an authorized ID (identification).

SABOTAGE: the word comes from the French for wooden shoe; it was used to describe clumsy work. In the late 19th century, it became a tactic used by militant trade-unionists. It now means any deliberate damage to operations or equipment.

SALAMIS: technique of accumulating round-off errors or other small quantities in calculations and saving them up for later withdrawal; usually applied to money, although it could be part of an inventory-theft scheme.

SCAVENGING: using discarded listings, tapes, or other information storage media to determine useful information such as access codes, passwords, or sensitive data. Also known as *dumpster diving.* Listing a source program containing hard-coded passwords, for example, would be profitable for a computer crook.

SIMULATION: using computers to simulate a complex system in order to defraud it; e.g., inventing transactions to produce a pre-arranged bottom line in a financial report.

SUPERZAPPING: using powerful utility software (e.g., QUERY, DISKEDIT) to access secure information.

TIME BOMB: program or batch file waits for a specific time before causing damage. Also known as time-bombs; used by disgruntled and dishonest employees who find out they're to be fired. Time bombs are a kind of Trojan Horse.

TROJAN HORSE: innocent-looking program that has nefarious functions. So called by reference to Odysseus' wooden horse filled with soldiers that helped to capture Troy. Typical Trojan Horse programs might alter data in a particular way, record passwords for later inspection, or even put together another program from pieces stored inside other Trojan Horses.

VIRUS: similar to a worm, but residing inside a bona-fide program. A virus transforms an ordinary program into an unintended Trojan horse. Viruses infect executable code such as programs (e.g., .EXE and .COM files under DOS)and boot sectors on disks and reproduce. So called by analogy with biological viruses, which subvert the functions of normal cells.

WIRETAPPING: eavesdropping on data or voice transmissions. Using a portable TV set and about $50 worth of parts from an electronics store, a knowledgeable person can see and record everything being transmitted between host and terminal on an asynchronous communications channel (e.g., a twisted pair carrying RS-232 traffic). From intercepting, it's a short step to modifying: inserting false messages into the data stream that look like bona fide transactions. Wiretapping will be discussed in this text in the chapters on network security.

WORM: program which spreads through a computer system or network, either by replicating itself like the INTERNET worm of late 1988 or by transferring a copy of itself elsewhere and destroying the previous version.

Copyright © 1996, 2004 M. E. Kabay. All rights reserved.

Sabotage

Thomas Whiteside catalogs a litany of physical attacks on computer systems dating back to the 1960s:

- 1968, Olympia, WA: an IBM 1401 in the state is shot twice by a pistol-toting intruder;
- 1970, University of Wisconsin: bomb kills one and injures three people and destroys $16 million of computer data stored on site
- 1970, Fresno State College: Molotov cocktail causes $1 million damage to computer system
- 1970, New York University: radical students place fire-bombs on top of Atomic Energy Commission computer in attempt to free a jailed Black Panther
- 1972, Johannesburg, South Africa: municipal computer dented by four bullets fired through a window
- 1972, New York: magnetic core in Honeywell computer attacked by someone with a sharp instrument, causing $589,000 of damage
- 1973, Melbourne, Australia: antiwar protesters shoot American firm's computer with double-barreled shotgun
- 1974, Charlotte, NC: Charlotte Liberty Mutual Life Insurance Company computer shot by a frustrated operator
- 1974, Wright Patterson Air Force Base: four attempts to sabotage computers, including magnets, loosened wires, and gouges in equipment
- 1977, Rome: four terrorists pour gasoline on university computer and burn it to cinders.
- 1978, Vandenburg Air Force Base, California: a peace activist destroys an unused IBM 3031 using a hammer, a crowbar, a bolt cutter and a cordless power drill as a protest against the NAVSTAR satellite navigation system, claiming it gives the US a first-strike capability.

Voice-mail sabotage

In the late 1980s, a New Jersey magazine publisher began receiving complaints from its customers. Voice mail messages renewing valuable and important advertising had never been heeded. Employees claimed they never received the calls at all, and the voice-mail system supplier was called in for technical support. Investigation showed everything normal, suggesting the dreaded intermittent

Copyright © 1996, 2004 M. E. Kabay. All rights reserved.

problem. However, customers began reporting a problem which could not be accounted for by defective software or hardware: outgoing messages had been altered to include rude and sometimes lewd language and suggestions. Attention shifted to inbound calls. In a short time, investigation showed that someone was interfering with the phone system, re-recording employees' welcome messages and deleting inbound messages from clients. The culprits proved to be a 14-year old and his 17-year old cousin, both residents of Staten Island.

Why did the youngsters attack the publisher's voice mail system? It seems that the younger had ordered a subscription to a magazine dedicated to Nintendo games (don't laugh, it's no weirder than magazines about home decoration). The magazine subscription offer included a colorful poster normally costing U$5. The magazine arrived; the poster didn't. The youngsters phoned the company, were assured they'd receive the poster, and waited. No poster. So they entered the company's voice mail, cracked the maintenance account codes and took over the system. Their shenanigans resulted in lost revenue, loss of good will, loss of customers, expenses for time and materials from the switch vendor, and wasted time and effort by the publisher's technical staff. Total cost (admittedly, estimated by the victim): U$2.1 million.

Computers can also be rendered unusable by damage to the infrastructure that supplies power and communications or to the building holding the equipment. The World Trade Center bombing was in the news as this chapter was being written; hundreds of firms lost access to their offices and to their computer systems as a result of a massive explosion in the parking garage under the twin towers of the building.

Albert the saboteur

One of the most celebrated cases of computer sabotage occurred at the National Farmers Union Service Corporation of Denver, where a Burroughs B3500 computer suffered 56 disk head crashes in the 2 years from 1970 to 1972. Down time was as long as 24 hours per crash, with an average of 8 hours per incident. Burroughs experts were flown in from all over the United States at one time or another, and concluded that the crashes must be due to power fluctuations.

By the time all the equipment had been repaired and new wiring, motor generators, circuit breakers and power-line monitors had been installed in the computer room, total expenditures for hardware and construction were over $500,000 (in 1970 dollars). Total expenses related to down time and lost business opportunities because of delays in providing management with timely information are not included in this figure. In any case, after all this expense, the crashes continued sporadically as before.

By this time, the experts were beginning to wonder about their analysis. For one thing, all the crashes had occurred at night. Could it be sabotage? Surely not! Why, old Albert the night-shift operator had been so helpful over all these years; he had unfailingly called in the crashes at once, gone out for coffee and donuts for the repair crews, and been meticulous in noting the exact times and conditions of each crash. On the other hand, all the crashes had in fact occurred on his shift....

Management installed a closed-circuit TV (CCTV) camera in the computer room--without informing Albert. For some days, nothing happened. Then one night, another crash occurred. On the CCTV

Copyright © 1996, 2004 M. E. Kabay. All rights reserved.

monitor, security guards saw good ol' Albert open up a disk cabinet and poke his car key into the read/write head solenoid, shorting it out and causing the 57th head crash.

The next morning, management confronted Albert with the film of his actions and asked for an explanation. Albert broke down in mingled shame and relief. He confessed to an overpowering urge to shut the computer down. Psychological investigation determined that Albert, who had been allowed to work night shifts for years without a change, had simply become lonely. He arrived just as everyone else was leaving; he left as everyone else was arriving. Hours and days would go by without the slightest human interaction. He never took courses, never participated in committees, never felt involved with others in his company. When the first head crashes occurred--spontaneously--he had been surprised and excited by the arrival of the repair crew. He had felt useful, bustling about, telling them what had happened. When the crashes had become less frequent, he had involuntarily, and almost unconsciously, re-created the friendly atmosphere of a crisis team. He had destroyed disk drives because he needed company.

I lay the major responsibility for Albert the Saboteur at the feet of managers who relegated an employee to a dead-end job and failed to think about his career and his morale. Other management aspects of this case are discussed in Chapter 4.

Sabotage as part of information warfare

Brad Schultz, writing in Computerworld in 1978 suggested perhaps the ultimate physical attack against a computer system: a nuclear bomb. “The federal DP reorganization committee found that Air Force computer facilities are vulnerable to nuclear attack....” This is undoubtedly true but hardly surprising.

In 1980, Alan Taylor suggested the severity of the sabotage problem facing management:

> Sabotage within a computer installation can be horrifying. Although more and more ingenuity has been used to protect accounting, terminals, and privacy in the computer area itself, protection against the absence of data caused by internal mishandling or sabotage has not yet made much headway. The absence of this protection is dangerous, but it is possible that it will be another 10 years or so before computer processes are effectively guarded against internal sabotage. The computer industry will ultimately protect people from their systems, but until then those in the industry will be made more and more subject to the disciplines that accompany dangerous privileges.

Reach out and touch someone: call-forwarding as a weapon

As an example of sabotage through administrative incompetence, consider the following tale of improper competitive advantage:

A plumber in Philadelphia was arrested in January 1995 and accused of having arranged for the local phone company to install call-forwarding on several phone lines. All the calls to these numbers were duly forwarded to the plumber’s office. Unfortunately, the calls were intended for several of his

Copyright © 1996, 2004 M. E. Kabay. All rights reserved.

competitors; he and his staff skimmed the profitable cases from the influx of calls from his competitors' clients and refused service or were rude to the rest, damaging his competitors' reputations. After a few weeks, a happy client called her plumber to thank him for having repaired a pipe over the Christmas holidays; he, of course, had no record of having worked over the holidays, and after a short investigation, the criminal scam was discovered and the perpetrators arrested.

This case was made possible only because no one bothered to verify that the numbers specified for call-forwarding actually belonged to the crooked plumber.

Disk-formatting as weapon

In a Washington, D.C. area office of the Bureau of Mines of the U.S. Department of the Interior, someone destroyed the data on hard disk drives of 19 microcomputers and stole two more. The incident occurred on Friday, August 12, 1994 around 18:30. The saboteur set up the instructions for formatting all 19 systems, then walked through the installation pressing the ENTER key on all the machines. The damage was complete within 15 minutes. Ironically, it appears that the criminal may have performed a dry run a week before, when two systems were inexplicably found formatted. After this incident, a few workers heeded security specialists' warnings that they should use access-control software with good passwords on their machines, but most did not. Those who passworded their computers were not hurt by the sabotage. Luckily for the Bureau, the culprit did not know enough about computers to overwrite the hard disks, and so technicians were able to salvage most of the data using disk utilities to undo the formatting.

In a recent application of HERF techniques for sabotage, a spectator was arrested for allegedly causing the crash of several large model airplanes at the Medeira races in Spain in the autumn of 1994. According to a report published in Schwartau's Security Insider Report, the accused "was using a frequency scanner to find what frequency the flier was using, then swapped the crystal of his own transmitter to match, thus causing the plane to lose control and in most cashes crash.... Just to add a bit of perspective, these planes cost upwards of $10,000 and travel at well over 100 mph. The impact energy is about three times that of a .45 bullet. I don't think there were any injuries, but there very easily could have been, to any of the thousands of spectators...."

Terrorism and information technology

With the tragic increase in terrorism of all kinds, some analysts warn that commercial computer systems are a potential target for social destabilization. J. Desmond wrote in 1985:

> Although the US has grown dependent on its data processing centers for its institutional well-being, the threat of attack against US data centers is a little-considered risk. Methods are available for analyzing and reducing the risk, but awareness in the data processing (DP) community of the seriousness of the problem is in small proportion to the risk itself. A report by Georgetown University's Center for Strategic and International Studies warned that computer systems should be safeguarded against terrorist sabotage that is intended to cripple or disrupt society. SRI International Inc. (Menlo Park, California), an acknowledged leader among security

Copyright © 1996, 2004 M. E. Kabay. All rights reserved.

experts, recommends that: 1. businesses adopt a sobering attitude about the threat of terrorism, and 2. a company secure itself against these threats in a reasonable and prudent business manner. SRI believes that if insurance premiums were based on a company's security measures, then companies would make a greater effort to have, at least, minimum standards of security in place.

Winn Schwartau, who has specialized in thinking about what he calls *information warfare* for many years, has repeatedly warned that information technology is vulnerable to terrorist disruption in many ways. For example, in his novel, *Terminal Compromise,* he envisages a systematic conspiracy to implant time bombs, including viruses, in U.S. software.

Sabotage has been a constant problem for anyone depending on expensive equipment; computers have been struck with axes, bombed, burned, drowned, shot and starved of electricity. These are the kinds of attacks that have concerned military thinkers involved in electronic warfare and countermeasures for years. However, new methods involving electromagnetic interference are causing concern in infowar circles. HERF (high-energy radio-frequency) guns can stop a computer dead at 100 m--or worse, cause mysterious malfunctions or data errors. In terms of productivity, having half a dozen people wasting three hours trying to analyze the peculiar behavior of a computer is more expensive than simply having the computer stop working.

An extension of the HERF attack is the EMP/T (ElectroMagnetic Pulse Transformer) bomb. This is a device designed to emit high-intensity radiation sufficient to damage modern I.T. equipment. A small, easily concealed EMP/T bomb detonated in a van on a downtown Toronto or Manhattan street could wipe out the stock exchanges, major telephone switches, and countless businesses (the ones without disaster prevention, mitigation and recovery plans). The total damage to the north American economy could greatly exceed the consequences of a physical explosion from a physically-comparable device.

On a more personal level, most airplanes flying today have fly-by-wire systems in which control surfaces are controlled by servo-motors. Instructions to the servo-motors are generated using electronic equipment of great sophistication. Ordinary cellular phones, portable computers, and even hand-held children's video games have been shown to affect some planes' stability, especially during takeoff and landing. Given the ease with which one can manufacture a powerful HERF gun using off-the-shelf electronic equipment (a domestic microwave oven is a start), there is reason to worry that criminals or terrorists stationed outside the security fences will eventually aim one of these devices at a plane landing at an airport.

Schwartau has written extensively about these issues in his bright-yellow *Security Insider Report,* which has been quoted in other security publications such as DROIS.

Preventing Sabotage

Preventing internal sabotage depends on proper employee relations. If Albert the Saboteur had been offered a rotation in his night shift, his employer might have saved a great deal of money.

Managers should provide careful and sensitive supervision of employees' state of mind. Be aware of unusual personal problems such as serious illness in the family; be concerned about evidence of financial strains. If an employee speaks bitterly about the computer system, his or her job conditions, or

Copyright © 1996, 2004 M. E. Kabay. All rights reserved.

conflicts with other employees and with management, TALK to them. Try to solve the problems before they blow up into physical attack.

Another crucial element in preventing internal and external sabotage is thorough surveillance. Perhaps your installation should have CCTV cameras in the computer room; if properly monitored by round-the-clock security personnel or perhaps even an external agency, such devices can either deter the attack in the first place or allow the malefactors to be caught and successfully prosecuted. Motion-activated cameras and video recorders can deter sabotage and other crimes and provide invaluable evidence for the police.

Safety equipment such as fire, water and smoke detectors may help to signal an attack quickly, thus reducing damage; again, such alarms may deter all but the criminally insane from starting their rampage.

Protection against outside attack is more a matter of physical barriers. You must prevent the penetration of your computer center by intruders. All the physical security methods that apply to any building can serve to reduce risk of sabotage; e.g., proper access controls, efficient fire detection and prevention equipment, and secure construction practices.

Piggybacking

One of my favorite *BC* cartoons (drawn by Johnny Hart) shows two cavemen talking about a third: “Peter has a mole on his back,” says one. The other admonishes, “Don't make personal remarks.” The final frame shows Peter walking by--with a grinning furry critter riding piggyback.

For readers whose native language is not English, “piggybacking” (origins unknown, according to various dictionaries) is the act of being carried on someone's back and shoulders. It's also known as pick-a-back. Kids like it.

So do criminals.

Now, if you are imagining masked marauders riding around on innocent victims' backs, you must learn that in the world of information security, piggybacking refers to unauthorized entry to a system (physically or logically) by using an authorized person's access code.

Physical piggybacking occurs when someone enters a secure area by passing through access control at the same time as an authorized person; e.g., walking through an door that has been opened by someone else.

Logical piggybacking means unauthorized use of a computer system after an authorized person has initiated an interaction; e.g., using an unattended terminal that has been logged on by an authorized user.

In a sense, piggybacking is a special case of impersonation--pretending to be someone else. See the following discussion for comments on impersonation.

Copyright © 1996, 2004 M. E. Kabay. All rights reserved.

Physical piggybacking

To interfere with piggybacking, we have to start by controlling access to the areas that should be secure. Which zones should be secure? The questions to ask concern the potential damage caused by unauthorized entry.

Questions to think about when deciding on access control to an area:

- Does this area contain valuable or delicate equipment? If it does, the expense of physical protection can reasonably be compared with the costs of insurance policies.
- Is the information which is accessible in this area sensitive, critical, or neither? If sensitive or critical, the costs to the organization of disclosure or damage must be considered.
- Is the area accessible to intruders (unauthorized non-employees)? Many clients have signs requiring visitors to report to a receptionist for identification; however, many receptionists let any confident-looking person in a business suit or technician's overalls stride on by without a peep.
- Do all employees need to be able to get in at all times?

Psycho-social dimensions of access control

There are difficult issues here. Allowing completely free access to what should be a secure area is an invitation to abuse; it may even prevent effective prosecution of crime by reducing the credibility of the security measures that have actually been implemented (“If security had really been important, the company would not have allowed me to get into the computer room in the first place and then I couldn't have accidentally modified my salary”).

On the other hand, restricting access severely may create a divide between authorized personnel (“the priests”) and the unauthorized (“the rabble”). Such issues become more important the fewer people there are in the organization. It would be absurd to restrict access to a computer room to three employees out of a total of five; but it would be equally absurd to allow access to 300 employees out of 500.

Avoid the error of equating access privileges with status in the organization. The CEO generally has no business entering a computer room without authorized personnel present. To allow unjustified access to senior managers gives other employees the wrong message. When I was Director of Technical Support at a service bureau, I trained two Systems Managers to take over the day-to-day operations of the multiple systems. As soon as they were ready, I asked them to remove the system supervisory capabilities from my logon-ID. For me to have continued with unnecessary access would have invited practical problems (e.g., I might have inadvertently interfered with the System Manager's policies). Keeping those unneeded capabilities would also have made it difficult to refuse computer-room access and special programming capabilities to programmers who didn't need them.

Copyright © 1996, 2004 M. E. Kabay. All rights reserved.

My recommendations are to restrict access to a mainframe or server computer room to operations staff--being sure to think about the special requirements of programmers in a very small shop. Incidentally, I once visited a client site where I noticed a blinking red light at the back of the closet where I was asked to hang my coat. Investigation revealed a file server among the salt-stained overshoes. This was accessibility carried to excess. Restrictions can reasonably be relaxed during daytime hours and tightened during off-hours.

Are there people in this area at all times during normal working hours, or is the place empty sometimes? An unattended computer room or office should be secured. Period. If it is necessary for an employee to be alone in the facilities for extended periods (e.g., night shift), be sure to arrange for monitoring by the building security guards. A closed-circuit camera or an hourly visit by a guard could save someone's life. Such monitoring may also be mandated by occupational safety regulations.

Guards and gates

Once you have determined that an area should be secured, what mechanisms are available to prevent physical piggybacking?

An obvious way is to post a guard at the entrance you wish to protect. The guard would be instructed not to allow anyone into the secure facility without authorization--accompanied or not. However, for total effectiveness, piggyback prevention would require a backup guard. Normal human beings require periodic absences from their workstations (lunch, coffee breaks, and their aftermath). Normal human beings can also fall asleep.

If you hire an outside security firm to provide guards, discuss the issues of bonding and performance guarantees. Some guards are hired with inadequate background checks and then minimally trained. You should provide all guards with an understanding of the importance of their job and the details of their responsibilities. Periodically challenge the guards by arranging to test their application of agreed-upon regulations; e.g., send an unauthorized person out the door with computer equipment.

If you do these tests, be sure to have written documentation of your plans and be physically nearby to intervene if the guards arrest the tester or propose to call the police. Clear any such test with your superiors and get written authorization to carry out your plan.

An alternative to the guard station at the door itself is a closed-circuit TV system (CCTV) with a movement-activated camera. One or more guards can then monitor an entire facility. The CCTV can also be hooked to a video-recorder for auditing purposes.

For wholly automatic operation, the facility must be equipped with a personnel-exclusion device, usually known in the trade as a man-trap. With the growing acceptance of gender-neutral language, this will presumably become known as a person-trap (I can't resist mentioning that my favorite gender-free term is “Doberperson Pinchperson”). The person-trap is installed in front of the secure door and prevents more than one person from trying to get in.

One such device looks like an instrument of torture: it's a floor-to-ceiling turnstile with a dozen projecting spikes. The only way two people would be physically capable of passing through this device

Copyright © 1996, 2004 M. E. Kabay. All rights reserved.

simultaneously would be if one of them were a midget or if both of them were experienced in making pornographic movies. The control for the turnstile is operated by the usual access-control device, such as coded cards, secret passwords, and so on.

Another person-trap is the height-weight cabinet, which checks the weight of the person in the cabinet. Even if two people were to fit intimately into the telephone-booth-sized unit, their combined weight would be greater than the tolerance set in the unit. The unit would communicate the error code to the access control computer, and entry would be refused to both people.

A height-weight cabinet also helps prevent passback--the act of giving an unauthorized person the means to enter a secure area; e.g., passing back one's ID card or key. Many computerized access-control systems remember who has entered and area and when they leave, precluding such double use of an ID.

Logical piggybacking

Unattended terminals or PCs are the portal for logical piggybacking. There are two solutions currently in use to prevent unauthorized use of a logged-on terminal or PC when the rightful session-owner is away:

- Branch to a security screen after a timeout
- Automatic logoff after a period of inactivity

A simple but non-automatic method is to lock the keyboard by physical removal of a key when one leaves one's desk. Because this method requires a positive action by the user, it is not likely to be fool-proof--not because people are fools, but because we are not machines and so sometimes we forget things.

One approach to preventing access at unattended logged-on terminals is at the operating system level. The operating system or a background program can monitor activity and abort a session that is inactive.

Such programs typically include inclusionary and exclusionary lists; i.e., you can specify either which logon IDs to monitor or which ones to ignore. Some programs also allow different timeouts for different targets; e.g., @.ACCTG might get a 10-minute limit whereas @.MATH might get 30 minutes. If the program you are running does not allow different intervals for different users, you can use the exclusionary lists as a workaround. Run (say) two different jobs with the utility; make LOGOFF1J monitor the first set of users and exclude the second set while applying the first logoff interval. Then make LOGOFF2J monitor the second set while excluding the first set and applying the second interval.

At the June 1989 meeting of the Montreal Regional HP3000 Users' Group in Montreal, Vladimir Volokh of VESOFT, INC. pointed out that it's critically important to measure the right things when deciding what is inactive. For instance, if a monitor program were to use only elapsed time, it could abort someone in the middle of a long processing transaction. If the monitor were to use only CPU activity, it might abort a process which was IMPEDED by a database lock through no fault of its own.

Aborting a session is a crude way of protecting the system against piggybacking. For example, if a poorly-designed application program were to allow locking around a terminal read, the program might

Copyright © 1996, 2004 M. E. Kabay. All rights reserved.

be aborted in the middle of a logical transaction; various datasets might be modified while others remained unmodified. An aborted program under such conditions would lead to logical corruption of the database. Most security experts would agree that application-level timeouts are preferable to the blunt object approach of operating system-level logoff utilities. Using this method, a program would periodically branch to a security screen for re-authentication.

The security screen is a display that asks for a password or for other authentication information such as questions from a personal profile. “Enter name, password, and your mother's birthday,” the system might flash after five minutes of inactivity. An intruder would likely have difficulty with some or all of those questions.

Most programming languages and systems provide a timed terminal read. A program can detect the end of the timed read and branch to the special security screen. Filling in the right answers then makes the program go back to the original screen display. Since this happens only after a reasonable delay, most people would not be inconvenienced.

A really smart program would actually measure response time for a particular entry screen and would branch to the security screen only if the delay were much longer than usual; e.g., if 99% of all the cases where the ABC123 screen were used completed within 5 minutes, the program would branch to the security screen after 5 minutes of inactivity. The DEF456 screen, on the other hand, which usually took, say, 10 minutes to complete, would not branch out to security until more than 10 minutes had gone by.

An ideal timeout facility would provide

- A configurable time-out function
- Automatic branching to a security screen
- User-configurable screen layout for re-authentication
- Integration with a security database, if available
- Automatic return to the previous (interrupted) state.

More sophisticated program-based re-authentication procedures would prevent piggybacking by means of biometric devices such as fingerprint recognition units, retinal scans, signature dynamics, and keystroke dynamics. However, such methods imply costs of upwards hundreds or thousands of dollars per workstation.

Currently, PCs can be protected with the timeout features of widely-available and inexpensive screen-saver programs. They allow users to set a count-down timer that starts after keyboard-input; the screen saver then requests a password before wiping out the images of flying toasters, swans and whatnot.

Copyright © 1996, 2004 M. E. Kabay. All rights reserved.

Impersonation

In 1970, Jerry Neal Schneider used "dumpster diving" to retrieve printouts from the Pacific Telephone and Telegraph company in Los Angeles. After years of collection, he had enough knowledge of procedures that he was able to impersonate company personnel on the phone. He collected yet more detailed information on procedures. Posing as a freelance magazine writer, he even got a tour of the computerized warehouse and information about ordering procedures.

In June of 1971, he ordered $30,000 of equipment to be sent to a normal PT&T drop-off point--and promptly stole it and sold it.

He eventually had a 6000 square-foot warehouse and 10 employees. He stole over $1 million of equipment--and sold some of it back to PT&T. He was finally denounced by a disgruntled employee and become a computer security consultant after his prison term.

In a discussion thread in the NCSA section on CompuServe in December 1992 and January 1993, I described this case (originally pieced together by Thomas Whiteside) and asked correspondents to discuss their experiences with impersonation.

An English participant commented that with overalls and a tool kit, you can get in almost anywhere. He wrote, "You just produce your piece of paper and say, "Sorry, it says here that the XYZ unit must be removed for repair." Someone else wrote in response that San Jose State University had lost some Macintosh computers to a thief using this trick.

Another NCSA Forum participant wrote,

> A long time ago when I was installing ACF2 at a GM Divisional Headquarters -- it was early on so we were doing some development there also--we often came in early in the morning or on weekends for a week or two.
>
> Even though we had proper credentials to get past the guard it was a hassle going through the routine. Eventually we realized that if we walked into the area with a box of doughnuts under our arm and waved at the guard, we were let past without having to show anything.

In the January 1993 class of the *Information Systems Security* course sponsored by the NCSA, a participant recounted the following astonishing story. A well-dressed business man appeared at the offices of a large firm one day and appropriated an unused cubicle. He seemed to know his way around and quickly obtained a terminal to the host, pencils, pads, and so on. Soon, he was being invited out to join the other employees for lunch; at one point he was invited to an office party. All this time, he never wore an employee badge and never told anyone exactly what he was doing. "Special research project," he would answer with a secretive air. Two months into his tenure, my course participant, a feisty information security officer, noticed this man as she was walking through his area of the office. She asked others who he was and learned that no one knew. She asked the man for his employee ID, but he excused himself and hurried off. At this point, the officer decided to call for the physical security guards. She even prevented the mystery man's precipitous departure by running to the only elevator on the floor and diving into it before he could use it to escape.

Copyright © 1996, 2004 M. E. Kabay. All rights reserved.

It turned out that the man was a former employee who had been fired and was currently under indictment for fraud. He had been allowed into the building every morning by a confederate, a manager who was also eventually indicted for fraud. The manager had intimidated the security guards into allowing the “consultant” into the building despite official rules requiring everyone to have and wear valid employee passes. The more amazing observation is that in two months of unauthorized computer and office use, this man was never once stopped or reported by the staff working in his area.

This case illustrates the crucial importance of a sound corporate culture in ensuring that security rules are enforced.

Data diddling

One of the most common forms of computer crime is data diddling--illegal or unauthorized data alteration. These changes can occur before and during data input or before output. Data diddling cases have included banks, payrolls, inventory, credit records, school transcripts, and virtually any other form of data storage known.

The Equity Funding Fraud

In his entertaining and informative book on computer crime, Thomas Whiteside describes the events of the late 1960s through 1973 which became known as the Equity Funding Fraud, a case of organized data diddling on a scale unparalleled to date.

The fraud

The case began with computer problems at the Equity Funding Corporation of America, a publicly-traded and highly successful firm with a bright idea. The idea was that investors would buy insurance policies from the company and also invest in mutual funds at the same time, with profits to be redistributed to clients and to stock-holders. Through the late 1960s, Equity's shares rose dizzyingly in price; there were news magazine stories about this wunderkind of the Los Angeles business community.

The computer problems occurred just before the close of the financial year. An annual report was about to be printed, yet the final figures simply could not be extracted from the mainframe. In despair, the head of data processing told the president the bad news; the report would have to be delayed. Nonsense, said the president expansively (in the movie, anyway); simply make up the bottom line to show about $10,000,000.00 in profits and calculate the other figures so it would come out that way. With trepidation, the DP chief obliged. He seemed to rationalize it with the thought that it was just a temporary expedient, and could be put to rights later anyway in the real financial books.
The expected profit didn't materialize, and some months later, the head of DP was in trouble again. The books were not going to balance; where were the large inflows of cash from investors that the company had counted on? It occurred to the executives at Equity that they could keep the stock price high by manufacturing false insurance policies which would make the company look good to investors. They

Copyright © 1996, 2004 M. E. Kabay. All rights reserved.

therefore began inserting false information about nonexistent policy holders into the computerized records used to calculate the financial health of Equity. These false records were conveniently identified with special customer code “99,” allowing them to be inserted into calculations of totals but permitting them to be excluded from audit listings. An auditor scanning randomly would only see records which had corresponding paper files for real policyholders.

In time, Equity's corporate staff got even greedier. Not content with jacking up the price of their stock (of which they owned large quantities), they decided to sell the policies to other insurance companies via the redistribution system known as re-insurance. Re-insurance brokers help multiple insurance companies spread the risk of insurance policies; e.g., a twenty-million-dollar building fire might bankrupt a particular insurance company, but if a group of 100 companies each had part of the coverage, no one of them would bear the entire cost of paying the victims for the damage. In any case, re-insurance companies pay money for policies they buy; only one year later do the issuing insurance companies have to pay the re-insurers the premiums paid in by the policy holders.

So in the first year, selling imaginary policies to the re-insurers brought in large amounts of real cash. Again, the head of DP rationalized this fraudulent sale as a “loan” to be repaid later.

But later was worse. It came time to start paying real money to the re-insurers for the policies in the names of fake people. What to do? Inventive to the last, the crooked crew at Equity decided that if the imaginary people were incapable of producing real money, they should be killed. And so pathetic hordes of people who had never existed began dying of heart attacks, car accidents, and, in one memorable case, of cancer of the uterus. The cancer victim was a man.

Having killed off some of the ghosts, Equity turned around and demanded real money for their beneficiaries--equally ghostly. Dutifully, the re-insurers poured cash into Equity for distribution to the unfortunate bereaved souls who had lost their spouses, parents, offspring, and siblings. Equity received over a million dollars for these false deaths.

Eventually, there came requests for documents associated with these unfortunate imaginary deaths. At this point, the executives engaged in all-night parties at which they invented the paper files that corresponded to the requested dossiers. These fabrications came complete with doctors' reports (copied from random parts of real dossiers), signatures, hospital records, and biographical information. Whenever a company auditor asked for the files for randomly selected policies, they would be produced at once--except for the code 99s. These were “presently in use”, the auditor would be told; they'd be available the next morning. And they were, too, thanks to the indefatigable forgers who had by this time been moved to a separate building.

By the spring of 1971, the executives were churning out from 20,000 to 50,000 fake policies per year; by 1972, 64,000 of the companies 97,000 policies were fraudulent. The face value of these invented people's insurance policies totaled $2.1 billion out of a total of $3.2 billion. Whiteside writes, “...out of $737 million in assets that the company reported in its last financial statement, $185 million was nonexistent.”

By late 1972, the head of DP was frankly worried. He had been calculating the rate of growth of the imaginary people in the company's files, and he found that by the end of the decade, at this rate, Equity Funding would have insured the entire population of the world. Its assets would surpass the gross

Copyright © 1996, 2004 M. E. Kabay. All rights reserved.

national product of the planet. Clearly, the rate of growth had to be moderated. The president merely insisted that this showed how well the company was doing.

Shortly before the bubble burst, the operations supervisor confronted the head of DP. What was the meaning of all these code 99s, he demanded to know. Where was the documentation which would show what these meant? The head of DP reassured him with a lie--a smaller crime than the unimaginable reality. Well, said DP, you see, it's that we've been selling policies directly to clients, thus cutting out our own agents--and they'd be real mad if they knew, so we code all those policies as 99s. To his shame, the head of operations acquiesced in this smaller crime.
The scheme fell apart when an angry operator who had to work overtime told the authorities about shenanigans at Equity. Rumors spread throughout Wall Street and the insurance industry. Within days, the Securities and Exchange Commission had informed the California Insurance Department that they'd received information about the ultimate form of data diddling: tapes were being erased. The officers of the company were arrested, tried, and condemned to prison terms.

The lessons

What can we learn from this fascinating scandal? Here are some thoughts for discussion:

Fraud is extremely difficult to detect if there are no honest people in the organization. The entire management group was implicated in this crime, from the top levels down to operations. It would have collapsed if an honest person had pursued the details until the picture became clear; information could have been given to legal authorities years before the final collapse, saving thousands of innocent victims who lost their investments because of the collapse of the company.

The auditors were incompetent. The firm was tiny--it was hand-picked by the directors of Equity so that Equity would be the auditors' biggest account, generating 80% of that firm's revenue. The auditors depended on inadequate sources of information. They actually asked employees of the firm they were auditing to provide them with the documents they needed. Auditors should always get the documents themselves (i.e., someone from the auditing firm should be physically present as the documents are located).

The auditors accepted excuses for delays in meeting their requirements for random samples of documents. It is not acceptable that a required document be delayed. The reason for the delay must be shown unambiguously to be legitimate.

The auditors were incapable of determining what the computer programs were doing with the data. A qualified auditor would have used independent data processing expertise to ascertain the function of code 99s by examining source code (and recompiling it to see that it generated the actual executable code being run) and tracking down the logic.

Another observation is that the bubble burst because of a disgruntled employee. It was not a clever program or a special security device that foiled the criminals' plan: it was an observant human being who was willing to blow the whistle and report his suspicions of criminal activity to the appropriate authorities.

Copyright © 1996, 2004 M. E. Kabay. All rights reserved.

As managers, make it clear in writing and behavior that no illegality will be tolerated in your organization. Provide employees with information on what to do if their complaints of malfeasance are not taken seriously by their superiors. You may demonstrate the seriousness of your commitment to honesty by including instructions on how to reach legal or regulatory authorities.

As employees, be suspicious of any demands that you break documented rules, unspoken norms of data processing, or the law. For example, if you are asked to fake a delay in running a program--for any ostensible reason whatsoever--write down the time and date of the request and who asked you to do it. I know that it's easy to give advice when one doesn't bear the consequences, but at least see if it's possible to determine why you are being asked to dissimulate. If you're braver than most people, you can try seeing what happens if you flatly refuse to lie. Who knows, you might be the pin that bursts whatever bubble your superiors are involved in. Maybe you'll get a movie made of your adventures....

If you notice an irregularity--e.g., a high-placed official apparently doing extensive data entry--see if you can discreetly find out what's happening. See what kind of response you get if you politely inquire about it. If a high-placed employee tries to enter the computer room without authorization, refuse access until your own supervisor authorizes entry--preferably in writing.

If you do come to the conclusion that a crime is being committed, inform your supervisor--if (s)he seems to be honest. Otherwise, inform the appropriate civic or other authorities when you have evidence and your doubts are gone. At least you can escape being arrested yourself as a co-conspirator.

In the U.S., whistle-blowers who report illegal activity within their organizations may be protected by law--at least, in theory--against retribution from their employers.

More recent data diddling

Some recent cases of data diddling:

- A church's phone was reputedly call-forwarded to a 900 sex line.

- A person accused of spamming the Internet found his company's 800 number listed as a phone-sex line in various alt.sex groups on the Internet, resulting not only in thousands of dollars of charges to his company but personal humiliation when the receptionists refused to put up with any more of the heavy-breathing callers and sent them all to his own phone extension.

- In another case discussed at a criminal hacker convention in December 1993, a poor soul found that a criminal hacker had used a war dialer (a program for automatically dialing phone numbers in sequence) and had left the victim's phone number on thousands of pager accounts. The innocent pager users were irritated at having made a call for nothing, but the victim's life was made untenable for a day.

- In a recent case in Toronto, a night auditor in a commercial center obtained computer records for 28,000 credit-card transactions from January 1989 to May 1994. Using these data, the criminal, working with dishonest business confederates, generated phony transactions and shared the proceeds, amounting to C$1.5 million.

Copyright © 1996, 2004 M. E. Kabay. All rights reserved.

! In October 1992, an Arizona state official was charged with embezzling $1.6 million in state funds. United Press International reported that Wayne Nelson was arrested after he deposited $460,000 into a checking account in the name of his own company.

! In November 1992, the complete dossier concerning the escape of notorious Colombian crime boss Pablo Escobar was destroyed hours before the information was due to be presented to the Senate in Bogota. Reuter reported that the mechanism of data destruction was unknown, although some reports claimed a virus was involved.

! In December 1992, an accidental data entry error caused a chemical factory to explode in the Netherlands. The typing mistake allowed the wrong ratio of chemicals to be mixed. Several people died because of the failure of the computer programs to catch the error before allowing the automated process to lead to the explosion.

! In January 1993, the owners of Value Rent-A-Car, Inc. were indicted on charges of rigging their computers to overcharge all customers who returned their rental cars with less than a full tank of gas. Over 47,000 customers were defrauded by the charges for the nonexistent extra five gallons of gas automatically added to the computer records of tank capacity. The perpetrators were convicted in

! In St. Petersburg, FL, a personnel supervisor altered customer records to show that credit cards issued by his employer, a chain of jewelry stores, had been stolen. Store policy required clerks to allow such "victims" of credit-card theft to continue using their accounts using name, Social Security number, and an authorization code from the company. A confederate would then show up at a store and insist on using the number of the "stolen" card, providing clerks with a secret code the personnel supervisor had issued. The supervisor would then reverse all indications that the card had been flagged as stolen. The scam was discovered when an anonymous tip to the police suggested they check the mainframe database records.

! In April 1993, electronic sign boards along Interstate 95 in Connecticut had glowing letters reading, "You all suck." A few days later, the boards showed insulting notes about the Governor of the state. It seems that a teenager had broken into the password-free computer system at the Connecticut Highway Department and amused himself altering the boring messages about road conditions.

! At Stirling University in Britain in April 1994, a vandal caused so much damage on the university Internet site that staff had to put in 6 person-weeks to repair the data corruption that interfered with E-mail, FTP and other functions.

! In August 1994, residents of Oak Avenue in San Rafael, CA 94901 suddenly lost access to their mail when someone deleted their ZIP code from the U.S. Postal Service's national database. All of their mail got redirected to the residents at corresponding numbers on Oak Avenue, San Rafael, CA 94904--who were surely not too pleased either. The error was propagated throughout the U.S. when mailing houses subscribing to the Postal Service's updates changed their own records to match the erroneous reassignment.

Copyright © 1996, 2004 M. E. Kabay. All rights reserved.

! At various times in recent years, self-styled cyberspace vigilantes have launched procedures called “cancelbots” into the Internet to track down and destroy USENET postings they dislike. One such occurrence took place in December 1994, when “Cancelmoose,” working through a Finnish anonymizing service, attacked promotional messages by author Michael Wolff.

All of these examples confirm that computerized or mechanical controls alone are insufficient to prevent computer crime. Only the vigilance of well-trained, security-conscious staff will make the automatic security provisions work effectively.

Superzapping

Don B. Parker defines superzapping as, “the unauthorized use of utility computer programs to modify, destroy, copy, disclose, insert, use, or deny use of data stored in a computer or computer media.” He explains that the name comes from a utility widespread in the IBM world. Parker describes how in one case, a New Jersey bank manager discovered how easy it was to alter data without leaving an audit trail; she transferred a total of $128,000 to the accounts of three friends before an alert customer noted a shortfall in a legitimate account and alerted the bank. The criminals were convicted of theft.

In my own experience, I was told by one customer about the consequences of undocumented superzapping: a “wizard” used to zap a table to patch a specific program problem rather than fixing the source code. When the wizard left on holiday, the application system failed; it took a week of chaos to try to fix the problem--and all attempts failed. The company had to wait for the wizard to return.

In another case, an Alberta service bureau discovered that one of its customers regularly uses a superzap program to modify production data. Other than warning the managers that such a procedure is inherently risky, there was nothing the bureau could do about it.

In one instance at my former employer's service bureau, we discovered that a programmer made changes directly in spoolfiles (spooled print files) on a monthly basis to correct a persistent error that had never been fixed in the source code. If such shenanigans were going on in a mere report, what might be happening in, say, print runs of checks?

Why tolerate superzaps?

If superzapping is so dangerous, why allow superzap programs to reside on the system at all?

Superzap programs serve us well in emergencies. No matter how well planned and well documented, any system can fail. If a production system error has to be circumvented NOW, patching a program, fixing a database pointer, or repairing an incorrect check-run spoolfile may be the very best solution--if the changes are authorized, documented, and correct. Repeated use of such utilities to fix the same problems, however, indicates a problem of priorities. Fix the problem now, yes; but find out what caused the problem and solve the root causes as well.

What kinds of utilities might qualify as superzaps?

Copyright © 1996, 2004 M. E. Kabay. All rights reserved.

- Privileged debuggers: tools which allow unrestricted access to memory and disk structures
- Disk editors: permit any change to be written to disk without passing through the file system
- Program patchers: modify executable program files without having to recompile source code
- Database tools: can change portions of a database without regard for logical consistency
- Spoolfile editors: modify output files before printing
- Alternate operating systems: replace the normal operating system for diagnostic purposes.

Controls on superzaps

System managers can control superzap programs by limiting access; software designers can help system managers by enforcing capability checking at run-time.

Security systems using menus can restrict users to specific tasks; the usual security matrix can prevent unauthorized access to powerful utility programs. Some programs themselves can check to see that prospective users actually have appropriate capabilities (e.g., in the HP3000 environment, “PM” capability to use privileged-mode debug and ASM” (system manager) for disk editors). Ad hoc query programs can sometimes be restricted to read-only in any given database.

On some systems, access control definitions (ACDs) permit explicit inclusion of user sets which may access a file (including superzap programs) for read and write operations.

Aside from using normal operating system security, one can also disable programs temporarily in ways which interfere with (they don't preclude) unauthorized access; e.g., a system manager can reversibly remove the capabilities allowing interactive or batch execution from dangerous programs.

Some operating systems provide opportunities for more sophisticated controls. For example, in the HP3000 environment running MPE/iX, VESOFT Inc. have devised an extension to their SECURITY/3000 access-control package which helps restrict unauthorized access to IMAGE databases by programs which go through the database management system (DBMS). By replacing calls to the DBOPEN intrinsic by calls to VEOPEN, programmers can ensure that each database has its own access control list--including restrictions on which programs and users can access a given database. It is also possible to convert compiled programs (e.g., the ad-hoc inquiry program, QUERY/3000) to force them to use VEOPEN, too. Even unconverted programs can be stopped by letting VEOPEN randomize database passwords in the root file. A program that calls DBOPEN instead of VEOPEN then fails on a password violation.

Copyright © 1996, 2004 M. E. Kabay. All rights reserved.

VEOPEN cannot prevent access by programs that do not use the DBMS; e.g., DISKEDIT, a disk editor that bypasses the file system altogether.

It may be desirable to eliminate certain tools altogether from general availability. For example, special diagnostic utilities which replace the operating system should routinely be inaccessible to unauthorized personnel. Such diagnostic tools could be kept in a safe, for example, with written authorization required for access. In an emergency, the combination to the safe might be obtained from a sealed, signed envelope which would betray its having been opened. I can even imagine a cartoon showing a sealed glass box containing such an envelope on the computer room wall with the words, "IN CASE OF EMERGENCY, BREAK GLASS" to be sure that the emergency crew could get the tape if it had to.

When printing important files such a runs of checks, it may be wise to print "hot" instead of spooling the output. That is, have the program generating the check images control a secured printer directly rather than passing through the usual buffers. Make sure that the printer is in a locked room. Arrange to have at least two employees watching the print run. If a paper jam requires the run to be started again, arrange for appropriate parameters to be passed to prevent printing duplicates of checks already produced.

Teamwork

Regardless of all the access-control methods described above, if an authorized user wishes to misuse a superzap program, there is only one way to prevent it: teamwork. By insisting that all use of superzaps be done with at least two members of the staff present, one can reduce the likelihood of abuse. Reduce, not eliminate: there is always the possibility of collusion. Nonetheless, if only a few percent (say, two percent for the sake of the argument) of all employees are potential crooks, then the probability of getting two crooks on the same assignment by chance alone is about 0.04%. True, the crooks may cluster together preferentially, but in any case, having two people using priv-mode DEBUG to fix data in a database seems better than having just one.

One method that will certainly NOT work is the ignorance-is-bliss approach. I have personally heard many system managers dismiss security concerns by saying, "Oh, no one here knows enough to do that." This is a short-sighted attitude, since almost everything described above is fully documented in vendor and contributed software library publications. Recalling that managers are liable for failures to protect corporate assets, I urge all system managers to think seriously about these and other security issues rather than leaving them to chance and the supposed ignorance of a user and programmer population.

Tracing superzap usage

At the first level of security, a system-access log will at least provide an idea of which access codes were used to log on to the computer system at which time and using which devices. The mere fact that a system can provide an audit trail of unauthorized access may itself reduce the likelihood of access.

Most access-control systems also provide for more detailed identification; e.g., required session identifiers and personal-information checking.

Copyright © 1996, 2004 M. E. Kabay. All rights reserved.

Many logging facilities also permit more detailed records to be kept of which files are closed by a process. It thus becomes possible to tell exactly which programs are being executed by a given user at what time and using which data files. Such logging works for programs that use the file system; however, other than knowing that a user ran a specific program there would be no audit trail of what the superzap program actually did to data.

When evaluating audit programs, look for records not only of file closure but also file opens, including failed attempt to open a file. Such records allow a security administrator to identify even failed attempts at opening a file. Repeated instances of such failures may signal an attempted security breach.

Database logging works well to record modifications of data, even by databases utility. However, such audit trails require logging to be enabled for the database involved.

Scavenging

As a security-conscious computer user, you have bought cables and locks to tie down your workstation; your mainframe computer is locked away behind armored doors equipped with retinal scan units, fingerprint recognition boxes, and a magnetic card access system. Everything seems as tight as a drum.

So why is your business competitor using your client list? And how come you've just been informed of a cracker attack via the security modem that's supposedly password-protected? And where did the cracker get the password for the accounting package your hot-shot programmers have been finishing? Why is the local newspaper publishing your financial figures?

Maybe your data are leaking out through your garbage can.

Computer crime specialists have described unauthorized access to information left on discarded media as scavenging, browsing, and dumpster-diving (from the name of the metal bins often used to collect garbage outside office buildings).

Case studies

Parker estimates that scavenging is probably the third most important method of computer crime; the first two are data diddling and unauthorized use of computer services.
Parker cites a fascinating case of scavenging at a service bureau for oil companies. A puzzled operator asked his manager why a specific job always read a scratch tape (a tape available for temporary use). Why would anyone want to read a scratch tape before writing on it? Investigation revealed that a rogue company was stealing geophysical data written by the oil companies “temporarily” on scratch tapes--and then selling it to their competitors.

Do not allow scratch tapes to contain confidential data. Erase them before returning them to the tape rack.

Copyright © 1996, 2004 M. E. Kabay. All rights reserved.

The case of Jerry Neal Schneider, discussed above in the section on impersonation, also involved scavenging. The thief had made a hobby of raiding the victim's dumpsters for years.

A computer database search turned up another interesting wrinkle in scavenging. According to Miles Benson, writing in *Computerworld,* a programmer earned a living by finding software projects which had been abandoned even though they were 90% complete. He would complete them himself for profitable sale to other companies. This “Ragpicker” made his first sale from a cross-reference program for FORTRAN, RPG and COBOL source. He even salvaged the documentation.

Little legal protection for garbage

Discarded garbage is not considered private property under the law, according to the U.S. Supreme Court ruling on the privacy of discarded garbage. The California vs Greenwood *et al.* case, No. 86-684 was argued on January 11, 1988 and decided May 16, 1988. Mr. Greenwood argued that his arrest on drug trafficking charges was illegally obtained by warrantless search of green plastic garbage bags he had placed outside his home.

Justices White, Rehnquist, Blackmun, Stevens, O'Connor and Scalia wrote,

> 'The Fourth Amendment does not prohibit the warrantless search and seizure of garbage left for collection outside the curtilage of a home.... Since respondents voluntarily left their trash for collection in an area particularly suited for public inspection, their claimed expectation of privacy in the inculpatory items they discarded was not objectively reasonable. It is common knowledge that plastic garbage bags left along a public street are readily accessible to animals, children, scavengers, snoops, and other members of the public. Moreover, respondents placed their refuse at the curb for the express purpose of conveying it to a third party, the trash collector, who might himself have sorted through it or permitted others, such as the police, to do so. The police cannot reasonably be expected to avert their eyes from evidence of criminal activity that could have been observed by any member of the public.....'

In other words, anything we throw out is fair game, at least in the US. Other readers would do well to determine the state of jurisprudence dealing with the privacy, if any, of garbage in their jurisdiction. The only protection is to make the garbage unreadable.

Discarded information can reside on paper, magnetic, and even electronic media. All of them have special methods for obliterating the unwanted information. Let's follow information from inside computer memory toward the outer world and look for ways of protecting our information against scavenging.

Electronic garbage

Under many operating systems, memory locations are not zeroed when they are discarded; they're simply marked as free. A memory dump, for example, would show the list of free terminal buffers; these would frequently have information from sessions that had released them. Similarly, at any given

Copyright © 1996, 2004 M. E. Kabay. All rights reserved.

moment, database control blocks are likely to have information in buffers that have been posted to disc but are available for re-use. A privileged process can easily read this discarded information.

Hewlett-Packard (HP) recognized the importance of destroying information in temporary work areas in memory when it put the LARC editor on the market as TDP/3000. Encryption in TDP allows one to specify that the work file be destroyed once the cleartext has been converted to ciphertext.

Spoolfiles may be an unnoticed form of electronic waste. They are stored on disk and should be inaccessible to unprivileged users except through spooler utilities that keep track of security authorization. An old spoolfile that has been lying around unused may provide information for anyone who can access it (including the system operators).

On smart terminals or terminal-emulation programs, there may be many pages of terminal memory accessible through the page-backward key. Users should home the cursor to the top of memory and clear it before leaving their terminals. When I was in charge of security at a service bureau, I modified the HP3000 operating system messages file to include the escape sequences that automatically homed cursor and cleared display as part of the logoff message.

Aside from screen memory, other parts of PC memory may contain interesting tidbits of leftover information. A user with access to commonly-available utilities can dump the contents of RAM to a file and examine it at leisure. If you have been processing confidential information during the day, before leaving, turn your PC off or force a cold boot operation to re-initialize memory. Locking your PC will also prevent data residues from being stolen.

Magnetic garbage

Most people know that when a file is erased or purged from a magnetic disk, operating systems usually leave the information entirely or largely intact but remove the pointers from the directory. For example, DOS obliterates the first character of an erased file with a special character and removes its entries from the FAT (file allocation table). Unerase utilities search the disk or diskette and reconstruct the chain of extents (areas of contiguous storage), usually with human intervention to verify that the data are still good.

Multi-user operating systems remove pointers from the disk directory and returns all sectors in a purged file to a disk free-space map, but the data in the original extents persist unless specific measures are taken to obliterate them.

Formatting a disk actually zeroes diskettes and hard disks; however, even formatting and overwriting data on magnetic media may not make the data unreadable to the most sophisticated equipment. Since information on magnetic tapes and disks resides in the difference in intensity between highly-magnetized areas (1s) and less-magnetized areas (0s), writing the same thing (0s or 1s) in all areas of the obliteration merely reduces the signal-to-noise ratio. That is, the residual magnetic fields still vary in more or less the original pattern--they're just less easily distinguished. Using highly sensitive readers, a magnetic tape that has been zeroed will still yield much of the original information.

Copyright © 1996, 2004 M. E. Kabay. All rights reserved.

One way of destroying data on magnetic media is to overwrite using random patterns and then zero the data. The random patterns make it far more difficult to extract useful information from the discarded disks and tapes.

Another problem of data residues occurs when you have a defective disk drive and want to get it fixed. If you can reformat the device before turning it over to a repair shop, that's fine. But what do you do if the drive is not functional? You can't reformat it because it doesn't work. But some repair plans explicitly or implicitly recycle used hard disks; in the RISKS Forum Digest on the Internet, a correspondent wrote that he had received a replacement disk unit which contained confidential data from a bank. Some users in high-security areas simply abandon any hope of fixing their defective drives. They destroy the equipment rather than allow it out of their control.

Paper

Paper waste can consist not only of letters and listings but also of carbon film. For more secure copies, consider using carbonless multipart forms. Printers using carbon-film ribbon (like the IBM Selectric typewriters do) may generate readable ribbon reels.

Rummaging in garbage cans for discarded but intact listings is a favorite cracker method for tracking down logon IDs, passwords, interesting program names, and opportunities for harm.

Many people justifiably feel that printing two-foot thick piles of computer listings that are used for only a few hours is an unreasonable use of resources. In their zeal for recycling, such environmentally-conscious folks may innocently do things like giving the local kindergarten their employer's entire client list or using a memory dump showing passwords as kindling. The message is not that all listings are sensitive, but that some thought should be given to deciding which listings may safely be used for such public use and distribution.

Better yet, look for ways of avoiding huge printouts. There are tools available in the midrange and mainframe marketplace that allow users to scan their spoolfiles either page by page or using a form of simple indexing. Think about whether users can get more out of electronic access to their reports than out of reams of paper. Some spoolfile tools also allow selective printing, which means that if different users need only parts of a large listing, they can generate their own subsets locally. Finally, some of the tools even allow for automated verification of size or content to ensure that erroneous spoolfiles never get printed at all.

Physical destruction

Physical destruction of magnetic media can be a reasonable solution to the problem of disposal. Some users with access to a machine shop simply have tapes cut in half with a bench saw. Hard disks can be crushed. Floppy diskettes can be burned.

As for paper, a review of shredders and disintegrators in an older edition of DROIS listed 18 suppliers and summarizes 132 models. The article defined four classes of shredder capacity: desk-side or personal,

Copyright © 1996, 2004 M. E. Kabay. All rights reserved.

office, heavy-duty, and industrial. Shredders have three types of cutting mechanisms, straight, cross-cut, and particle-cut; the degree of security depends on how small the shredder can make the output fragments. Disintegrators use cross-cutting blades with mesh that keeps the paper in the cutting chamber until the particles are small enough to escape. Shredders cost from hundreds to many thousands of dollars depending on capacity, fineness of output, and duty cycle.

Back doors

In the movie, *War Games,* a young computer cracker becomes interested in breaking through security on a computer system he's located by automatic random dialing ("war dialing") of telephone numbers. He eventually manages to break security by locating a secret password that gives him the power to bypass normal limitations. He goes on to play Global Thermonuclear War--which nearly results in the real thing.

The unauthorized, undocumented code in the source which bestows special privileges is, in the language of computer security, a "back door," sometimes called a "trap door." Glenn Roos defined it neatly as, "a method of gaining access to things normally out of reach."

Back doors are part of a program; they are distinguished from Trojan Horses, which are entire programs with a covert purpose. A back door will not cause harm by itself; it merely allows a breach of normal controls by those aware of the feature. A Trojan Horse is a program which may cause harm during normal usage by innocent users.

Cases

Thomas Whiteside describes experiments in cracking the MULTICS operating system developed by Honeywell Inc. and the Massachusetts Institute of Technology. Steven B. Lipner, working for MITRE Corporation, and Roger R. Schell of the US Air Force were authorized to try to crack MULTICS' security starting with an ordinary, unprivileged logon. In trials from 1972 to 1975, they managed to find flaws in the operating system through which they gained enough power to insert modifications in the system code that gave them back doors through which they could then subvert normal security. They were able to obtain maximum security capabilities on several MULTICS systems.

Whiteside goes on to summarize research on cracking the UNIVAC operating system in the late 1970s. The classified report to the US government stated that the volume of classified data that back door techniques permitted the experimenters to retrieve without authorization was so huge they had to put limits on how much the system spewed out for them.
Donn B. Parker describes two back door cases. In the first, a programmer discovered a back door left in a FORTRAN compiler by the writers of the compiler. This section of code allowed execution to jump from a regular program file to code stored in a data file. The criminals used the back door to steal computer processing time from a service bureau. The other case Parker describes was similar; some remote users from Detroit used back doors in the operating system of a Florida time-sharing service to find passwords that allowed unauthorized and unpaid access to proprietary data and programs.

Copyright © 1996, 2004 M. E. Kabay. All rights reserved.

Finding back doors

How can we spot back doors in our programs? It is less difficult to identify back doors after they've been used than before they're accessed. If Henrietta Hacker boasts about being able to crack the accounting program she wrote last year “any time, any place”, maybe it's time for a source-code audit.

As for finding back doors before they spring open, your search for back doors should include the following:

- Undocumented code
- Code not executed during testing
- Undocumented embedded alphanumerics
- Peculiar entry points
- Unexplained functions

Every line of code in a program must make sense for the ostensible application. Every line of code must be exercised during system testing. All alphanumerics in source code have to make sense; a more difficult problem is dealing with numeric codes which may have a hidden meaning. Every entry point for a compiled program must make sense in the programming context.

Preventing back doors

How can we prevent programmers from leaving back doors in our production and utility software?

Documentation standards are not merely desirable; they can make back doors difficult to include in production code. Deviations from such standards may alert a supervisor or colleague that all is not as it seems in a program. Using team programming (more than one programmer responsible for any given section of code) and walkthroughs (following execution through the code in detail) will also make secret functions very difficult to hide.

Test-coverage monitors show which lines of source code have been executed during system tests. Such programs identify the percentage of code that is executed by a test or series of tests of a COBOL program. They then specifically identify which lines of code were executed and which were left unexecuted by the test(s). They can also count the number of times that each line is executed. Finally, test-coverage monitors provide a detailed program trace showing the path taken at each branch and conditional statement.'

Copyright © 1996, 2004 M. E. Kabay. All rights reserved.

Operating-system back doors

It is impractical--some would say impossible--for ordinary customers to locate back doors in their operating system's code. For example, according to sources at HP, MPE/iX lab staff currently do not know exactly how many lines of source code the operating system has: it changes every day. Try running exhaustive tests on that!

Under some versions of the HP3000's MPE/iX operating system, there was a documented mechanism for system managers to bypass the automatic invocation of special functions at logon. These logon User-Defined Commands (UDCs) were required for many security programs. Without the logon UDCs, it was possible for imposters who had obtained the MANAGER.SYS password to gain access to the system without having to run the gauntlet of authentication programs (e.g., random questions such as "Where was your mother born?"). The bypass caused a furor in the user community and was quickly repaired. This case also demonstrates the value of not concealing security problems.

In the UNIX system versions distributed by Sun Microsystems, Digital Equipment Corporation and others, there was a back door to the DEBUG option for the *sendmail* program. The back door allowed William T. Morris' Internet worm of November 1988 to propagate explosively through the Internet.

Canonical passwords

Something akin to back doors is canonical passwords; i.e., passwords on vendor accounts that are identical from system to system. Cliff Stoll, in his battle with West German crackers, was horrified to discover how many systems allowed easy access using standard passwords. In my own practice, I have often found vendor service accounts using the original passwords assigned at system configuration. These accounts usually have full supervisory capabilities, compromising the security of the entire system. This point is made so often in articles on security that I won't belabor it--just be sure you explicitly change the passwords on accounts received from vendors.

Trojan horses

Some of my students have expressed bewilderment over the term Trojan "*horse."* They associate "Trojan" with condoms and with evil programs. Here's the original story:

> ...But Troy still held out, and the Greeks began to despair of ever subduing it by force, and by advice of Ulysses resolved to resort to stratagem. The Greeks then constructed an immense wooden horse, which they gave out was intended as a propitiatory offering to Minerva, but in fact was filled with armed men. The remaining Greeks then...sailed away....

[The Horse is then dragged into the walled city of Troy and the people celebrate the end of the long war.]

Copyright © 1996, 2004 M. E. Kabay. All rights reserved.

> ...In the night, the armed men who were enclosed in the body of the horse...opened the gates of the city to their friends, who had returned under cover of the night. The city was set on fire; the people, overcome with feasting and sleep, put to the sword, and Troy completely subdued.

Bullfinch thus describes the original Trojan Horse. Today's electronic Trojan is a program which conceals dangerous functions behind an outwardly innocuous form.

Case studies

One of the nastiest tricks played on the shell-shocked world of microcomputer users was the FLU-SHOT-4 incident of March 1988. With the publicity given to damage caused by destructive, self-replicating virus programs distributed through electronic bulletin board systems (BBS), it seemed natural that public-spirited programmers would rise to the challenge and provide protective screening.

Flu-Shot-3 was a useful program for detecting viruses. Flu-Shot-4 appeared on BBS and looked just like 3; however, it actually destroyed critical areas of hard disks and any floppies present when the program was run. The instructions which caused the damage were not present in the program file until it was running; this self-modifying code technique makes it especially difficult to identify Trojans by simple inspection of the assembler-level code.

HP itself put a Trojan into the HP3000 operating system with IOCDPN0.PUB.SYS. This program's name implied that it ought to be an I/O driver for a CarD PuNch, just like IOTERM0 and IODISC0. Indeed, IOCDPN0 was tagged as a required driver by SYSDUMP so you couldn't get rid of it. However, rather than being an innocuous old driver, the program was actually a powerful utility for accessing the low-level routine ATTACHIO. Using IOCDPN0, one could read and write to the memory structures controlling terminals, tapes, printers, and other peripherals. There were even macros to permit HP technicians to repeat I/O operations when MPE couldn't help because of bad data or other unacceptable conditions. A typical use would be to read a bad tape and recover valuable data unreadable through normal I/O.
Another Trojan was a blocking-factor program that one of his colleagues wrote. This vanilla program, derived from the Contributed Software Library (CSL) from INTEREX, the International Association of HP Computer Users, calculated optimum blocking factors admirably--but it posted an invisible timed terminal read at an undocumented but fixed period after initialization. If the user knew exactly what to type at exactly which time, he or she could obtain system manager (SM)status and all other capabilities for their user ID for that session. In a sense, this example also illustrates the concept of a back door.

An incident that looked like a Trojan Horse occurred in 1983, when HP issued one of its periodic revisions of the MPE/V operating system. My operations team and I were just beginning our acceptance tests at 03:00, after production had completed and the operator had finished a full backup. We shut down the HP3000, switched disk packs to the test configuration, and began booting the system with the fresh Master Installation Tapes from HP. To our horror, we saw the message “WARNING: EXPERIMENTAL SOFTWARE PASS ‘ 9” appear on our console, followed by the usual “DO NOT INTERRUPT WHILE BOOTING.” Even though we knew that the only risk was that we'd trash our test disk packs, the message still shocked us. It turned out to be a only a harmless leftover from the Master Installation Tape quality assurance process.

Copyright © 1996, 2004 M. E. Kabay. All rights reserved.

One of the participants in my Information Systems Security course reported a case of tampering on a UNISYS mainframe used in a military installation. A user was catching up on his work one evening when suddenly his display showed every single file in all of his disk directories being deleted one by one. Nothing he could do would stop the process, which went on for several minutes.

He reported the incident immediately to his superior officers. Panic ensued until midnight, when the it was found that a program called JOKE.RUN had been assigned to the function key. The program merely listed file names with "DELETING..." in front of each. No files had actually been deleted. Investigation found the programmer responsible; the joke had originally been directed at a fellow programmer, but the redefinition of the function key had accidentally found itself into the installation diskettes for a revision of the workstation software. It took additional hours to check every single workstation on the base looking for this joke. The programmer's career was not enhanced by this incident.

PC Trojans include

- The Scrambler (also known as the KEYBGR Trojan), which pretends to be a keyboard driver (KEYBGR.COM) but actually makes a smiley face move randomly around the screen
- The 12-Tricks Trojan, which masquerades as CORETEST.COM, a program for testing the speed of a hard disk but actually causes 12 different kinds of damage (e.g., garbling printer output, slowing screen displays, and formatting the hard disk)
- The PC Cyborg Trojan (or "AIDS Trojan"), which claims to be an AIDS information program but actually encrypts all directory entries, fills up the entire C: disk, and simulates COMMAND.COM but produces an error message in response to nearly all commands.

1993-1994: Internet monitoring attacks

Trojan attacks on the Internet were discovered in late 1993. Full information about all such attacks is available on the World Wide Web site run by CIAC, the Computer Incident Advisory Capability of the U.S. Department of Energy (http://ciac.llnl.gov/cgi-bin/index/bulletins). On February 3, 1994, CIAC issued Bulletin *E-09: Network Monitoring Attacks*. The Bulletin announced,

> CIAC and other response teams have observed many compromised systems surreptitiously monitoring network traffic, obtaining username, password, host-name combinations (and potentially other sensitive information) as users connect to remote systems using telnet, rlogin, and ftp. This is for both local and wide area network connections. The intruders may (and presumably do) use this information to compromise new hosts and expand the scope of the attacks. Once system administrators discover a compromised host, they must presume monitoring of all network transactions from or to any host "visible" on the network for the duration of the compromise, and that intruders potentially possess any of the information so exposed.
> The attacks proceed as follows. The intruders gain unauthorized, privileged access to a host that supports a network interface capable of monitoring the network in "promiscuous mode," reading

Copyright © 1996, 2004 M. E. Kabay. All rights reserved.

> every packet on the network whether addressed to the host or not. They accomplish this by exploiting unpatched vulnerabilities or learning a username, password, host-name combination from the monitoring log of another compromised host. The intruders then install a network monitoring tool that captures and records the initial portion of all network traffic for ftp, telnet, and rlogin sessions. They typically also install "Trojan" programs for login, ps, and telnetd to support their unauthorized access and other clandestine activities.
>
> System administrators must begin by determining if intruders have compromised their systems. The CERT Coordination Center has released a tool to detect network interface devices in promiscuous mode. Instructions for obtaining and using the tool appears later in this bulletin--the tool is available via anonymous ftp. If a site discovers that intruders have compromised their systems, the site must determine the extent of the attack and perform recovery as described below. System administrators must also prevent future attacks as described below.

CIAC works closely with CERT-CC, the Computer Emergency Response Team Coordination Center of the Software Engineering Institute at Carnegie Mellon University in Pittsburgh, PA. The instructions from CERT-CC included detailed instructions on verifying the authenticity of affected programs and instructions on removing the key vulnerabilities.

A few weeks later, CIAC issued Bulletin E-12, which warned ominously,

> The number of Internet sites compromised by the ongoing series of network monitoring (sniffing) attacks continues to increase. The number of accounts compromised world-wide is now estimated to exceed 100,000. This series of attacks represents the most serious Internet threat in its history.
>
> IMPORTANT: THESE NETWORK MONITORS DO NOT SPECIFICALLY TARGET INFORMATION FROM UNIX SYSTEMS; ALL SYSTEMS SUPPORTING NETWORK LOGINS ARE POTENTIALLY VULNERABLE. IT IS IMPERATIVE THAT SITES ACT TO SECURE THEIR SYSTEMS.
>
> Attack Description
>
> The attacks are based on network monitoring software, known as a "sniffer", installed surreptitiously by intruders. The sniffer records the initial 128 bytes of each login, telnet, and FTP session seen on the local network segment, compromising ALL traffic to or from any machine on the segment as well as traffic passing through the segment being monitored. The captured data includes the name of the destination host, the username, and the password used. This information is written to a file and is later used by the intruders to gain access to other machines.

Finally, another CIAC alert (E-20, May 6, 1994) warned of "A Trojan-horse program, CD-IT.ZIP, masquerading as an improved driver for Chinon CD-ROM drives, [which] corrupts system files and the hard disk." This program affects any MS-DOS system where it is executed.

Copyright © 1996, 2004 M. E. Kabay. All rights reserved.

Hardware Trojans

On November 8, 1994, a correspondent reported to the RISKS Forum Digest that he had been victimized by a curious kind of Trojan:

> I recently purchased an Apple Macintosh computer at a "computer superstore," as separate components - the Apple CPU, and Apple monitor, and a third-party keyboard billed as coming from a company called Sicon.
>
> This past weekend, while trying to get some text-editing work done, I had to leave the computer alone for a while. Upon returning, I found to my horror that the text "welcome datacomp" had been *inserted into the text I was editing*. I was certain that I hadn't typed it, and my wife verified that she hadn't, either. A quick survey showed that the "clipboard" (the repository for information being manipulated via cut/paste operations) wasn't the source of the offending text.
>
> As usual, the initial reaction was to suspect a virus. Disinfectant, a leading anti-viral application for Macintoshes, gave the system a clean bill of health; furthermore, its descriptions of the known viruses (as of Disinfectant version 3.5, the latest release) did not mention any symptoms similar to my experiences.
>
> I restarted the system in a fully minimal configuration, launched an editor, and waited. Sure enough, after a (rather long) wait, the text "welcome datacomp" once again appeared, all at once, on its own.

Further investigation revealed that someone had put unauthorized code in the ROM chip used in several brands of keyboard. The only solution was to replace the keyboard. Readers will understand the possible consequences of a keyboard which inserts unauthorized text into, say, source code. Winn Schwartau has coined the word, "chipping" to refer to such unauthorized modification of firmware.

Diagnosis and prevention

It is difficult to identify Trojans because, like the ancient Horse built by the Greeks, they don't reveal their nature immediately. The first step in catching a Trojan is to run the program on an isolated system. That is, try the candidate either on a system whose hard disk drives have been disconnected or which is reserved exclusively for testing new programs.

While the program is executing, look for unexpected disk drive activity; if your drives have separate read/write indicators, check for write activity on drives.

Some Trojans running on micro-computers use unusual methods of accessing disks; various products exist which trap such programmatic devices. Such products, aimed mostly at interfering with viruses, usually interrupt execution of unusual or suspect instructions and indicate what's happening but prevent the damage from occurring. Several products can "learn" about legitimate events used by proven programs and thus adapt to your own particular environment.

Copyright © 1996, 2004 M. E. Kabay. All rights reserved.

If the Trojan is a replacement for specific components of the operating system, as in the network monitoring problem described by CIAC above, it is possible to compute check sums and compare them with published checksums for the authentic modules.

The ideal situation for a microcomputer user or a system/network manager is to know, for every executable file (e.g., PROG, .COM, or .EXE) on the system

- Where it comes from
- What it's supposed to do.

Take, for example, shareware programs. In general, each program should come not only with the name and address of the person submitting it for distribution but also with the source code. If the requisite compiler is available, one can even compare the object code available on the tape or diskette with the results of a fresh compilation and linkage to be sure there are no discrepancies. These measures make it easier to hope for Trojan-free utilities.

It makes sense for system managers to forbid the introduction of foreign software into their systems and networks without adequate testing. Users wishing to install apparently useful utilities should contact their system support staff to arrange for acceptance tests. Installing software of unknown quality on a production system is irresponsible.

When organizations develop their own software, the best protection against Trojans is quality assurance and testing (QAT). QAT should be carried out by someone other than the programmer(s) who created the program being tested. QAT procedures often include structured walk-throughs, in which designers are asked to explain every section of their proposed system. In later phases, programmers have to explain their code to the QAT team. During systems tests, QAT specialists have to ensure that every line of source code is actually executed at least once. Under these circumstances, it is difficult to conceal unauthorized functions in a Trojan.

Salamis

In the salami technique, criminals steal money or resources a bit at a time. Two different etymologies are circulating about the origins of this term. One school of security specialists claim that it refers to slicing the data thin--like a salami. Others argue that it means building up a significant object or amount from tiny scraps--like a salami.

Round-off errors

The classic story about a salami attack is the old “collect-the-roundoff” trick. In this scam, a programmer modifies the arithmetic routines such as interest computations. Typically, the calculations are carried out to several decimal places beyond the customary 2 or 3 kept for financial records. For example, when currency is in dollars, the roundoff goes up to the nearest penny about half the time and

Copyright © 1996, 2004 M. E. Kabay. All rights reserved.

down the rest of the time. If the programmer arranges to collect these fractions of pennies in a separate account, a sizable fund can grow with no warning to the financial institution.

More daring salamis slice off larger amounts. The security literature includes case studies in which an embezzler removed $0.20 to $0.30 from hundreds of accounts two or three times a year. These thefts were not discovered or reported: most victims wouldn't bother finding the reasons for such small discrepancies. Other salamis use bank service charges--increasing the cost of a check by $0.05, for example.

In another scam, two programmers made their payroll program increase the federal withholding amounts by a few cents per pay period for hundreds of fellow employees. The excess payments were credited to the programmers' withholding accounts instead of to the victims' accounts. At income-tax time the following year, the thieves received fat refunds from Internal Revenue.

In January 1993, four executives of a Value Rent-a-Car franchise in Florida were charged with defrauding at least 47,000 customers using a salami technique. The federal grand jury in Fort Lauderdale claimed that the defendants modified a computer billing program to add five extra gallons to the actual gas tank capacity of their vehicles. From 1988 through 1991, every customer who returned a car without topping it off ended up paying inflated rates for an inflated total of gasoline. The thefts ranged from $2 to $15 per customer--rather thick slices of salami but nonetheless difficult for the victims to detect.

Unfortunately, one would guess, salami attacks are *designed* to be difficult to detect. The only hope is that random audits, especially of financial data, will pick up a pattern of discrepancies and lead to discovery. As any accountant will warn, even a tiny error must be tracked down, since it may indicate a much larger problem. For example, Cliff Stoll's famous adventures tracking down spies in the Internet began with an unexplained $0.75 discrepancy between two different resource accounting systems on UNIX computers at the Keck Observatory of the Lawrence Berkeley Laboratories. Stoll's determination to understand how the problem could have occurred revealed an unknown user; investigation led to the discovery that resource-accounting records were being modified to remove evidence of system use. The rest of the story is told in *The Cuckoo's Egg.*

If more of us paid attention to anomalies, we'd be in better shape to fight the salami rogues. Computer systems are deterministic machines--at least where application programs are concerned. Any error has a cause. Looking for the causes will seriously hamper the perpetrators of salami attacks.

Logic bombs

A logic bomb is a program which has deliberately been written or modified to produce results when certain conditions are met that are unexpected and unauthorized by legitimate users or owners of the software. Logic bombs may be within standalone programs or they may be part of worms (programs that hide their existence and spread copies of themselves within a computer systems and through networks) or viruses (programs or code segments which hide within other programs and spread copies of themselves).
An example of a logic bomb is any program which mysteriously stops working three months after, say, its programmer's name has disappeared from the corporate salary database.

Copyright © 1996, 2004 M. E. Kabay. All rights reserved.

According to a report in the National Computer Security Association section on CompuServe, the Orlando Sentinel reported in January 1992 that a computer programmer was fined $5,000 for leaving a logic bomb at General Dynamics. His intention was to return after his program had erased critical data and get paid lots of money to fix the problem.

In 1985, a disgruntled computer security officer at an insurance brokerage firm in Texas set up a complex series of Job Control Language (JCL) and RPG programs described later as "trip wires and time bombs." For example, a routine data retrieval function was modified to cause the IBM System/38 midrange computer to power down. Another routine was programmed to erase random sections of main memory, change its own name, and reset itself to execute a month later.

Time bombs

Time bombs are a subclass of logic bombs which "explode" at a certain time. The infamous Friday the 13th virus is a time bomb. It duplicates itself every Friday and on the 13th of the month, causing system slowdown; however, on every Friday the 13th, it also corrupts all available disks. The Michelangelo virus tries to damage hard disk directories on the 6th of March. Another common PC virus, *Cascade,* makes all the characters fall to the last row of the display during the last three months of every year.

The HP3000 *ad hoc* database inquiry facility, QUERY.PUB.SYS, had a time-bomb-like bug which exploded after the 1st of January 1990. Users noticed stack overflows when trying to use certain features of the REPORT command. HP quickly sent out patches to fix the problem.

Renewable software licenses

In the movie *Single White Female,* the protagonist is a computer programmer who works in the fashion industry. She designs a new graphics program that helps designers visualize their new styles and sells it to a sleazy company owner who tries to seduce her. When she rejects his advances, he fires her without paying her final invoice. However, the programmer has left a time bomb which explodes shortly thereafter, wiping out all the owner's data. This is represented in the movie as an admirable act.

In the CONSULT Forum of CompuServe, several consultants brazenly admitted that they always leave secret time bombs in their software until they receive the final payment. They seemed to imply that this was a legitimate bargaining chip in their relationships with their customers.

In reality, such tricks can land software suppliers in court.

Gruenfeld (1990) reported on a logic bomb found in 1988. A software firm contracted with an Oklahoma trucking firm to write them an application system. Some time later, the two parties disagreed over the quality of the work. The client withheld payment, demanding that certain bugs be fixed. The vendor threatened to detonate a logic bomb which had been implanted in the programs some time before the dispute unless the client paid its invoices. The client petitioned the court for an injunction to prevent the detonation and won its case on the following grounds:

Copyright © 1996, 2004 M. E. Kabay. All rights reserved.

- The bomb was a surprise--there was no prior agreement by the client to such a device.
- The potential damage to the client was far greater than the damage to the vendor.
- The client would probably win its case denying that it owed the vendor any additional payments.

A legitimate use similar to time-bomb technology is the openly time-limited program. One purchases a yearly license for use of a particular program; at the end of the year, if one has not made arrangements with the vendor, the program times out. That is, it no longer functions. When the license is renewed, the vendor either sends a new copy of the program, sends instructions for patching the program (that is, perform the necessary modifications) or dials up the client's system by modem and makes the patches directly.

Such a program is not technically a time bomb as long as the license contract clearly specifies that there is a time limit beyond which the program will not function properly. However, it is a poor idea for the user. In the opinion of Mr. Gruenfeld,

> What if the customer is told about the bomb prior to entering into the deal? The threat of such a sword of Damocles amounts to extortion which strips the customer of any bargaining leverage and is therefore sufficient grounds to cause rejection of the entire deal. Furthermore, it is not a bad idea to include a stipulation in the contract that no such device exists.

In addition, a time-limited program can cause major problems if the vendor refuses to update the program to run on newer versions of the operating system. Even worse, the vendor may go out of business altogether, leaving the customer in a bind.

My feeling is that if you are paying to have software developed, you should refuse all time-outs. However, if you a simply renting off-the-shelf software such as utilities, accounting packages and so on, it may be acceptable to let the vendor insist on timeouts--provided the terms are made explicit and you know what you're getting into.

If you do agree to time limits on your purchase, you should require the source code to be left in escrow with a legal firm or bank. Don't forget to include the requirement that the vendor indicate the precise compiler version required to produce functional object code identical to what you plan to use.

In summary, if a vendor's program stops working with a message stating that it has timed out, your software contract must stipulate that your license applies to a certain period of use. If it does not, your vendor is legally obligated to correct the time bomb and allow you to continue using your copy of the program.

Copyright © 1996, 2004 M. E. Kabay. All rights reserved.

Circumventing logic bombs

The general class of logic bombs cannot reasonably be circumvented unless the victim can figure out exactly what conditions are causing the bomb. For example, at one time, the MPE-V operating system failed if anyone on the HP3000 misspelled a device class name in a :FILE equation. It wasn't a logic bomb, it was a bug; but the workaround was to be very careful when typing :FILE equations. I remember we put up a huge banner over the console reminding operators to double-check the spelling following the ;DEV' parameter.

Time bombs may be easier to handle than other logic bombs, depending on how the trigger is implemented. There are several methods used by programmers to implement time bombs:

- One is a simple-minded dependence on the system clock to decide if the current date is beyond the hard-coded time limit in the program file; this bomb is easily defused by resetting the system clock while one tries to solve the problem with the originator.
- The second method is a more sophisticated check of the system directory to see if any files have creation or modification dates which exceed the hard coded limit.
- The third level is to hide the latest date recorded by the program in a data file and see if the apparent date is earlier than the recorded date (indicating that the clock has been turned back).

If the time limit has been hard coded without encryption, then a simple check of the program file may reveal either ASCII data or a binary representation of the date involved. If you know what the limiting date is, you can scan for the particular binary sequence and try changing it in the executable file. These processes are by no means easy or safe, so you may want to experiment after a full backup and when no one is on the system.

If the time limit is encrypted, or if it resides in a data file, or if it is encoded in some weird aspect of the data such as the byte count of various innocuous-looking fields, the search will be impracticably tedious and uncertain.

Much better: solve your problems with the vendor before either of you declares war.

Illogic bomb

An interesting legal issue involving logic bombs cropped up a few years ago in Britain. As described in an article in the *Computer Fraud and Security Bulletin,* the events were as follows:

- Early 85: consultant for freight company writes program
- Nov 85: consultant reconfigures system at a second plant

Copyright © 1996, 2004 M. E. Kabay. All rights reserved.

- Jan 86: only four terminals work at first plant; consultant says bug is in screen handler, then goes on holiday.

- Jan 86: system manager locates logic bomb timed to explode 7 Jan 86; program created during initial programming phase. Also locates logic bomb at second plant that would have caused system failure. Date of creation: Jan 86 during consultant's visit.

The consultant was accused of multiple counts of criminal deception. He was acquitted because of a quirk of the British legal system called Section 69:

> Section 69 of the Police and Criminal Evidence Act 1984 governs all computer generated work that is placed before the criminal courts of England and Wales. It states that such evidence will only be submitted if a certificate is provided by the system manager stating ... that there are no reasonable grounds for believing that at all material times, the computer was operating properly, or, if not, that any respect in which it was not operating properly or out of operation could not have affected the production of the print-out document or the accuracy of its contents.

This section thus made it functionally impossible to use computer-generated documentation in a court case in the UK. No one can possibly claim direct knowledge of the absence of tampering. In the case at hand, it was not possible to prove beyond doubt that the audit trail information was beyond tampering; in fact, the defense accused the system manager of having falsified the information because of personal rivalry in a love triangle. Sounds like a soap opera, but it cost a company a great deal of money while the systems were down.

Section 69 makes it highly unlikely that incriminating evidence seized in an accused criminal hacker's own computer system will ever be usable in court. What idiot will certify that his or her own computer, used for hacking, is perfectly correct in providing incriminating data?

Law-makers in other countries, beware. Poorly formulated laws in areas beyond the expertise of legislators may backfire and weaken the rule of law instead of strengthening it.

Data leakage

The most obvious form of unauthorized disclosure of confidential or proprietary data is direct access and copying. For example, Thomas Whiteside writes that in the early 1970s, three computer operators stole copies of 3 million customer names from the Encyclopedia Britannica; estimated commercial value of the names was $1 million. Other cases of outright data theft include

- the Australian Taxation Commission, where a programmer sold documentation about tax audit procedures to help unscrupulous buyers reduce the risks of being audited

- the Massachusetts State Police, where an officer is alleged to have sold computerized criminal records

- the theft of FBI National Crime Information Center data

Copyright © 1996, 2004 M. E. Kabay. All rights reserved.

- o the sale of records about sick people from the Norwegian Health Service to a drug company
- o the misuse of voter registration lists in California, New York City, the U.S. House of Representatives and Sweden.

In June 1992, officers of the Pinellas County sheriff's office were alerted to the theft of subscribers' credit card information from the computers of Time magazine. An analyst working in the customer service offices of the publication in Tampa, Florida was arrested in July. Police found 80,000 names, credit card numbers and expiration dates on diskettes in the accused's home. As far as the police knew, the only purchasers of the data were undercover agents who bought 3,000 credit card numbers at a dollar each.

Ordinary diskettes can hold more than a megabyte of data; optical disks and special forms of diskette can hold up to gigabytes. Ensure that everyone in your offices using PCs or workstations understands the importance of securing diskettes and hard drives to prevent unauthorized copying. The effort of locking a system and putting diskettes away in secure containers under lock and key is minor compared to the possible consequences of data leakage.

Electronic mail can also be a channel for data leakage. For example, in September 1992, Borland International accused an ex-employee of passing trade secrets to its competitor--and his new employer--Symantec Corporation. The theft was discovered in records of MCI Mail electronic messages allegedly sent by the executive to Symantec.

In November 1992, NASA officials asked the FBI to investigate security at the Ames Research Center in Mountain View, California. An internal audit had revealed “major, major indication of potential violations of national security.” Both the Washington Post and United Press International had stories on the problems, presumed to be cases of data leakage.

A case of data leakage via Trojan occurred in October 1994, when a ring of criminal hackers operating in the United States, England and Spain stole the telephone calling card numbers of 140,000 subscribers of AT&T Corp, GTE Corp, Bell Atlantic and MCI Communications Corp. These thefts are estimated to have resulted in U$140 million of fraudulent long distance calls. In a significant detail, Ivy James Lay, a switch engineer working for MCI, was known in criminal hacker circles as “Knight Shadow.” He was accused of having inserted Trojan horse software to record calling-card and ordinary credit-card numbers passing through MCI's telephone switching equipment. European confederates, led by 22-year old Max Louarn, of Majorca, Spain, paid him for the stolen data, then set up elaborate call centers through which users could make overseas calls.

Copyright © 1996, 2004 M. E. Kabay. All rights reserved.

Steganography and inference

Unfortunately, there are more subtle ways of stealing information. Security specialists have long pointed out that information can be carried in many ways, not just through obvious printed copies or outright copies of files. For example, a programmer may realize that (s)he will not have access to production data, but the programmer's programs will. So (s)he can insert instructions which modify obscure portions of the program's output to carry information. Insignificant decimal digits (e.g., the 4th decimal digit in a dollar amount) can be modified without exciting suspicion. Such methods of hiding information in innocuous files and documents are collectively known as “steganography.”

Charles Pfleeger points out that even small amounts of information can sometimes be valuable; e.g., the mere existence of a specific named file may tell someone what they need to know about a production process. Such small amounts of information can be conveyed by any binary operations; i.e., anything that has at least two states can transmit the knowledge being stolen. For instance, one could transmit information via tape movements, printer movements, lighting up a signal light, and so on.

The wide variety of covert channels of communication make it impossible to stop data leakage. The best you can do is to reduce the likelihood of such data theft by enforcing strong quality assurance procedures on all code developed in-house. For example, if there are test suites which are to produce known output, even fourth decimal point deviations can be spotted. This kind of precision, however, absolutely depends on automated quality assurance tools. Manual inspection is not reliable.

The same preventive measures applied to detect Trojans and bombs can help stop data leakage. Having more than one programmer be responsible for each program can make criminality impossible without collusion--always a risk for the criminal. Random audits can make increase the risk of making improper subroutines visible. Walkthroughs force each programmer to explain just what that funny series of instructions is doing and why.

Again, the best defense starts with the educated, security-conscious employee.

Extortion

Computer data can be held for ransom. For example, according to Whiteside, in 1971, two reels of magnetic tape belonging to a branch of the Bank of America were stolen at Los Angeles International Airport. The thieves demanded money for their return. The owners ignored the threat of destruction because they had adequate backup copies.

In 1973, a West German computer operator stole 22 tapes and received $200,000 for their return. The victim did not have adequate backups.

In 1977, a programmer in the Rotterdam offices of Imperial Chemical Industries, Ltd. (ICI) stole all his employer's tapes, including backups. Luckily, ICI informed Interpol of the extortion attempt. As a result of the company's forthrightness, the thief and an accomplice were arrested in London by officers from Scotland Yard.

Copyright © 1996, 2004 M. E. Kabay. All rights reserved.

Clearly, one of the best defenses against extortion is to have adequate backups. Another is to encrypt sensitive data so they cannot be misused even if they're stolen.

A Public Broadcasting System (PBS) television show in early 1993 reported that there are rumours that unscrupulous auditors have occasionally blackmailed white collar criminals found during audits.

The best way to prevent embarrassment or blackmail during an audit is to run internal audits. Support your internal audits staff. Explain to them what you need to protect. Point out weak areas. Better to have an internal audit report that supports your recommendations for improved security than to have a breach of security cost your employer reputation and money.

Another form of extortion is used by dishonest employees who are found out by their employers. When confronted with their heinous deeds, they coolly demand a letter of reference to their next victim. Otherwise they will publicize their own crime to embarrass the their employer. Many organizations are thought to have acceded to these outrageous demands. Some scoundrels have even asked for severance pay--and, rumor has it, they have been paid.

Such narrow defensive strategies are harming society's ability to stop computer crime.

Hiding a problem makes it worse. A patient who conceals a cancer from doctors will die sooner rather than later. Organizations that conceal system security breaches make it harder for all system managers to fight such attacks. Victims should report these crimes to legal authorities and should support prosecution.

I will return to this topic in the section on prosecuting criminal hackers later in this text.

Forgery

Criminals have produced fraudulent documents and financial instruments for millennia. Coins from ancient empires had elaborate dies to make it harder for low-technology forgers to imitate them. Even thousands of years ago, merchants knew how to detect false gold by measuring the density of coins or by testing the hardness of the metal. Cowboys in Wild-West movies occasionally bite coins, much to the mystification of younger viewers.

Copyright © 1996, 2004 M. E. Kabay. All rights reserved.

Whiteside provides two particularly interesting cases of computer-related forgery. The most ingenious involved a young man in Washington, DC, who printed his own account's routing numbers in magnetic ink at the bottom of the deposit slips you usually find in bins at any bank. He replaced the blank deposit slips by the doctored ones. Hundreds of people used these slips to deposit money to what they assumed would be their accounts. The victims wrote their own account numbers in, handed their money and the slips to tellers, and their accounts were apparently credited as usual. In fact, however, all the slips with magnetic ink were automatically sorted and processed, diverting $250,000 of other people's money into the criminal's bank account. When customers complained about their bouncing checks, the bank discovered too late that the thief had fled, taking $100,000 along with him.

If a teller had observed that customers were writing in account numbers different from the magnetically-imprinted codes at the bottom of each deposit slip, the fraud would have been impossible.

The other case cited by Whiteside concerned checks which were fraudulently printed with the name and logo of a bank in New York but with the routing numbers and false account number from a totally different bank on the west coast. The criminal deposited the check at a third bank. The check would automatically be routed by the Federal Reserve System according to the magnetic ink codes, ending up in the processing hopper of the west coast bank. There, not having a valid account number, the check would pop out for human handling. The clerk responsible for exceptions would immediately see the prominent logo of the New York bank and send it there by mail. Days would pass before the check ended up in New York. Of course, the New York bank's automatic check processing equipment would respond to the fake routing code and send it back to the Fed, and so it went in an endless loop. Apparently the farce ended only when the checks became so worn that they required physical repair. The inconsistency was finally noticed by a human being and the deception was discovered. Unfortunately, by this time the thief had absconded with about $1 million.

Once again, human awareness and attention could have foiled the fraud.

Desktop forgery

But things are getting worse. Forgers have gone high-tech. It seems nothing is sacred any more, not even certificates and signatures.

A fascinating article in *Forbes Magazine* in 1989 showed how the writer was able to use modern desktop publishing (DTP) equipment to create fraudulent checks. He used a high-quality scanner, a PC with good DTP and image-enhancement (touch-up) programs and high-resolution laser printers. The total cost of such a system at this writing (Spring 1995) is about $3,000-$5,000 in all. Color copiers and printers have opened up an even wider field for forgery than the monochrome copiers and printers did.

The *Forbes* article and other security references list many examples of computer-related forgeries. A Boston resident forged checks by digitizing company logos and printing them on check stock. He defrauded computer suppliers and sold stolen computers all over the Caribbean. Another forger generated official-looking documents from the Connecticut Bank & Trust company attesting to his financial reliability. Using these references, he is alleged to have borrowed more than $10 million and then filed for bankruptcy after moving the money offshore. A European thief deposited and then

Copyright © 1996, 2004 M. E. Kabay. All rights reserved.

withdrew $3 million in fake cashier's checks made with a laser printer and a color copier. Prisoners even managed to effect their own release by sending a FAX of a forged document to their prison officers.

In December 1992, California State Police in Los Angeles arrested 32 people for issuing fake smog control certificates. Each certificate sold for about $50. Another forgery case involved the CIA--as victims, not perpetrators (for a change). In October 1992, Joseph P. Romello pleaded guilty to having defrauded the CIA of more than $1.2 million. In one of his crimes, he tricked the Agency into paying $708,000 for nonexistent computer hardware and provided forged documents for the files showing that the equipment had been received.

You should verify the authenticity of documents before acting on them. If a candidate gives you a letter of reference from a former employer, verify independently that the phone numbers match published information; call the person who ostensibly wrote the letter; and read them the important parts of their letter.

Financial institutions should be especially careful not to sign over money quickly merely because a paper document looks good. Thorough verification makes sense in these days of easy forgery.

Fake credit cards

Credit cards have become extensions of computer databases. In most shops where cards are accepted, sales clerks pass the information encoded in magnetic strips through modems linked to central databases. The amount of each purchase is immediately applied to the available balance and an authorization code is returned through the phone link.

The Internet RISKS bulletin distributed a note in December 1992 about credit card fraud. A correspondent reported on two bulletins he had noticed at a local bookstore. The first dealt with magnetically forged cards. The magnetic stripe on these fraudulent cards contains a valid account code that is different from the information embossed on the card itself. Since very few clerks compare what the automatic printers spew forth with the actual card, thieves successfully charge their purchases to somebody else's account. The fraud is discovered only when the victim complains about erroneous charges on the monthly bill. Although the victim may not have to pay directly for the fraud (the signature on the charge slip won't match the account owner's), everyone bears the burden of the theft by paying higher credit card fees.

In one of my classes, a security officer from a large national bank explained that when interest rates on unpaid balances were at 18%, almost half of that rate (8%) was assigned to covering losses and frauds.

In January 1993, a report on the Reuter news wire indicated that credit card forgery is rampant in southeast Asia. Total losses worldwide reached $1 billion in 1991, twice the theft in 1990. In a single raid in Malaysia in August 1992, police found 2,092 fake cards simulating MasterCard, VISA and American Express. The use of digitized photographs embedded in the cards themselves will help make counterfeiting more difficult.

Those of you whose businesses accept credit cards should cooperate closely with the issuers of the cards. Keep your employees up to date on the latest frauds and train them to compare the name on the card itself with the name that is printed out on the invoice slip. If there is the slightest doubt about the

Copyright © 1996, 2004 M. E. Kabay. All rights reserved.

legitimacy of the card, the employee should ask for customer identification or consult a supervisor for help.

Ultimately, it may become cost-effective to insist on the same, rather modest, level of security for credit cards as for bank cards: at least a PIN (personal identification number) to be entered by the user at the time of payment. There are, however, difficulties in ensuring the confidentiality of such PINs during telephone ordering. A solution to this problem is variable PINs generated by a "smart card:" a micro-processor-equipped credit card which generates a new PIN every minute or so. The PIN is cryptographically related to the card serial number and to the precise date and time; even if a particular PIN is overheard or captured, it is useless a very short time after the transaction. Combined with a PIN to be remembered by the user, this system may greatly reduce credit-card fraud.

Illegally copied software

In Chapter 4, I will discuss the legal implications of using stolen software. Here, I want to alert you to the danger of buying or downloading illegally copied software.

In October 1992, Microsoft announced that U.S. Marshals had seized more than 150,000 copies of counterfeit MS-DOS Version 5 software. The packages included authentic looking details such as holograms, diskette labels and manuals. The police had to use 16 eighteen-wheeler trucks to cart away the evidence. Under current U.S. Copyright law, maximum fines are $25,000 and imprisonment up to a year, or both. However, if new legislation before the U.S. Senate actually passes, penalties will rise to a maximum of $250,000 and up to five years in jail.

In the years since that major bust, there have been several other cases reported of large-scale counterfeiting. Much of the crime has been based in mainland China, where factories have been pumping out sophisticated copies of every major product on the software market. Conditions have become so bad that the Chinese government has been cracking down on industrial-scale software theft not only to respond to foreign pressure but also because home-grown software firms find it hard to pay for their investments and employees when over 95% of all Chinese software is copied illegally. In an investigation in April 1995, investigators found over 97% of all software in use in Eastern Europe and the former Soviet Union to be stolen.

A major channel for distribution of stolen software is pirate bulletin board systems. These amateur systems have occasionally reached semi-professional status, with one Montreal pirate operation grossing over C$200,000 a year in membership fees from people all over the world. Employees must be warned never to download proprietary software from such boards for their own use or for corporate use. Not only is it illegal, it's dangerous: the stolen software is not usually checked for viruses or Trojans, and some participants seem to find it amusing to insert such features in the code they upload to the BBS.

La Presse, the largest newspaper in the greater Montreal area, published a news story about major raids on pirate BBS. Translation and summary of the 13 April 1995 article posted to *RISKS Forum Digest* by MK):

> Major Strike by the RCMP in the InfoBahn
> [Gros coup de la GRC dans l'inforoute]

Copyright © 1996, 2004 M. E. Kabay. All rights reserved.

by Eric Trottier, La Presse

The RCMP has decided to do a little house-cleaning in the joyously anarchic world of the electronic highway.

Thanks to a computer-science infiltration operation, the federal police yesterday dismantled 11 bulletin boards that were trafficking in tens of thousands of software packages around the world.

"It's the first time we have been able to implement this type of penetration of BBSs. Even in the U.S., the most important dragnet of this type has so far only allowed the dismantling of six BBSs at a time," said Sergeant Serge Corriveau to *La Presse* shortly after the investigators completed more than a dozen penetrations and seized more than C$200,000 [U$140,000] of computer equipment.

Key points from the article:

- News of the raid spread rapidly through the Internet;
- The 11 BBSs were involved in large-scale fraud in N.America and Europe. Subscription fees of C$30-C$50 per month allowed participants to download copies of proprietary software at will.
- "Everything available legally on the market was offered by these BBSs," said Sgt Corriveau.
- Some of the more audacious BBSs offered beta copies of Windows95.
- There are about 700 BBSs in the greater Montreal area; the RCMP estimate that three-quarters of them traffic in stolen software.
- Some of the BBS have become virtual flea markets of pornography, bomb-making instructions, and details of how to succeed at suicide.
- In one of the shut-down systems, stolen goods and illegal assault weapons were advertised for sale.
- It has taken a year to infiltrate the BBSs; some officers had to wait up to four months to gain entrance to the inner areas of the boards they were investigating.
- The raids involved 75 officers in Montreal, Outremont, Repentigny, Longueuil, Saint-Amable, and the St-Jerome area.
- The BBSs shut down are: Notice, Twins, Red Alert, Perfect Crime, Beyond Corruption, Line-Up, Wolf Pack, On the World, Restricted Area and Necromancer Mecon.

Copyright © 1996, 2004 M. E. Kabay. All rights reserved.

- Most had about 6 telephone lines for full-time access, serving 100-250 clients, with some in Europe. The largest, Notice, had 350 clients who each paid $50/month, for an untaxed revenue of C$210,000 per year.

- The police estimate that 11 to 15 criminal hackers will be indicted as a result of the raids. They each face fines of C$25,000 to C$100,000.

Some of the software on the boards has been hacked to include fraudulent variations on well-known company names. "Microsloth" and "WurdPerfict" are examples. Any software which even looks like proprietary software should be evaluated carefully to see if it is a modified stolen copy.

As a consumer of software, you should register your purchase at once. That way, if you have been sold counterfeit goods, you will find out at once and perhaps be able to participate in stopping a crime. Who knows: you may end up with free software for life from a grateful software vendor.

Arguments excusing software theft

Some of the arguments employees (or your children!) will advance to defend the practice of software theft should be met immediately and squashed. Here are classic defenses of illegal copying [and some suggested discussion points]:

- Everyone's doing it. [Response: so what? Doesn't make it right or even legal.]

- We won't get caught. [Response: so what? Being caught has no bearing on whether the act is moral or legal.]

- It's the company's fault: if they don't want theft, they should charge less. [Response: rubbish. First of all, even shareware authors get cheated by people who use their software without paying for it--and these are packages for which the authors ask for a few dollars. Secondly, the owner of the software has no obligation to meet someone else's view of appropriate pricing. Thirdly, no one has a right or entitlement to use proprietary software; if you don't like the price, find a more cost-effective alternative.]

- But I need it and I can't afford to pay it. [Response: so? Going to rob a bank tomorrow? Or why not just mug someone?]

- It doesn't hurt anyone. [Response: yes it does. Stealing software makes theft by others even more likely.]

- It only hurts a company--I wouldn't steal it from an individual. [Response: the company is a group of people who agree to work together according to terms they agree on. Steal from the company and you steal from employees, owners and other stakeholders. You may even hurt honest users by contributing to higher prices.]

Copyright © 1996, 2004 M. E. Kabay. All rights reserved.

- No software should every be copyrighted--it should always be free. [Response: do you earn a salary? Why don't you donate your time? Do you pay for goods in a store? Why not decide that it should be free and just steal it?]

As professionals involved in using and managing information systems, we have a duty to society to speak out against the perverse values which condone theft. Don't let a single case of software theft go by without objecting to it.

Simulation

Using computers in carrying out crime is nothing new. Organized crime uses computers all the time, according to August Bequai. He catalogs applications of computers in gambling, prostitution, drugs, pornography, fencing, theft, money laundering and loan-shark operations.

A specialized subset of computer-aided crime is simulation, in which complex systems are emulated using a computer. For example, simulation was used by a former Marine who was convicted in May 1991 of plotting to murder his wife. Apparently he stored details of 26 steps in a "recipe" file called "murder." The steps included everything from "How do I kill her?" through "Alibi" and "What to do with the body."

If it is known that you will carry out periodic audits of files on your enterprise computer systems, there's a better chance that you will prevent criminals from using your property in carrying out their crimes. On the other hand, such audits may force people into encrypting incriminating files. Audits may also cause morale problems, so it's important to discuss the issue with your staff before imposing such routines.

Simulation was used in a bank fraud in England in the 1970s. A gang of thieves used the system for a complex check kiting operation. Now, check kiting consists of writing checks alternately from one bank to another faster than the float period during which the deposit exists in the receiving bank but before it has been deducted from the issuing bank. The apparent amount rises like a kite as money shuttles back and forth. Then one day the criminal clears all the money out of the accounts and disappears. Naturally, banks know all about this trick, so any repeated sequence of deposits and withdrawals from one account to another results in a freeze on the accounts until the money actually clears. Knowing this restriction, the criminals in England used 12 banks to shuttle money around. The scheme would have worked if the computer hadn't broken down. Scotland Yard were alerted to a rash of bad checks all over London. They traced the conspirators back to a back room where a computer programmer was desperately trying to fix his broken computer system. He had no backup hardware.

Implications

I see the following major implications from this survey of computer crime techniques:

- Crime is not primarily a technical issue. Human awareness and commitment to security accomplish more than blind dependence on technological solutions alone.

Copyright © 1996, 2004 M. E. Kabay. All rights reserved.

- Personnel management plays a crucial role in establishing a corporate culture in which information is treated with as much care as money.
- Audit trails play an important role in deterring and detecting crime.
- Computer crime, like other crime, should be reported and analyzed.

Copyright © 1996, 2004 M. E. Kabay. All rights reserved.

CHAPTER NOTES

1. On computer crime in general:

Denning, Dorothy E. (1991). The United States vs. Craig Neidorf: a debate on electronic publishing, constitutional rights and hacking. *Communications of the ACM* 34(3):24

Denning, Dorothy E. (1991). Denning's rebuttal. *Communications of the ACM* 34(3):42

Garfinkel, S. & G. Spafford (1991). *Practical UNIX Security.* O'Reilly & Associates, Inc. (Sebastopol, CA). ISBN 0-937175-72-2.

Kabay, M. E. (1993). Viruses should not be protected by First Amendment. *Network World* 10(9):27 (Mar 1, 1993).

Parker, D. B. (1988). *Computer crime update.* DROIS #IS09-200-051.

Parker, D. B. (1983). *Fighting Computer Crime.* Scribner's (New York). Republished as Computer crime methods, DROIS #IS09-200-101.

Parker, D. B., S. Levy, E. Spafford, P. Hawthorn, M. Rotenberg, J. J. BloomBecker, R. Stallman (1991). Colleagues debate Denning's comments. *Communications of the ACM* 34(3):33

Stoll, C. (1989). *The Cuckoo's Egg: Tracking a Spy through the Maze of Computer Espionage.* Pocket Books (New York). ISBN 0-671-72699-9.

Whiteside, T. (1978). *Computer Capers: Tales of Electronic Thievery, Embezzlement, and Fraud.* New American Library (New York). ISBN 0-45162080-1.

2. Information warfare

Desmond, J. (1985). International terrorism: clear and present danger. *Computerworld* 18(53):15

Kabay, M. E. (1995). Information warfare. Canadian Security Intelligence Service *Commentary*, in press. Will be available for download from NCSA Forum library on OPSEC/InfoWar.

Schwartau, W. (1994). *Information Warfare: Chaos on the Electronic Superhighway.* Thunder's Mouth Press, New York. ISBN 1-56025-080-1. 432. Index.

Schwartau, W. (1991). *Terminal Compromise.* Inter.Pact Press (Seminole, FL). ISBN 0-962-87000-5.

Security Insider Report, W. Schwartau, ed. Inter.Pact Press / 11567 Grove Street North / Seminole, FL 34642.

Copyright © 1996, 2004 M. E. Kabay. All rights reserved.

3. Data diddling

Neumann, P. G. (1992). Fraud by computer. AInside RISKS" Column. *Communications of the ACM* 35(8):154.

Pacenti, J. (1993). Rental-Car Fraud. *Associated Press Newswire* 92.01.08 " 22:53

4. Sabotage

Fredell, Eric (1988). Peace activist found guilty of wrecking DOD computer. *Government Computer News* 7(1):8 (Jan 8, 1988)

Schultz, B. (1978). Report calls DP at DOD harmful to U.S.security. *Computerworld* 12(32):1
Taylor, A. (1980). Protection still lacking from internal sabotage. *Computerworld* 14(9):31

5. Scavenging

Anonymous (1987). Secure destruction of waste media: a review. *Datapro Reports on Information Security* report #IS48-050-101.

Benson, M. (1978). ARagpicker" finds riches in software scraps. *Computerworld* 12(38):26.

Swiss, T. (1992). Similar but different user interfaces and traces of memory. RISKS-L (RISKS Forum Digest of the ACM, P. G. Neumann, moderator) 14(15) [92.12.07]

This article describes the problems of memory traces on PCs and workstations. It is published in the electronic subscription list, open to all, called RISKS-L: FORUM ON RISKS TO THE PUBLIC IN COMPUTERS AND RELATED SYSTEMS. ACM Committee on Computers and Public Policy, Peter G. Neumann, moderator. To subscribe, send a request containing only the words ASUBSCRIBE <id>" (without quotation marks and including your Internet ID in place of the symbol <id>) to risks-request@csl.sri.com via the Internet.

6. Trojan Horse programs

Bullfinch, T. (1855). *The Age of Fable.* Reprinted in *Bullfinch's Mythology* in the Modern Library edition. Random House (New York).

7. Logic bombs

Anonymous (1992). FBI investigating security at NASA center. *UPI Newswire* 92.11.18 " 00:17.

Anonymous (1990). Section 69. *Computer Fraud and Security Bulletin* April, 1990. Elsevier Advanced Technology Publications, Crown House, Linton Road, Barking, Essex, IG11 8JU, U.K. Phone 01-594-7272.

Anonymous (1990). The hacker's friend. *Computer Fraud and Security Bulletin* April, 1990. Elsevier Advanced Technology Publications.

Copyright © 1996, 2004 M. E. Kabay. All rights reserved.

Gruenfeld, L. (1990). Pay up or bombs away. *Computerworld* 24(25):23 (18 June 90).

Joyce, E. L. (1988). Time bomb: insider the Texas virus trial. *Computer Decisions* 20(12):38. This paper discusses a time bomb, not a virus.

Polilli, S. (1988). Texas hunts virus villains; first defendant charged with sabotage. *Software Magazine* 8(12):26

Sawyer, K. (1992). FBI probes NASA research center in California; earlier internal review found Amajor indication" of possible national security violations. *Washington Post Newswire* 92.11.20.

8. Data leakage

Pfleeger, C. P. (1989). *Security in Computing.* Prentice-Hall (Englewood Cliffs, NJ). ISBN 0-13-798943-1.

9. Forgery

Anonymous (1992). Microsoft raids lead to largest counterfeit.... *OTC Newswire* (92.10.07 " 13:26).

Anonymous (1992). Smog check sweep. *AP Newswire* 92.12.18 " 11:00.

Charbuck, D. (1989). Desktop forgery. *Forbes* (Nov 27, 1989):246
Hamid, A. J. (1993). Credit card forgery rampant in S.E. Asia. *Reuter Newswire* 93.01.06 " 04:25.

Leichter, J. (1992). Latest (?) credit card scams. Internet *RISKS-L* (RISKS Forum Digest of the ACM, P. G. Neumann, moderator) 14(20) [92.12.31]

10. Computers in crime

Bequai, A. (1987). *Technocrimes: The Computerization of Crime and Terrorism.* Lexington Books (Lexington, MA). ISBN 0-669-13842-8.

Cox, T. (1992). Conviction upheld in "recipe murder." *UPI Newswire* 92.07.21 " 00:16.

Copyright © 1996, 2004 M. E. Kabay. All rights reserved.

NCSA Guide to Enterprise Systems Security

M. E. Kabay, Ph.D.
Associate Professor, Information Assurance
Dept. of Computer Information Systems
Norwich University, Northfield, VT 05663-1035 USA

Copyright ©1996, 2004 M. E. Kabay. All rights reserved.

The following is an excerpt from

Kabay, M. E. (1996). *The NCSA Guide to Enterprise Security: Protecting Information Assets*. McGraw-Hill (New York). ISBN 0-07-033147-2. (now out of print)

Chapter 3: Computer viruses

After studying this chapter, the reader should be able to

1. define computer viruses and worms and describe their effects.
2. describe the history of self-reproducing programs and how they work.
3. define the extent of the virus problem in terms of prevalence, diversity and severity.
4. recognize characteristic virus behaviour.
5. define approaches to diagnosis, recovery and prevention of viral infection.
6. discuss why people write viruses and explain why viruses are rare outside the PC and Macintosh worlds (e.g., UNIX, LANs, mainframes).
7. discuss the implications and repercussions of the Internet Worm of 1988.
8. discuss the possibilities of helpful viruses.
9. discuss policy issues such as outlawing publication of functional viral codes.

Rogue software

Science fiction authors have long written about artificial life forms. In the early 1970s, author David Gerrold named a program VIRUS and imagined it spreading from computer to computer through phone linkages. Others imagined life-forms evolving in computer networks and

predators seeking them out and destroying them. It was a common joke among science fiction fans that one day the North American telephone grid would develop consciousness.

It isn't entirely science fiction any more.

Computer organisms are reproducing worldwide. Some are mutating at a furious rate, spawning offspring in the blink of an eye. Aggressive anti-virus programs (AVPs) contend with viruses in memory and on disk. With the help of unethical, immoral, careless, stupid or crazy virus authors, viruses evolve in response to selection pressures, hiding themselves in new niches of the computer universe, or "cyberspace." Virus authors even take ideas from each other's viruses, leading to a form of primitive viral sexuality.

Because of the popularity of virus stories in the popular press, you have probably been asked about viruses by your friends, family and colleagues. This chapter provides the information you need to discuss viruses intelligently and to set rational company policies for preventing and resolving virus infections. It also presents some of the policy issues facing our society as cyberspace becomes more richly populated.

What are viruses and worms?

Viruses are little programs that copy themselves into "host" programs or into special executable "bootstrap" areas of disks. Once these infected programs are executed, the computer viruses, like biological viruses, subvert the normal functions of the operating system (OS). These parasitic programs commandeer CPU, memory and disk resources to replicate themselves. They insert themselves into other programs, thus spreading the infection. When victims distribute infected programs and diskettes, the viruses extend their range. Computer viruses even show some parallels to sexual reproduction: they can exchange "genetic" material through the agency of the twisted human beings who enjoy creating harmful programs and who share their knowledge with each other.

Worms are free-standing programs which replicate, usually in networks. They do not integrate their code into host programs.

The popular press has confused the public about these distinctions and seems to apply the word "virus" to practically any kind of computer problem, whether involving replicating code or not. During the Michelangelo scare of 1992, parents were reported as having threatened to take their children out of school for fear the computer virus would affect their health. Several callers to the NCSA virus hotline asked whether viruses could enter their computer through the power cord.

In January 1992, *U.S. News and World Report* published an article about the "Iraqi Virus" that had been used by the US in the Gulf War against Iraq. This virus was supposed to have been inserted in the printer ROMs of equipment sent to the Iraqis before the war. The report gained wide publicity through the work of a television news show. Unfortunately, the report was based

on an April Fool's joke published in 1991. Despite irrefutable proof of its origin, the story has never been retracted.

What do viruses do?

Computer viruses insert their own executable instructions into the normal code of their hosts. Except for the “overwriting” viruses, no functional virus deliberately damages the program it infects. A virus which causes problems in execution of its host will be discovered too quickly to replicate.

Never harmless

Some computer viruses may be intended to be harmless. Unfortunately, virus writers often write bad code, so their viruses have bugs. Virus authors fail to take into account changes in OS versions--and you can't order an upgrade to your current virus version from your neighbourhood store. These people are testing their programs on our computers--without our permission.

Other viruses are obviously intended to do harm. Their “payloads” include nasty messages clearly identifying the damage they cause or are designed to cause.

Whether intentionally or not, viruses have been observed to

- destroy a disk directory, making it impossible to retrieve your files without special repair utilities;
- erase or modify specific programs or data files;
- interfere with program functions (e.g., slowing down processing);
- create bad sectors on disk;
- decrease disk free space;
- write unwanted volume labels on disks;
- format all or part of a disk;
- use up portions of RAM;
- hang a system, forcing a reboot;
- interfere with screen displays.

Even when viruses do not in fact cause any tangible or visible harm, their mere presence casts into doubt the integrity of all the programs and data in the infected system.

As for scary messages such as “Now erasing hard disk,” I expect to learn one day that a victim will have been found dead of a heart attack. In front of this unfortunate person will be a screen display announcing some horrifying attack on their computer. I wonder if we will ever see a virus author convicted of manslaughter?

Wasting time

Even trivial effects can have a noticeable effect on productivity. Fridrick Skulason, creator of FPROT (a well-known anti-virus product, or AVP), reported at an NCSA conference that he had tried the experiment of allowing the Ping-Pong virus (also known as the Italian or Bouncing Ball virus) to continue sending a blip back and forth all over his screen while he was trying to work on a paper. After half an hour he had a headache and felt very irritated with the creator of this pesky virus.

In a session of the *Information Systems Security* course, a participant reported a case in which a secretary enquired politely if it was possible to “turn off the screen saver in WordPerfect.” The entire 12-PC secretarial pool was under the impression that their word processing software came with an undocumented feature--a bouncing ball that moved all over the screen.

Viruses even affect productivity of people's whose PCs weren't infected. This phenomenon is known as the water-cooler effect. Observers have seen an entire day lost when even a single microcomputer is affected by a virus. Coworkers spend longer on breaks discussing the virus; they congregate at the water cooler and spend valuable time recounting anecdotes about the virus infections their friends have experienced, the virus infections their spouse's friends experienced, and the virus infections they have read about in the computer magazines they read.

Finally, viruses interfere with technical support. Naive users are all too ready to ascribe any problem to viruses. Help-desk staff have reported cases of the Bad-Version Virus, the I-Purged-the-File-but-Forgot Virus, the I-Was-Saving-a-File-When-the-Power-Failed Virus and the Computer-Plug-Fell-Out-of-the-Wall Virus. Convincing the befuddled user to go through systematic diagnosis under these conditions can be a strain on both parties.

History of malicious code

In a special report for DROIS, Reed Phillips described the origins of viruses as stretching back to the work of von Neumann in the late 1940s on self-reproducing automata. In the 1960s, programmers at Bell Labs were playing “Core Wars” on their mainframe computers. Programs would be launched with the goal of seizing as much memory as possible by reproducing and preventing other programs from reproducing.

Worms

In 1970, Bob Thomas of Bolt, Beranek and Newman launched a demonstration program through the ARPANET, one of the original components of what eventually became the Internet. The

program replicated and moved through the network, displaying the message, “I'm the creeper, catch me if you can!” Another program, called the Reaper, chased the Creeper and destroyed it.

Early viruses

According to Spafford and others, Apple II microcomputer users invented computer viruses in the early 1980s. Spafford lists these early viruses as Festering Hate, Cyberaids and Elk Cloner. In 1983, Fred Cohen created a self-replicating program for a VAX 11/750 mainframe at the University of Southern California. His thesis advisor, Len Adelman, suggested calling it a virus. Cohen demonstrated the virus to a security class. Cohen continued his work on viruses for several years; his Ph.D. thesis presented a mathematical description of the formal properties of viruses. He also defined viruses neatly and simply as “A computer program that can infect other computer programs by modifying them to include a (possibly evolved) copy of itself.”

Late 1987: a rash of viruses in the U.S.

On October 22, 1987, a virus apparently written by two brothers in Lahore, Pakistan was reported to the Academic Computer Center of the University of Delaware in Newark. This virus destroyed the data on several hundred diskettes at U of D and also at the University of Pittsburgh School of Business. It destroyed the graduate thesis of at least one student.

In November 1987, students at Lehigh University in Bethlehem, PA began complaining to the staff at the computer centre that they were getting bad diskettes. At one point, 30 students returned diskettes in a single day. It turned out that there was a virus adding itself to the COMMAND.COM file on the DOS system diskettes. When the Lehigh staff examined the virus, they discovered that it was programmed to copy itself four times after each infection. On the fourth replication for any given copy, the virus would destroy the file allocation table of the diskette or hard disk, making the data unrecoverable (at that time, there were no utilities available for reconstituting files easily once the pointers from cluster to cluster on the disk had been lost). Several hundred students lost their data. As Phillips points out, it is simple luck that the Lehigh virus was spotted and disinfected before students took diskettes home with them for the Thanksgiving break. Release into the wider world could have had even worse results than the localized outbreak.

In December 1987, a German student released a self-reproducing program that exploited electronic mail networks on the ARPANET and BITNET networks. This program would display the request, `Please run me. Don't read me.' While the victim ran the program, it displayed a Christmas tree on screen; at the same time, it used the victim's email directory and automatically sent itself to everyone on the list. Because this rogue program did not embed itself into other programs, experts call it the Christmas-Tree Worm.

Unfortunately, this worm had no mechanism for remembering where it had come from. Since most people to whom we write include our names in their address list, the worm usually mailed itself back to the computer system from which it had originated as well as to all the other

computer systems named in the victim's directory. This reflection from victim to infector reminds me of an uncontrolled nuclear chain reaction. The greater the number of cross references among email address directories, the worse would be the growth of the worm.

The original version of this worm worked only on IBM VM/VMS mainframe computers; luckily, there weren't very many of them on the ARPANET and BITNET networks. However, a source-code version of the worm was installed into the IBM internal email network and recompiled. Because of the extensive cross-references in the email system, where many employees corresponded with hundreds of other employees, the worm reproduced explosively. According to Phillips, the network was clogged for three hours before IBM experts identified the problem, wrote an eradicator, and eliminated the worm.

Also in December 1987, Richard Brandow, publisher of *MacMag* in Montreal, hired a programmer to write the first political propaganda virus. This virus was a logic bomb with a trigger date of March 2, 1988; on that date, it would display the `Universal Message of Peace' from Brandow on all affected machines and then delete itself. Brandow deliberately placed infected programs on the CompuServe and Genie networks. Brandow is alleged to have given a copy of an infected `Mr Potato Head' game to a supplier of software routines for Aldus. Aldus accidentally included the virus in 5,000 copies of the drawing program, *Freehand.* Brandow and programmer Drew Davidson were roundly condemned for their actions.

Early 1988: an anti-Zionist virus?

In December 1987, PC users at the Hebrew University in Jerusalem noted occasional program slowdowns and disk space shortages. Investigation revealed a virus, now known as Jerusalem (also known as Hebrew, Friday the 13th and Israeli) that attached itself to the end of .COM and .EXE files. On every day except a Friday the 13th, it allowed infected programs to run normally for the first 30 minutes, then introduced loops which slowed execution to about 10% of normal speed and showed a 2x12 character rectangle at the bottom of the screen. It infected all available programs. Luckily for the investigators, it superinfected .EXE programs by adding its bytes even if the file had already been infected. It did not affect COMMAND.COM. Users identified the infection by noticing that their .EXE programs were growing unwieldy.

The interesting feature of the Jerusalem virus is that it had a different effect on a Friday which fell on the 13th of a month. On such Friday the 13th, the virus was programmed to destroy all programs as soon as they were launched. The first day that qualified in 1988 was May 13. On May 14, 1948, the State of Israel was proclaimed in Tel Aviv. This coincidence of dates has suggested to many observers that the Jerusalem virus was politically motivated and may qualify as an early example of information warfare. However, because nothing is definitely known about the origins of the virus, this contention remains speculative.

Virus as revenge

In January of 1988, Dave Lavery of NASA noted widespread problems on Macintosh computers used in his organization. He was able to help Apple scientists determine that a virus was infecting programs and interfering with their functions. A timer was set to crash infected programs after 20 minutes of operation. Investigators found that this *Scores* virus was deliberately programmed to damage two specific programs written at Electronic Data Systems (EDS), the company founded by Ross Perot. Scores attacks all files containing the identifiers ERIC and VULT. The author may have been an angry ex-employee who had been fired by EDS in 1987. It is thought that the virus accidently escaped into the general Mac world. Scores is still at large, although it can easily be detected and disinfected now. Some analysts suggest that this virus was an early example of automated sabotage--a harbinger of future industrial information warfare.

How do viruses work?

Viruses `live' in executable code. Such code is found in files (programs, overlays) and special sections of disks (boot sectors). `Data' files which can serve as macros for other programs such as spread sheets, editors, disk editors, debuggers, and fourth generation languages can be modified to act like viruses; however, such implementations of self-replication have not been a problem so far.

File infectors

When you run a program, a section of the OS called the loader puts the program code into memory so it can be executed. File infector viruses modify programs so viral code gets included in memory.

A few unsuccessful viruses (e.g., Whale) are overwriting viruses. They actually delete essential program components as the virus overwrites the host. Infected programs therefore fail obviously.

Normal file infectors attach their code to the program file and replace a specific machine instruction with a BRANCH or JUMP instruction at a given point in the infected program. This replacement forces execution to switch to the viral code, where unauthorized functions can be activated. The viral code then executes the program instruction which was obliterated by the viral JUMP instruction and then jumps back to the next instruction in the original program.

Boot-sector viruses

Boot-sector viruses reside in the special regions of disks and diskettes called bootstrap sectors. We speak of `booting' a system when we start it because of the way operating systems load themselves. Most computers keep the operating system (OS) code in software so it can be improved easily (putting it in ROM makes it more expensive to upgrade the OS). But how does a computer start reading the files containing the OS if the OS isn't loaded yet? This chicken-and-egg problem was solved in the early years of computer design by building very simple instructions in the hardware to enable it to read a single external record on a specific device. This

record then instructs the processor in how to read more records to load the OS into memory. Because this process reminded the early engineers of the American expression, `Lifting yourself off the ground by pulling on your bootstraps,' they called the first external record the bootstrap code.

In the DOS world, every disk and diskette contains a reserved area called the bootstrap sector. On disks formatted to include the OS, the bootstrap sector contains usable code. When a DOS system is powered up or reset, the hardware always reads any disk defined as the boot disk; this is usually diskette reader A. If there is a diskette in the boot drive and if the bootstrap sector contains executable code, that code is automatically loaded into memory and executed. DOS has no provision for verifying that the bootstrap code is authorized or valid. Any code found in the bootstrap area is executed during system initialization.

Whenever an infected diskette is present in the boot-diskette drive (or when an infected hard disk is online) during the boot process, the boot-sector virus gets loaded into memory. From that point on, the viral code can interfere with normal system functions.

Primitive viruses like Lehigh changed the modification date on infected files and thus quickly revealed themselves and were stopped from spreading. Virus authors therefore began to develop methods for hiding their creations from view. These methods are collectively called `stealth' techniques and are discussed in the section on AVP technology.

How bad is the problem?

The virus threat can be measured by the

- number of infections (and their consequences)
- cost of protecting against and recovering from infections.
- number of distinct virus types (often called species)

Number of infections

The first wild (non-laboratory) DOS viruses appeared in the US in late 1987. Since then, the estimated number of attacks has doubled every four to five months. The work of Dr Peter S. Tippett showed a doubling time of about 4.3 months; a study commissioned by the NCSA and carried out by Dataquest provided support for this exponential growth model. The NCSA study included only large commercial organizations with at least 300 PCs.

Unfortunately, the main findings concerned `encounters' of viruses. An encounter was defined as having at least one infection. The large average number of PCs meant that it was easy for low individual PC infection rates to result in high overall encounter rates. If you have n computers

and a probability p of infecting any single computer, what is the probability P{>0} that you will have at least one infection?

The reasoning goes as follows:

a) Let the probability that a single PC will be infected be p.

b) Then the probability that a single PC will not be infected is (1-p).

c) The probability P{0} that no PC will be infected if you have n independent opportunities to infect a PC is (1-p)^n.

d) Therefore the probability P{>0} that at least one PC will be infected is 1-[(1-p)^n].

Even for a small p, a large n makes it very likely that an organization will have a virus encounter. For example, the following table shows the likelihood of infection of at least one PC if the probability that a single PC will be infected is p = 0.001:

n	[1-(1-p)^n]
2	0.002
4	0.004
8	0.008
16	0.016
32	0.032
64	0.062
128	0.120
256	0.226
512	0.401
1024	0.641
2048	0.871
4096	0.983

An analysis by Kephart and White of IBM reported by Jim Daly of *Computerworld* and by Mark Gibbs suggested per-PC infection rates of about .001 or 0.1% per year. Furthermore, the rate was growing.

The USA Research study of 1992 included smaller organizations. The data suggested much higher rates of infection, reaching about 3% per PC per year and 10% per Macintosh per year in 1991. The USA Research study suggested that the number of infected PCs might decline in the next few years thanks to the increasing use of AVPs. It is interesting that the projected rates of PC incidents quoted by Gibbs for 1992 and 1993 approach the 3% value.

Some security officers attending the January 1993 *Information Systems Security* course sponsored by the NCSA reported on an informal survey of virus prevalence they had carried out. Their employer sent out diskettes (known to have been uninfected when they were sent) all over the world so suppliers could submit their bids on diskette. Of the 180 diskettes received from the U.S., 5 (3%) were infected; 3 of 140 from Europe were infected (2%); and 15 of 350 returned from Asia were infected (4%).

Costs of virus attacks

Estimates of the damage caused by viruses vary, but the median figure from the NCSA study was about $6,000 per `disaster' (defined as infection of at least 25 PCs or diskettes). This figure included the cost of time wasted and lost productivity before and during recovery. One respondent reported costs of $2 million in a single disaster. Gibbs recalculated these data to give an estimated cost of about $100 per infected PC.

The USA Research study reported costs in the $800 range per PC infected, including an average of about 4 hours to recover data on affected systems and a total of 6 hours on average for complete recovery.

Gibbs supplied an example from an unnamed insurance company which apparently had all 100 of the PCs on a LAN struck by a Dark Avenger Mutation Engine (DAME) virus. It took three days to disinfect the PCs; the company estimated costs of at least a quarter million dollars.

Gibbs provided a detailed model and work sheets for calculating the estimated cost of virus attacks. He includes such factors as confidence in security perimeters, expected infection rates, and degree of networking among computers. He also showed readers how to analyze the costs of anti-virus defences. His methods are well thought out and usable.

Types of viruses

The other dimension of the problem is the number of different viruses. But answering the simple question, `How many viruses are there?' is not so simple. Before you can count things you have to be able to name distinct sorts. Because of the difficulties in defining and distinguishing among similar strains of viruses, the consensus among AVPDs is only approximate. There are said to be between 2000 and 3000 distinct viruses in the world today (March 1993).

Viruses are created by human beings. Some write completely new viruses but most virus authors merely copy existing viruses, change a few bytes, and release the new version into cyberspace. As a result, researchers have been able to discern family relationships among viruses. For example, Gibbs showed a family tree of the Jerusalem viruses that includes 30 different viruses, ranging from SURIV 3.00 (thought to the be ancestor of Jerusalem) through a total of 3 further generations to such variants as Taiwan 3, Fu Manchu-B and Sunday viruses.

At the 1991 Anti-virus Product Developers'(AVPD) Conference sponsored by the NCSA, several speakers addressed the issue of virus identification, classification, and genealogy. The Conference Notebook included an interesting summary of naming problems by Dr David Stang.

Lawrence Bassham and Timothy Polk of the National Institute of Standards and Technology (NIST; Washington, DC) addressed the audience on "Virus naming & standardization of virus counting." The current disorder among virus names causes confusion and makes it harder for users and experts to discuss their problems and solutions. Virus names should be unique, memorable (numbers aren't), should (if possible) describe relationships to other viruses, and should describe some element of virus behaviour. NIST proposes guidelines reflecting these principles. In addition, NIST suggests avoiding the names of people or organizations and urges experts to avoid profanity and other offensive terms.

Existing viruses are named by looking for the mostly widely used terms that conform to the guidelines. For example, NIST would name the `Sunday' virus by noting that it is part of the Jerusalem virus family, so the NIST name would be JERUSALEM-SUNDAY. Variants would be JERUSALEM-SUNDAY;2 and so on. In contrast, the Virus Test Centre at the University of Hamburg uses a 5-level classification (they feel that 3 levels is too limiting). They have begun working on taxonomic nomenclature to identify common features of viruses.

At the Conference, I commented that all the organisms on this planet have been named uniquely using two names: but that's possible only because there has been solid work in describing clusters of characteristics. Taxonomy works when one can `chunk'; i.e., when one groups characteristics functionally.

The battle between lumpers and splitters, so familiar in the world of biological taxonomy, also emerges in the virus world. Lumpers like to keep different organisms in the same group (`taxon') whereas splitters like to put them into separate taxa. How will one decide that two rogue programs are variants of the same virus or sufficiently different to warrant being called different viruses?

Phylogeny

In biology and in astrophysics, naming things implies a model of evolutionary relationships. Taxonomy implies phylogeny.

At the 1991 NCSA Conference, Fridrick Skulason (FRISK Software; Reykjavik, Iceland) presented a review of the relationships among viruses. He pointed out that it's easier to modify an existing virus than to create a new one. He summarized the range of modifications actually seen in viruses:

- invisible changes that don't alter function;
- small functional changes such as different activation conditions for logic bombs;

- changes due to using different assemblers;
- differences due to different compilers in the same high-level language.

In addition, Skulason pointed out that we may encounter viruses that result from translating existing designs into different high-level languages.

At what point does a virus cease qualify as different from another? It depends on the researcher's opinions. It is this ambiguity that accounts for the wide variation in professional estimates of the number of viruses found in cyberspace.

Skulason also presented the results of some of his research into measuring the evolutionary relationships among viruses. He proposed a simple method for calculating a coefficient of relatedness:

- isolate the viral code;
- decrypt encrypted sections (these 2 steps are necessary for any method);
- generate all fixed-length substrings from both viruses (he has been successful using 8-byte substrings);
- calculate what percentage of substrings from A are found in B and what percentage from B are found in A;
- average these percentages.

He found that viruses known to be unrelated produced less than 50% substrings in common, whereas viruses known to be related produced around 95% in common. In all his tests, related viruses produced at least four times greater overlap than unrelated viruses.

During the discussion, I proposed that discriminant function analysis might be useful, possibly using statistical measures of goodness of fit. A small group of interested AVPDs met over lunch and agreed that it would be valuable if AVPDs pursued such avenues together. They discussed a study using Monte Carlo methods to allow discriminant functions to `evolve' as a function of the pool of viruses used for input. It would be interesting to know if such functions would be chaotic systems (wildly varying results as a function of minor differences in input), in which case the discriminant functions would be useless.

Most common viruses

The NCSA study in 1991 showed that two species alone accounted for most of the DOS virus infections in large firms (counting by number of PCs infected). Among the firms examined, Jerusalem (and variants) and Stoned accounted for about 85% of the virus incidents.

Statistics

According to Dr Alan Solomon, creator of Dr Solomon's Anti-Virus Kit, the most common viruses in the wild (i.e., not in the anti-virus laboratories) in 1992 were

- Jerusalem.Standard
- Stoned.Standard
- Anticad 4.Danube
- Vacina-05
- Yankee-Doodle-44
- Cascade 1701 & -1704
- Michelangelo
- Green Caterpillar.1
- Tequila
- Frodo
- Dark Avenger-4 and -1
- Form
- Vienna.

These data are highly variable in space and time. Virus frequencies are different in various parts of the world and change monthly. For example, work reported at a conference in the UK in 1992 showed the following variations over time in virus infections in the UK:

- Stoned represented 30% of the infections in early 1991 and declined to 20% within a year.
- Form appeared in late 1991 with about 16% and had risen to 22% within a few months.
- Tequila rose from negligible to 10% in the early months of 1992.
- Joshi rose marginally from 4% at the start of 1991 and reached 5% by the end of that year.

The WILD List

Joe Wells at Symantec has been producing *The Wild List* for some years now. It is available online in the NCSA Forum. The list shows viruses which have been reliably reported "in the wild" by virus researchers around the world. The list does not include frequency information, so it is not a list of "common" viruses; however, it does demonstrate how few viruses are circulating widely enough to be spotted in ordinary users' computer systems.

Characteristics of common DOS viruses

Here are short descriptions of some viruses common in the DOS world. The list is in alphabetical order. For convenience, even the viruses mentioned above in the historical discussion are included.

Anticad-4 (aka Invader, Plastique Boot) was detected in China in September 1990. It infects .COM files, .EXE files and boot sectors. Once the virus has been loaded into memory by running any infected file, all files which are opened will be infected (except COMMAND.COM). The virus cannot conceal the increase in length it causes during infection. Thirty minutes after the virus is activated, it may play a melody by Mozart until the system is rebooted. Rebooting the system using the Control-Alt-Delete keys while the melody is playing causes the virus to overwrite the first track of any hard disk available. Anticad-4 has spread rapidly throughout the world.

Cascade (Autumn Leaves, Blackjack, 1704, Herbst): detected in September 1988 at the University of Konstanz in Germany. This file-infector extends the size of its host programs by 1704 bytes. Once loaded into memory, the virus infects every .COM file the user executes. The trigger is the date: in November and December, the virus makes letters on screen fall straight down, leaving blanks in their place. If the virus increases the .COM program file length beyond 63576 bytes, the infected program cannot run.

Columbus Day was discovered in March 1989. It is a time bomb set to detonate on Friday the 13th of October. There was widespread publicity about it in the professional press but not in the public press. Perhaps as a result of the advance warnings, only a few dozen cases were every reported. Most people who found it on their systems were able to eliminate it.

Dark Avenger-3 (V2000, Eddie 3): this nasty file infector scurrilously claims to have been written by a respected anti-virus researcher, Vesselin Bontchev (it was not). It also includes a string reading, "Copy me - I want to travel." On every 16th execution of an infected .COM or .EXE file, the virus randomly overwrites a data sector on disk. It also traps all calls to the DIR command and subtracts its own 2000 byte length from the actual length of infected files. This subtraction qualifies it as a stealth virus (see below).

Form, a boot-sector sector virus, was discovered in Zurich, Switzerland in February 1990. It puts "The FORM-Virus sends greetings to everyone who's read this text" in the boot sector. On every

read from a floppy disk, the virus tries to infect that floppy. It makes keys click and slows down response.

Frodo, also known as the 4096, IDF, Stealth and 100 years virus, is a file infector discovered in Haifa, Israel in October 1989. It infects programs when they are loaded and changes their date of modification to a century after their original last modification. Once the virus is memory resident, all attempts to read the viral code in infected files are turned aside. The system usually hangs when an infected program is run any time after the 22nd of September and the and of the year.

Green Caterpillar (aka 1575/1591 or 15xx, was detected in Ontario, Canada in January 1991. This file infector attacks any files it can reach whenever the COPY or DIR commands are executed. Two months after the first infection, running an infected file makes a green caterpillar creep over the screen, starting in the upper left corner.

Jerusalem (aka Israeli, Hebrew, Friday the 13th): file-infector. Adds 1813 bytes to .COM and 1808-1823 bytes to .EXE files. It can superinfect .EXE files. Slows program execution after 30 minutes any day and shows rectangle at bottom left of screen. On a Friday the 13th, it erases any program that is executed.

Joshi (aka Happy Birthday Joshi) is a boot-sector virus that takes up 6 Kb of RAM when active. It was first reported on 28 Feb 1990 and has been increasing in frequency since then. On color monitors, it is triggered on the 6th of January, when it displays “Type ‘Happy Birthday Joshi’” and locks the system until the user types the string as shown. This virus relocates boot-sector code to tracks 41 or 81 on diskettes or to track 0, sector 9 on hard disk and can cause problems when you try to format a diskette (displays a message indicating a bad track 0).

Michelangelo is a boot-sector virus. On March 6 of any year, it overwrites the File Allocation Sector (FAT) and the Master Boot Record (MBR) on hard disks. It also infects all floppies it can access during any I/O to that floppy. The virus is thought to have appeared in April 1991 in Sweden and the Netherlands. It spread more rapidly through the PC cyberspace than any other virus known at that time. It was shipped accidentally in 500 computers from Leading Edge Products and was found in 900 diskettes of demonstration programs from Da Vinci Systems.

For unknown reasons, Michelangelo captured the imagination of the popular press. Hundreds of articles appeared in newspapers; there were programs and warnings on TV. John McAfee, founder of McAfee Associates and provider of well-known AVPs was interviewed in Australia. He was asked how many computers could be infected. He answered with a shrug, “I don't know. Could be 500, could be 5 million.” The newspaper report quoted only the upper figure, and it was spread widely by repetition through the press. The NCSA's 800-number was flashed on TV screens after a short segment; within minutes, the phones were swamped. In the week leading up to March 6, there were over two thousand calls to the NCSA asking for help. AVPDs reported the same phenomenon.

McAfee and other AVPDs developed special versions of their AVPs which could diagnose and eradicate Michelangelo. Whether because of the publicity plus the AVPs or possibly because the danger had been overstated, estimates of the numbers of affected PCs were in the 10,000 range worldwide. One year later, in 1993, Michelangelo had faded into obscurity, with only a few sporadic cases of damage reported among anti-virus professionals.

Ping-Pong (aka Bouncing Ball, Italian, Turin) was discovered at the University of Turin, Italy in March 1988. This boot-sector virus infects every disk that is read or written to once the virus is active. The virus is triggered after any I/O that occurs when the system clock is on the half-hour or the hour (e.g., 01:00, 01:30, etc.). Since the virus has no mechanism for determining the characteristics of the disks it infects, it can damage data on any disk or diskette that deviates from the format parameters it expects.

Stoned (aka New Zealand, Marijuana): boot-sector virus which infects floppy disks on I/O functions (e.g., during DIR A:\ or TYPE commands) and infects hard disks when you boot the PC with an infected diskette in the boot drive (A:\). If the system clock value ends with 3 0 bits, the PC beeps and displays, “Your PC is now Stoned!.....LEGALISE MARIJUANA!” Because the virus overwrites sections of disks, it may damage your data or make the disk unusable.

Tequila was detected in April 1991 in Steinhausen, Switzerland, possibly by authors 18 and 21 years old (these people were interrogated by Swiss Police). This stealth virus uses a self-encryption algorithm. It infects .EXE files and the MBR. The additional 2468 bytes of viral code are invisible on the DIR or other DOS commmands. It does not infect files that include the strings “SC” and “V” in their names to avoid AVPs. Within the infected file, the virus encrypts its code using its own encryption algorithm as the key; the ciphertext is decrypted only during execution. Tequila also inserts random, nonfunctional “junk” code that confuses many signature-based AVPs. The infected MBR is not encrypted, but the virus conceals itself by diverting all I/O to the displaced MBR code. Once the copy in memory has been triggered at a random time after activation, the virus displays a fractal design when any program terminates. It also attempts to delete all files which have been marked with a validation string (checksum) by McAfee's SCAN program.

Vacsina refers to a string found in a series of innocuous viruses written by a Bulgarian experimenter. These file infectors seem to be designed to be harmless; they deliberately let themselves be identified by most AVPs. VACSINA was the basis for the later Yankee Doodle viruses.

Vienna (aka 648)is a file infector that never becomes memory resident (it works only while an infected .COM program is loaded). As part of its infection process, it sets the seconds bits of the infected program's time stamp to 62 as a marker for itself. Usually the virus infects the first uninfected .COM file it finds. However, there is a 1 in 8 probability that instead of adding viral code to the end of the target program, Vienna will overwrite the first five bytes of the .COM file. In these cases, the virus inserts a jump instruction into the BIOS routine for rebooting the system. In other words, the virus converts 1 out of 8 infected programs into a Trojan horse. Running any

of these modified programs resets the system, causig everything currently in memory to be lost. If the system has disk caching enabled, rebooting without a change to post the dirty buffers to disk will cause data corruption on disk.

Yankee-Doodle viruses are file infectors from Bulgaria. Many of them play the named tune at 5 pm.; others have different triggers. They are mostly harmless.

Macintosh viruses

CODE 252 infects applications on the Mac. It replicates every time an infected program is run between 1 January and 6 June. On and after its trigger date, June 6, it changes its mode of action. From that point until the end of the year, infected programs display the infantile but alarming message, “You are infected with a virus. Ha Ha Ha Ha Ha Ha Ha. Now erasing all disks. Ha Ha Ha Ha Ha Ha Ha. (Click to continue).”

At that point, the virus actually disinfects itself: it patches the infected file and eliminates its own code from memory. This is one of the few self-removing viruses known.

INIT 1984: The INIT 1984 virus infects system extensions. It changes the names and attributes of files and folders and can destroy data. Its trigger date is Friday the 13th.

MBDF A: On February 14, 1992, three Macintosh games were posted to several bulletin board systems (BBSs). Obnoxious Tetris and Ten Tile Puzzle were infected with a new virus, MBDF A. Tetricycle was a Trojan virus dropper carrying an encrypted version of the virus.

MBDF A infects Macintosh system files. Although it was not designed to cause damage, it slows down response so that some users become impatient and reboot their systems. If the virus is writing to disk at that time, the reboot can corrupt the system.

A Welsh professor of mathematics noticed that checksummed programs were showing tampering. He reported the problem to a consortium of anti-virus researchers working with Apple to stem the virus problem. Thanks to the rapid notification, they were able to trace the origins of the infected files to Cornell University.

Two students were arrested and held overnight on first-degree computer-tampering, a felony (i.e., a crime punishable by imprisonment) under New York State law. They pleaded guilty to second-degree computer tampering, a midemeanor. A third student pleaded guilty to a charge of disorderly conduct. The students worked part-time in the University's computer labs.

Virus factories

A surprising number of viruses have been traced to the “Bulgarian Virus Factory” in Sofia. The programmers working there include the notorious Dark Avenger.

In April 1988, a Bulgarian magazine published a translation of a German article about computer viruses. Six months later, the Vienna virus appeared in Sofia, followed by Cascade and Ping Pong. Bulgarian programmers disassembled these viruses and optimized the code; soon they began writing their own. Yankee Doodle was written in response to an ill-advised challenge issued by computer scientist Vesselin Bontchev, who claimed that viruses could not infect .EXE files. One of his friends promptly wrote Old Yankee, which does precisely that.

Another virus writer, T.P., went through several cycles of writing viruses, AVPs to defeat his own viruses, and new viruses to defeat his AVPs. He generated over 50 different varieties, including the VACSINA strains and the original Yankee Doodle. His viruses were widely distributed because he shared his PC with other users who inadvertently spread the infection. T.P. gave up writing viruses when he got bored.

Another virus writer appeared in the Spring of 1989. He signed his viruses, “Dark Avenger” and made them highly infectious and viciously damaging. These “fast infector” viruses infect every file as soon as it is opened (e.g., by antivirus scanners). Worse still, on every 16th run of an infected program, the viral code wrote, “Eddie lives...somewhere in time!” in random sectors on the hard disk. Because the damage might not show up for a while, the victim's backups often became contaminated.

Dark Avenger has written DARK AVENGER, V2000 and variants, V2100 and variants, 651, DIAMOND and variants, NOMENKLATURA, 512 and variants, 800, 1226, PROUD, EVIL, PHOENIX, ANTHRAX, and LEECH viruses. He has deliberately uploaded his viruses to European BBSs and has even uploaded Trojans written to “drop” these viruses on innocent victims. For example, logging on as anti-virus researcher Bontchev, he uploaded the program UScan, which he claimed to be an AVP. Instead, it infects every program available with ANTHRAX. Bontchev writes,

> While the other Bulgarian virus writers seem to be just irresponsible or with childish mentality, the Dark Avenger can be classified as a “technopath.” He is a regular user of several Bulgarian BBSs, so one can easily exchange e-mail messages with him. When asked why his viruses are destructive, he replied that “destroying data is a pleasure” and that he "just loves to destroy other people's work.”

Several other programmers in Bulgaria have been responsible for a zoological garden of viruses: 1963, ANTI-PASCAL605, BOOTHORSE, BOYS, DARK LORD, DARTH VADER, DESTRUCTOR, DIR, DIR II, DREAM, ETC, GERGANA, HACKER, HAPPY NEW YEAR, INT 13, JUSTICE, KAMIKAZE, MG, MICRO-128, MINIMAL-45, MURPHY, MUTANT, NAUGHTY, NINA, PARITY, RAT, SENTINEL, SHAKE, TERROR, THE NUMBER OF THE BEAST, TINY, TONY, V123, V127, V270x, VFSI, WARRIER, WARRIOR, WWT, and XBOOT.

Dr Bontchev wrote in 1991 that he was concerned about the lack of anti-virus laws in Bulgaria. He predicted that the wide availability of virus source code on virus-oriented BBSs would lead to an explosion of virus writing which would spread throughout the world.

He was right.

Virus by number

The Virus Creation Laboratory, the Dark Avenger Mutation Engine, and the Mass-Produced Code Generator allow novice virus authors to generate new viruses in minutes.

Automation comes to vandalism.

Virus Creation Laboratory

VCL 1.00 appeared in late 1991. This virus generator comes with an attractive graphical user interface (GUI) complete with mouse support, pull-down menus, and context-sensitive help. Users can select features such as encryption, virulence (e.g., how many files to infect at once), special effects (e.g., clearing the screen, rebooting the system, corrupting files) and details of the trigger events. The VCL generates only .COM-file infectors and permits authors to include internal comments in the generated code. The author even has the cheek to include an impressive copyright notice claiming that any attempt to interfere with the VCL will result in legal proceedings. I don't know if this programmer has a sense of humour or if (s)he is a lunatic.

Whatever the author's motivation, (s)he is a careless programmer. There are problems with the installation routine. Unfortunately, it is still possible to create working viruses with this tool. Version 2.0 of the VCL appeared in late 1992.

Dark Avenger Mutation Engine

DAME (sometimes abbreviated MtE) appeared in 1991 and was written in Sofia, Bulgaria. It is a tool for creating polymorphic viruses which encrypt themselves. However, the user has to know how to write Intel 80xxx assembler code to actually create live viruses. The DAME has been used to created several viruses, including Dedicated Pogue, Fear and Groover.

Mass-Produced Code Generator

In August 1992, a group of cybervandals released the Mass-Produced Code Generator (MPC). This tool creates polymorphic stealth viruses; it generates over 150 randomized encryption engines in a single execution. The MPC includes its own source code among the files found on underground BBSs.

The Good Times "Virus" Rumor

In early December 1994, the Computer Incident Advisory Capability (CIAC) of the Department of Energy reported a spate of enquiries about the following scary message:

Here is some important information. Beware of a file called Goodtimes.

Happy Chanukah everyone, and be careful out there. There is a virus on America Online being sent by E-Mail. If you get anything called "Good Times", DON'T read it or download it. It is a virus that will erase your hard drive. Forward this to all your friends. It may help them a lot.

In fact this message was a hoax. There has never been a virus residing in a plain-text message; however, this message has circulated around the world through the earnest efforts of technically unsophisticated victims. CIAC reported that many people had observed that "the warning message and its [denunciation] are seen to behave like viruses (memetic lifeforms) with a human serving as the replicating mechanism (just like chain letters)." The spread of the hoax was made worse by the tendency of some victims to delete replies debunking the story because the e-mail message included the words "Good Times" in the subject line.

Later variants of the Good Times Virus Hoax have included increasingly fanciful descriptions of the damage it would cause. Naturally, someone did actually create a real virus which includes the string "Good Times" but it is just a normal computer virus, not a magic e-mail message. The hoax has been cropping up every three or four months for over a year and shows no sign of every being extinguished. Once in cyberspace, misinformation is immortal.

You can download information about the Good Times hoax from the CIAC Web site (http://ciac.llnl.gov/ciac/CIACHome.html) or from the NCSA Forum on CompuServe (GO NCSAFO).

Anti-virus products

AVPs fill three needs:

- diagnosis (locating virus-infected files and boot sectors after the fact);
- disinfection (getting rid of the damage and restoring the intact files and sectors); and
- inoculation (preventing damage).

Diagnosis and stealth

One of the easy ways that you can tell a system is infected is to notice unauthorized changes in files (e.g., altered dates, increased lengths). Some AVPs generate a checksum that depends on the sequence of bytes in a file. Changing anything in the file changes the checksum. The security

program can thus identify infected programs. Unfortunately, many viruses evade this simple technique.

The first move towards stealth was to avoid changing the modification date of infected files. Next, some viruses appeared that trap the internal procedures (called interrupts) used to get information about files. By capturing these interrupts, the viruses can mask their presence by subtracting their own size from file sizes before passing the information to the DIR command. More advanced stealth techniques were designed to foil scanners.

Many stealth viruses trap the low-level I/O routines that AVPs need to compute the checksums. The viruses remove all signs of their own presence before passing data about infected programs to checksum algorithms. As a result, the checksum matches the original value before infection.

Another approach to detecting infection is to look for the viral code itself. AVPDs have identified unique sequences within thousands of viruses and built libraries of these search strings, called virus “signatures.” Scanner programs look for signatures on disk or in memory; they display an alert upon discovery. Scanners suffer from both types of ascertainment error: false positives, where a signature is actually part of an uninfected file, and false negatives, where a new virus or a variant of an old one lack the expected signatures. There is a tension between attempts to reduce each type of error. One can lower the rate of false positives by becoming more stringent in defining signatures, but then the number of viruses missed increases.

In the early years of AVP development, some AVPDs failed to encrypt their lists of signatures. When two scanners were run on the same system, they often mis-identified each other as viruses. Sometimes reports of infections would go on for pages as each AVP catalogued the other's signature files. Today all AVPDs encrypt search strings.

Polymorphic stealth viruses interfere with scanners by encrypting their signatures. During execution, the unencrypted stub of the virus decrypts the rest of itself as it loads into memory. The Dark Avenger Mutation Engine spawns hundreds of different polymorphic viruses with every execution. More advanced stealth viruses introduce random variations in their code (e.g., switching the sequence of instructions without altering functionality), making it even harder to define a single search string.

As the variety of viruses grows, AVPDs keep up by issuing updates to their signature lists. Users of such scanners must keep their versions current, usually by dialling up a BBS and downloading new signature files.

A complementary approach to detecting virus infection is the generic AVP; e.g., NOVI. These AVPs scan for characteristic patterns that cannot be masked (JUMP codes with unusual addresses, for example, that divert execution to the viral area and then back into the regular code). Generic AVPs also watch for abnormal behaviour, such as peculiar OS interrupts, thus trapping some viruses that use stealth techniques.

Errors

AVPs illustrate the principles of hypothesis testing as taught in elementary statistics classes. An AVP helps a user decide whether a system is infected or not. If an AVP uses lax rules for detecting viruses, it may falsely claim that there's a virus when there isn't. This error is called the false positive. Contrariwise, if an AVP uses stringent rules to detect viruses, it may falsely claim that there is no virus infection when there really is one. This is called a false negative.

There is an inverse relationship between the two types of error; the lower we make the false positives, the greater the risk of generating false negatives (and vice versa).

One of the best ways of reducing error rates is to apply two independent tests. The probability that both tests will make the same type of error is the product of the individual error rates. For example, if a signature-string based scanner has a 1% chance of missing a virus infection and a generic virus scanner has a 2% change of doing the same, the likelihood of missing the virus infection may be as low as 0.01 x 0.02 = 0.0002 or 0.02%.

Disinfection

Once a virus is identified, how do we get rid of it? All effective viruses must by definition leave the original code intact somewhere on disk--otherwise they qualify as mere overwriting viruses, which have virtually no chance of being spread to other victims. Many AVPs find the original code and patch it back into place after removing the viral instructions.

Clearing viruses out of infected files is only part of the problem. If viruses have caused damage to data files, no program can possibly repair all the damage. By far the best approach to restoring full function is to restore the original versions of affected programs and data files from uninfected backups.

Preventing infection

All evidence suggests that the primary vector of infection is the diskette. According to the NCSA survey, nearly 90% of all virus infections are traceable to infected diskettes and infected programs transferred via diskette. Here are some practical guidelines for reducing the risk of infection:

- Check for viruses on every diskette you receive.
- Check every diskette you give away or lend.
- Prevent children from inserting unverified diskettes into your PCs. Buy a diskette drive lock and keep the key to start virus-proofing your home computer.

- Scan your hard disks, including file servers, using both a scanner with up-to-date search strings and a generic scanner. TSR AVPs are useful to catch viruses that escape the disk scan.

- Do not reboot a PC when a diskette is in the bootable drive.

Hardware anti-virus devices such as ThunderBYTE (Brookline, MA), Virus Trap (JAS Technology, Warrenton, VA) and C:CURE (Leprechaun Software, Marietta, GA) write-protect all or part of a hard disk. No known virus can replicate on such protected drives. However, as pointed out by Leprechaun, some programs need to modify themselves and won't work on a protected drive. In addition, deprotecting the drive to install new software may allow infected programs into the system. Furthermore, once present in an infected program, the virus could conceivably become memory resident and cause trouble without modifying other programs.

Macintosh AVPs

Michelle Hasson has published a list of AVPs for Macintosh users:

Anti-Virus, (part of MacTools 2.0 @ $149) / Central Point Software (503-690-8090)

Disinfectant (free)

GateKeeper (free)

SAM ($99; upgrades, $12) / Symantec (408-253-9600)

Virex ($99.95; upgrades, $15; annual subscription, $75) / Microcom (919-490-1277)

VirusBlockade (shareware, $70)

VirusDetective (shareware, $40).

These and other shareware and freeware products can be downloaded from reputable public networks such as CompuServe and GEnie, which check uploads carefully for virus infections before releasing them for downloading. In addition, you may be able to find trustworthy local BBSs which make the same safe files available. Look for BBSs where only real names are allowed and where there is evidence of a serious attitude to preventing damage to members' computers. Beware BBSs where there are closed sections reserved for special categories of members, files of stolen software and “handles” which run to the morbid, obscene or just plain disgusting. Such signs indicate that you've stumbled into a pirate BBS; your chances of picking up viruses from such BBSs are higher than average.

Why do people write viruses?

The consensus among anti-virus researchers is that most virus authors are misguided rather than evil. Except for the lunatic few, most of these people seem to be irresponsible rather than deliberately vicious. Some of the younger folk seem to be primarily curious; they often naively believe that it is easy to contain viruses one is creating "for fun" and are crestfallen when their creations escape. Some have even cooperated with anti-virus teams by giving them source code for their escaped viruses. Many others are immature people who seek heightened reputation within a peer group, much as juvenile delinquents have often committed crimes and misdemeanours for acceptance into gangs.

Another factor which stimulates virus writing is the virus-distribution BBSs. Many of these claim to support research, yet they carry out no background checks at all on their members and even encourage the use of pseudonyms. In order to download viruses from these boards, prospects have to upload a new virus. Since finding a new virus is difficult, most of the juveniles who subscribe to these BBSs simply patch an existing virus. They modify text strings (e.g., "Ha Ha Ha" becomes "Ho Ho Ho") or alter trigger conditions. Many of these people have no concept of the internals of the OSs they attack; their hobby has all the intellectual glamour of teaching a parrot to talk.

A respected anti-virus researcher has spoken with many virus-distribution BBS sponsors. He has found that all of them were simply misinformed; none were very bright. Few responded to his explanations of the damage viruses caused to others; they seemed impervious to a sense of responsibility for their actions in spreading damaging viruses. However, when he explained the legal consequences to *them*, they became alarmed and shut down their BBSs within weeks.

A few virus authors seem genuinely disturbed. Dark Avenger, for example, is authentically evil (Bontchev calls him a technopath). His viruses are designed to damage users in the worst possible way--by insensible, gradual destruction of data integrity. Robert T. Morris, creator of the Internet Worm, appears to be a neurotic young man with a desire to prove something, perhaps to his famous father, R. H. Morris, a well-respected information security specialist.

Viruses on non-DOS operating systems

Cybercrime today is still not fundamentally winnable using technological solutions only. The DOS and Macintosh OSs are relatively primitive in their security structures. Unlike mainframes, PCs have no hierarchy of security levels to distinguish between user functions and OS functions. OS/2 includes such functions and may be more robust. UNIX variants and proprietary mainframe OSs are much less vulnerable to viruses than DOS.

OS/2

In March of 1993, OS/2 still had no viruses specifically written to attack this OS. For one thing, OS/2 uses a 4-level protection mechanism for guarding memory and preventing system crashes. These mechanisms make it inherently more difficult to write OS/2 viruses.

However, at the 1992 Conference of the NCSA, Kevin Haney of the National Institutes of Health in Bethesda, MD reported on experiments with DOS viruses running under OS/2. Because of the strong DOS-emulation capabilities, he found that DOS viruses can in fact damage OS/2 systems. The Stoned-B virus, for example, not only successfully infected hard disks and diskettes, it also showed the message, “Your PC is now Stoned!” before hanging the system.

Several file-infector viruses (including Devil's Dance, Yankee Doodle, Cascade and Sunday) were able to enter memory when infected DOS programs were run; since they then behaved as if they were running under DOS, their attempts to damage files, file allocation tables and root directory entries failed, causing unpredictable but unpleasant results.

The file infectors studied by Haney also successfully infected both DOS and OS/2 programs. Some of the infected OS/2 programs were damaged by the virus and could not load successfully.

LANs

Only a few viruses have been identified on LAN OSs. However, LAN file servers and other host systems may store files which are themselves infected with DOS or Mac viruses; this phenomenon is known as heterogeneous virus transmission. Peter Radatti warned of this problem in his presentation at the NCSA 1992 Conference. A few AVPs run on LANs and recognize DOS virus infections.

UNIX

UNIX computers are not as vulnerable to viruses as DOS machines. UNIX evolved in an academic environment in which security was considered less important than availability. Much of the OS developed through the efforts of countless students and devoted hackers (the good kind). The openness of its source code led to improvements in all aspects of the OS. In particular, UNIX includes security features common in mainframe OSs. In UNIX and other multi-user OSs, access to memory and disk resources are limited by the security level of each process. The process is the Cartesian product of processor, program, user, and time: the execution of a particular piece of code at a particular time by a specific user on a particular central processing unit. Unless a process has been assigned the highest security priority, it cannot access other processes' reserved memory areas. Programs cannot normally read and write areas of disk except through file system routines. File systems usually include provisions to define an access mask that prevents anyone except authorized users from reading, writing, appending, locking, executing and saving files in specific areas, partitions, accounts, or groups.

Viruses have a hard time navigating through such restrictions--if they are used. If a virus were to enter a UNIX system through the actions of a superuser (someone who logs on as the root user, for example), it would acquire all the capabilities of that user, including the ability to override normal security restrictions.

However, an additional obstacle to virus infections is the sheer variety of UNIX systems. UNIX comes in many flavours or dialects. Despite the marketeers' cries of "Open Systems! Huzzah!", programs intended for multiple UNIX platforms are generally *source-code* compatible, not object-compatible. That is, users have to compile the source code of a program using their own compilers in order to achieve runnable code. DOS runs primarily on Intel processors and their clones. In contrast, UNIX is designed to run on multiple platforms. Since the object code must use the machine instruction set for each computer, it is inherently unlikely that a single compiled virus will successfully infect multiple platforms.

However, this advantage may fade if a single platform comes to dominate the UNIX marketplace. When enough object-code compatible computers exist to allow the spread of infected programs, UNIX may see a rise in the number of viruses.

Another factor reducing the prevalence of UNIX viruses is cost. UNIX requires an order of magnitude more disk space and memory than DOS even to boot up on comparable platforms. Until the costs of PCs running DOS and PCs or workstations running UNIX lead to the spread of UNIX in the PC-owning population, UNIX computers will continue to be less subject to attack than DOS systems.

As a result of these factors, UNIX viruses are still [1993] not much of a problem. For those who are concerned, however, Woodside Technologies (Sunnyvale, CA; 408-733-9503) introduced Fortress in 1992. Fortress is a UNIX security product which includes antivirus checking as well as provisions against Trojan horses, worms, and weak passwords. The product uses a GUI and runs under several UNIX OSs.

Proprietary mainframe and midrange operating systems

Mainframe and midrange computers from IBM, HP, DEC, Prime, Data General, Tandem, Stratus and other manufacturers are virtually impervious to viruses created by the young virus writers who plague the PC world. Such systems are relatively rare, making them an unappealing target for people whose chief desire seems to be seeing their virus progeny spread far and wide. They are still far too expensive for most criminal hackers to afford (although used midrange computer costs are reaching the low thousands of dollars). Their OSs have extensive security mechanisms in place and production systems often use add-on software for additional protection. Large-system managers are justifiably careful about the software they move onto their systems and usually demand the source code for any contributed utility software they receive. Many system managers require that all routines be compiled from source; no run-only modules are allowed on their systems. No production system would normally allow untested software to be placed in the production accounts. And finally, most proprietary OSs do not include current source code. Virus creators need not be stymied by such facts, but the difficulties do make virus infections a minor issue for mainframes for the foreseeable future.

The Internet Worm of 1988

The Internet is a global network of networks spanning academic institutions, government agencies and commercial organizations. The Internet includes an unknown number of hosts and users; estimates range from 40,000 to 500,000 hosts and millions of users. All the networks that are interconnected to form the Internet allow free and unfettered transmission of electronic mail. The Internet is loosely coordinated through the Network Information Center (NIC) at Stanford Research Institute (SRI) in Menlo Park, CA and through the Network Operations Center (NOC) at Bolt Beranek and Newman (BBN) in Cambridge, MA.

The Internet has become an indispensable component of the world's scientific and technical communities' communications. Many of us would much rather send each other an email message over the Internet than send an (ugh) snail mail letter.

The following account is drawn from the detailed and highly readable report by Eugene Spafford at the 1989 European Software Engineering Conference.

At 17:00 EST on the 2nd of November 1988, Robert T. Morris, a student at Cornell University in Ithaca, New York released a worm into the Internet. By midnight, it had attacked VAX computers running 4 BSD UNIX and SUN Microsystems Sun 3 computers throughout the United States. One of the most interesting aspects of the Worm's progress through the Internet was the almost complete independence of its path from normal geographical constraints. It sometimes leaped from coast to coast faster than it reached physically neighbouring computer systems. The worm graphically demonstrated that cyberspace has its own geography.

The worm often superinfected its hosts, leading to slowdowns in overall processing speed. The first Internet warning ("We are under attack") was posted at 02:38 on the 3rd of November to the TCP-IP list by a scientist at University of California at Berkeley. At 03:34, Andy Sudduth, a friend of Morris' at Harvard, posted a warning message ("There may be a virus loose on the internet") anonymously and included a few comments on how to stop the Worm. Unfortunately, Spafford writes, the Internet was so severely impeded by the Worm that this message was not widely distributed for over 24 hours.

By 06:00 on the morning of the 3rd of November, messages were creeping through the Internet with details of how the Worm worked. The news spread via news groups such as the TCP-IP list, Usenix 4bsd-ucb-fixes, and the Usenet news.announce.important group. Spafford and his friends and colleagues on the Internet collaborated feverishly on providing patches against the Worm.

Meanwhile, as word spread of the attack, some systems administrators began cutting their networks out of the Internet. The Defense Communications Agency isolated its Milnet and Arpanet networks from each other around 11:30 on November 3rd. At noon, machines in the science and technology center at the Stanford Research Institute were shut down.

By late on November 4th, a comprehensive set of patches was posted on the Internet to defend systems against the Worm. That evening, a New York Times reporter told Spafford that the author of the Worm had been found.

By November 8th, the Internet seemed to be back to normal. A group of concerned computer scientists met at the National Computer Security Center to study the incident and think about preventing recurrences of such attacks. Spafford put the incident into perspective with the comment that the affected systems were no more than 5% of the hosts on the Internet. It would be foolish to dismiss Morris' electronic vandalism as a prank or to claim that the Worm alerted managers to weak security on their systems. Nonetheless, it is true that the incident contributed to the establishment of the Computer Emergency Response Team at the Software Engineering Institute of Carnegie-Mellon University. For these blessings, however, we owe no gratitude to Robert T. Morris.

In 1990, Morris was found guilty under the Computer Fraud and Abuse Act of 1986. The maximum penalties included five years in prison, a $250,000 fine and restitution costs. Morris was ordered to perform 400 hours of community service, sentenced to three years probation, and required to pay $10,000 in fines. He was expelled from Cornell University. His lawyers appealed the conviction to the Supreme Court of the United States. Their arguments included lack of evil intent (he didn't mean to cause harm, honest--even though his Worm took extraordinary precautions to conceal itself) and the scandalous behaviour of Cornell University authorities, who had the temerity to search their own electronic mail message system to locate evidence which incriminated Morris. The lawyers also argued that sending a mail message might become a crime if Morris' conviction were upheld. The Supreme court upheld the decision by declining to hear the appeal.

Helpful viruses?

A few people, including Fred Cohen, argue that viruses are not inherently evil. In theory, self-replicating, self-disseminating programs called “knowbots” might be helpful. For example, knowbots could seek information throughout a network or update specific programs on PCs linked to a LAN. Fred Cohen has continued his research with viruses and is a leading proponent of this possibility.

In mainframe systems, batch jobs often include an instruction which schedules a copy of the job for a later time once the original job has completed its work. In a sense, one could call these cyclically repeating jobs “worms.”

However, until there are knowbots programmed to ask permission to enter and trained to disappear when we tell them to, viruses will remain unwanted intruders into our private cyberspace. They damage our systems, they waste our time, they cause fear, and they move us to spend money on AVPs. To be useful, viruses would have to be written to check the OS and configuration of each system they infect to verify compatibility. It's bad enough having to suffer the bugs foisted on us by poor quality assurance in ordinary software; self-replicating code that has reached our computers without any possibility of production control is bound to cause a mess.

Policy issues

Although public policy issues may not affect the day-to-day security of your computer systems, they influence the long-term prospects for reducing the virus threat.

Should writing viruses be illegal? If not, should virus authors be sued for damages? Are books which give detailed information on how to build a working viruses--including functional code--protected by the First Amendment to the Constitution of the U.S.? The First Amendment guarantees freedom of speech. Are computer programs speech under law? Are the authors of viruses legally responsible for viral effects on computers belonging to people they've never met? Legislators at the federal and state levels have been grappling with such issues for several years. Because of ambiguities in the law, prosecutors unfamiliar with information technology find it difficult to prepare an effective case against cybercriminals. Even the victims of cybercrime have trouble measuring the extent of damage. How much did *your* last virus infection cost you?

Writing viruses

The industry is divided over whether to pursue attempts to pass anti-virus legislation. The NCSA has sponsored several meetings of members of its AVPD Consortium over the years but the group seems no closer to agreement on this issue. Some people argue that writing a virus should itself be illegal. Such laws would make it clear to everyone that writing viruses is *bad*. Having legally prescribed punishments for virus writing would discourage some casual hobbyists from contributing their pathetic efforts to the pool of viruses.

However, others object that such laws would make anti-virus work more difficult. They warn that regulating virus writing might justify a new bureaucracy dedicated to virus control. The law might be unenforceable and therefore ill-advised. Even more fundamentally, the harm from a virus, they argue, comes not from its existence but from its dissemination to unsuspecting victims. Writing the virus does nothing as long as other people don't infect their computers. Even sending the virus to a willing recipient doesn't seem to be a problem: after all, people are free to run whatever programs they want on their own computers. Making virus *writing* illegal would be a form of prior restraint instead of focussing on clearly harmful acts.

Even defining a virus in legal terms would be difficult, especially given the low level of technical knowledge among the legislatures of the world. Some humorists argue that a sloppy definition might classify MS-DOS as a virus... and with good reason, they add.

Furthermore, say the sceptics, viruses are written all over the world and the damages often occur in other countries. How will anti-virus laws be enforced intentionally?

I would like to see clear laws in place worldwide making it a serious crime to write computer programs which, without permission, insert their own code into programs or other executable code. To include worms, we might have to include programs which propagate without authorization. This simple idea would focus on the fundamental attribute of viruses and worms:

their sneaky invasion of *our* computers. Ideally, the U.N. would frame a convention urging nations to allow extradition of people alleged to have written viruses that have harmed the citizens of another nation.

Publishing functional viral code

A January 1993 discussion in the NCSA section on the CompuServe network considered the issue of forbidding publication of functional viral code. Participants drew parallels between writing down viral code and writing down instructions on creating harmful devices such as bombs. The slippery-slope argument was invoked by one prominent member of the anti-virus community, who said: “My concern is that if we can justify the suppression of information as ‘undesirable’ or ‘potentially dangerous’ is it that much further a jump to ... suppression of other ‘information?’”

In my opinion, First Amendment rights do not apply to viral code. I wrote a short opinion piece on this topic for *Network World* in 1993 that stimulated a lot of commentary on the Internet. In the passages below, I have incorporated additional material drawn from my discussions on the Internet into the original text of the article.

Some people have suggested that publishing functional viral code is useful and necessary because everyone should understand how viruses work to be able to combat them. I disagree. No one has explained why it is useful for users and programmers to have access to detailed, working code. Generalized descriptions are fine; even fragments of code may be justifiable. But I draw the line at publishing functional code that can be typed into an assembler or a debug facility and create a working virus.

People who build AVPs need the code but can get it through private, controlled channels. People who build computer system hardware and want to devise better anti-virus traps can also use real viruses obtained through controlled channels. So can OS gurus. Computer scientists and AVPDs wishing to publish research on specific features of viruses can share their knowledge constructively by printing portions of the code in question without making the entire functional virus available to all and sundry. As long as what is disseminated does not work if entered directly as printed or transmitted, I see no problem.

But public, unrestricted dissemination of functional viral code to, say, disturbed fifteen year olds intent on causing havoc is unnecessary and harmful and ought to be punished in the same way we place pre-emptive restrictions on other potentially harmful acts.

The arguments protecting an author's right to publish detailed, functional viral code are based on the following questionable assumptions and reasoning:

- All speech is protected under the First Amendment to the U.S. Constitution;
- Written viral code is speech;

- Therefore, writing and publishing viral code cannot be forbidden by law in the U.S.

However, Prof. Virginia Black of Pace University in New York, a specialist in the philosophy of law, points out that not all speech is protected. One can prevent or punish speech on many grounds, even in the U.S. For example, one can

- Show that such speech or writing is harmful.

This utilitarian approach balances harmful consequences against a right. For example, there are prominent signs posted at every U.S. airport security barrier warning that all references to bombing or hijacking, including jokes, may be prosecuted under U.S. federal law. However, any claimed harmful consequences would have to be agreed upon as serious, "for all the time people harm each other and we would live in a totalitarian state if *every* alleged harm were legally prohibited."

- Show that such writing amounts to a *speech act* and so is *not* protected under a freedom-of-speech law because its intent is ... to act or get others to act in a certain way.

Inciting others to commit crimes is not protected speech. If disseminating computer viruses becomes a crime, it may be possible to punish people for recommending that others spread viruses.

- Show that whereas something may be a form of speech, it nevertheless abridges or interferes with *another right* that people have.

So just because something may be speech, it does not automatically take precedence over every other right we accept. Releasing a virus by publishing functional code harms everyone whose computers are infected by the virus.

- Ignore the strictly rule stuff above and argue from an *age-old equity principle*: the law does not protect wrongful gain (one may not gain from another's loss).

The person who publishes the viral code profits through the sale of the book, which tells some unscrupulous person how to write a virus which causes someone else's loss. The author is indirectly profiting from someone else's loss.

But is viral code speech at all, let alone protected speech?

I think that considering programs to be a form of speech rests on a misperception due to the way we represent programs. Programs look like written language. Programs use letters and numbers. They can be interpreted by human beings.

It's irrelevant how we *represent* computer programs. A program is the instructions themselves, not the medium in which they're coded. A program in assembler is a program whether it resides on a hard disk, a floppy diskette, or a portion of a memory array. Indeed, that sequence of computer instructions would be the program itself even were it written on a papyrus, chiselled in stone, signalled by semaphore or printed in a book.

If computer programs were represented as coloured squares and circles with lines coming out of them, perhaps we would be less inclined to think of them as speech. For example, consider a wire-board controlling a card sorter. Is the wire-board speech? Not in any sense most people would use the word. How about a paper punch tape controlling a machine tool? What about a useful computer program expressed as machine language codes (0001010000110101)? I don't consider these codes to be speech and I don't think anyone else should either.

The general principle I attack in the assumption that published viral code is speech is that describing something or including something in a category need not be agreed to. If I decide to call cats (or ketchup) vegetables, this may be odd and interesting (or politically expedient), but other people don't have to agree to my use of the language. Here are some analogies to think about:

- Someone laces ink with poison and prints books with it. Anyone who touches such a book gets sick. Can writing this book be protected by First Amendment rights?

One lawyer replied that the case was no different from hitting someone over the head with a heavy book. The poison ink is not the speech, the ink is.

- Angrily Berserk works in a factory with Charming Delightful and Eerily Frustrated. Angrily decides to kill Charming by publishing a printed tape for the robotic equipment they all use. Eerily cuts out the machine-readable tape and includes it in Charming's pile of tapes for the next day's operations. Charming doesn't notice anything wrong and gives the tapes to the robot, which reads the instructions into its memory. Some time later, Charming's robot punches 2,000 extra holes at random, four of which end up in Charming's head. Is Angrily's act protected because the published paper tape contains letters and numbers such as “A0 1F 22 BB?”

- A molecular geneticist named Gene Hacker is arrested by police for having made several colleagues very ill with a new virus. Gene constructed the virus from bits and pieces of known RNA. Gene argues in court that his act is protected by the First Amendment: the virus, he claims, is speech. It is speech because it consists of four nucleotide codes, A, U, C and G, put together in a particular way. He claims to “write” using ribonucleotides just as computer virus authors “write” using machine instructions. Gene argues that his virus is just as much a symbolic expression of his opinions and feelings as the virus authors' printing their viral

codes in publications. Indeed, he argues, he has been “publishing” his biological virus just as they have published their computer viruses.

- Faced with considerable scepticism from the court, Gene's lawyers continue the battle. Some lawyers and thinkers argue that publishing computer viral code cannot be a crime because the viral code is only potentially dangerous. The virus machine instructions written on paper don't actually do anything until they enter the victims' computers and get executed by their central processing units. By analogy, Gene cannot be guilty of a crime, since his virus was completely inactive until it entered his victims' cells and got translated by their ribosomes.

Viral code is a program. Programs are not speech. Therefore viral code is not speech.

I do not argue that writing about viruses, describing how to create them, or advocating that other people write or disseminate viruses could or should be prosecuted. Nor do I suggest that private communication from an individual to another named individual should in any way be curtailed. If a person wants to exchange functional viral code with another, so be it.

The issue is *publication* of such code, by which I mean uncontrolled dissemination of viruses at large via newspapers, magazines, journals, electronic mail distribution lists such as Internet lists, CompuServe forums, and open BBS systems.

Publishing *functional* viral code in ready-to-run form is an outrage that need not be protected by the First Amendment. It will be a difficult task distinguishing between legitimate and illegitimate representation of viral code--but the job has to be done. If we as a society decide that writing and disseminating viruses are criminal acts, we are entitled to prosecute such writers without fear of having First Amendment arguments hampering our efforts.

The *Network World* essay provoked a storm of activity on the Internet (specifically, the lawyer's aba-unix-list@cayman.com list). I received over 100 Kb of electronic mail on this issue within one week of publication of the opinion piece, mostly from lawyers interested in the constitutional law issues. In general, the lawyers disagreed strongly with the assertion that a virus is not speech. There was some interest, however, in the question of whether disseminating ready-to-go viruses through an electronic mail network could be forbidden without conflicts with the First Amendment.

One Internet correspondent commented that any attempt to suppress the publication of viral code, whether speech or not, was pointless. Such suppression would be another example of what he called, “security by obscurity.” He pointed out that anyone who is interested enough in decoding viruses can use widely-available binary editors.

An author who did publish workable code for viruses claimed in his defense that he had not seen his published viruses appearing in the wild, and therefore the risks of publication are overrated. To this position I answer that although keeping functional viral code out of the hands of novice

programmers is certainly not sufficient to stem the tide of new viruses, it can only help the battle. Who knows how many nut-cases were initiated into the dubious joys of virus writing by copying those printed viruses?

Such laws would also make a strong statement about the values of society. We do not approve of viruses, and we are willing to punish people who spread such programs about. Faced with clear cut interdiction, it would be easier to convince young people that the game was not worth the risk.

Virus bulletin board systems

Another issue is virus-distribution BBSs. As described in the section on the Bulgarian virus factory, some BBS operators invite participants to download viruses in return for uploading at least one new virus. In contrast with these underground BBSs, there are a few BBSs which cater to serious antivirus researchers. These BBS operators require real names, not pseudonyms; they check the bona fides of prospective participants by calling their employers and verifying that the candidates have a legitimate reason for downloading viruses. They do not require new viruses or any other kind of initiation rite.

Some respected anti-virus researchers object to the existence of any BBS that allows viruses to be downloaded. One argument is that such BBSs contribute to the spread of viruses; another is that their existence in the AVPD community makes it impossible to attack the “bad” virus-distribution BBSs. How can we claim to oppose the distribution of viruses if we do it ourselves?

Legitimate BBS operators argue that their intentions are clear and that there is no evidence that their BBSs contribute to the spread of viruses. The people using their services are professionals in the computer security field, including AVPDs, OS specialists working on anti-virus strategies and security officers from large corporations who wish to test AVPs themselves. All the viruses available in the secured areas of their BBSs are generally available in the wild, but at much greater cost. It is unacceptable, argue these operators, for anyone to impugn their motives or the professional responsibility of their members.

Such debates have a tendency to become heated.

My own position is that it is possible to formulate standards of containment for computer viruses just as virologists, bacteriologists and molecular geneticists have devised standards of containment for dangerous biological organisms.

For example, the Centers for Disease Control (Atlanta, GA) have defined standards for storing the remaining stocks of smallpox. These organisms are stored in a three-level containment building in which each layer has lower air pressure than the adjacent outer layer, forcing airflow inward. Workers wear sealed protective suits when handling the smallpox stocks, and they spray the suits with caustic anti-microbials when leaving the inner area. Then the workers take their

suits off and shower under antibiotic sprays in the middle area before being allowed into the outer zone.

Genetically engineered viruses and bacteria often include deletion mutations that mean the organisms cannot survive in the wild. They can live and reproduce only under special conditions such as on media supplemented with particular food substances.

In cyberspace, we could devise containment barriers such as computers without removable storage media and with encrypting modems. As for damaging viruses, we could require that every virus being studied in a secured facility be modified at once by adding or appending a special code module. The code would force the damaged virus to look for a condition specific only to the modified OS on which it was intended to run. On normal, unmodified OSs, the damaged virus would fail to reproduce or perhaps even to execute at all.

AVPD testing

Many organizations have published the results of AVPD tests. The notes at the end of this chapter list 49 reviews of AVPDs, each carried out with a different methodology and with different results. When you read such reviews, keep in mind that much of the evaluation is subjective. Ease-of-use, ease-of-installation and quality of documentation are obviously subjective. But the choice of the test battery is also subjective, even though the results are reported as if they were hard data. “This product recognized 91.3% of the viruses in the test battery and that product recognized only 89.2%” certainly sounds like a precise comparison. Unfortunately, the apparent precision may mislead readers into believing that a 91.3% score means the first product is necessarily better at identifying viruses than the product which identified “only” 89.2%. Such a conclusion is unjustified.

Virus test libraries are maintained by all AVPDs and also by independent agencies and individuals. For a period, the NCSA maintained a virus library. Patricia Hoffman puts enormous effort into managing a library on which she bases VSUM, a hypertext database which provides easy access to detailed information for over a thousand viruses and variants. All such efforts depend on the cooperation of countless researchers and other correspondents. These collaborators must supply the librarian with infected files and diskettes along with accompanying documentation on who found the virus where and when.

At any time, virus librarians can either use the virus collection for their own AVPD tests or make the battery of viruses available to others for test purposes. Either route can be acceptable to the AVPD community--as long as the following principles prevail in all tests:

- Tests must be announced in advance.
- The test library must be made available to every AVPD whose product is to be compared with other products *before* the test is carried out.

- The test must be carried out with the latest versions of AVPs submitted by their developers once they have been informed of the upcoming test.

To withhold the test library from AVPDs immediately renders the AVP evaluation suspect. Most AVPs include virus signatures as part of their armament. If AVPDs have not had the opportunity to test their AVPs against available batteries of viruses, how are they to determine suitable signature strings? If the library is not shared, then the AVPDs who contribute the most viruses will naturally get the highest scores.

Even if the library is shared among competing AVPDs, there are other problems for the industry to sort out. For example, sharing the library among AVPDs who contribute unequally to the collection may be seen as reducing the competitive position of the main contributors. The only solution to this problem is perceptual: the AVPDs have to come to a consensus that the aim of their collaboration is to improve *all* AVPs' capacity to detect and neutralize viruses. Competition among AVPDs should be concentrated in providing good quality software with low rates of false positives and low rates of false negatives.

As a user, you should be aware that the quest for ever-higher apparent rates of virus identification may be rooted more in marketing than in technology. As pointed out in an earlier section of this chapter, the industry cannot even agree on precisely how to enumerate viruses. If the AVPD tester is a lumper, the total number of viruses identified by a specific AVP will appear lower than if the same product were tested on the same sample by a splitter. It is impossible to compare the quality of AVPDs without knowing the test methodology used to generate the results.

In addition, the identification percentages based on virus libraries must not be construed as a measure of how effectively the rated AVPDs will perform in reducing the likelihood that your computer will be infected. Remember, over 80% of all virus infections are by Jerusalem and Stoned viruses. Imagine that both AVPs A and B can detect Jerusalem and Stoned equally well (100% identification, no false positives, no false negatives). Suppose product A spots 95.2% of the remaining 20% and product B spots *only* 90% of that remaining 20%. Then product A will have an effective score of 80% (for Jerusalem and Stoned) plus 95.2% of 20% or 19% = 99% detection. Product B will have the same 80% + 90% of 20% or 18% = 98% detection. When you look at the difference that way, it hardly seems to justify all the fuss in the advertisements.

Public education

As a society, we must apply ethical principles to technology. There are many young adults today who have grown up with PCs and misuse them without qualm. Eleven year olds have successfully written viruses.

How many parents have given their children computers and then ignored the way their kids use those computers? Children have hacked into private networks, stolen telephone services, and damaged medical records--all without the slightest involvement from their parents. One child

had persuaded his parents that he needed banks of modems to play; actually, he was running a massive modem- and FAX-number discovery operation, scanning thousands of numbers per night and selling the results at a dollar a pop to the phone number brokers who supply criminal hackers and junk FAX users.

What, exactly, is little Johnny doing down there in the basement with all that equipment you bought him?

By all means install anti-virus software on your PCs. Use access control software, audit trails, and all the paraphernalia of computer security to protect your systems. But in the long run, law and order are best served by coming to agreements about the principles of morality, not simply by putting up barriers. We need to teach ourselves and our children that technology can be misused just as any other tool can. When normal people have just as strong an emotional revulsion towards virus writing as towards smashing windows, we will be in a better position to fight the computer virus plague.

CHAPTER NOTES

1. Phillips, R. (1990). Computer viruses: a threat for the 1990s. DROIS IS09-250-101. This excellent report provides a concise, well organized overview of the virus problem.

2. The following collection includes valuable reviews of technical and theoretical aspects of the virus problem:

   Hoffman, L. J. (1990). *Rogue Programs: Viruses, Worms, and Trojan Horses*. Van Nostrand Reinhold (New York). ISBN 0-442-00454-0.

3. Spafford, E. H., K. A. Heaphy, & D. J. Ferbrache (1989). *Computer Viruses: Dealing with Electronic Vandalism and Programmed Threats*. Originally published by ADAPSO. Reprinted as "What is a computer virus?" in Hoffman (see note 2, above), Chapter 2, p. 29 ff.

4. Concerning the mythical "Gulf War" virus, see

   Anonymous (1992). The Gulf War flu. *U.S. News & World Report* 112(2):50 (Jan 20, 1992).

   Schwartau, W. (1992). Iraqi virus hoax. *Security Insider Report* (April 1992).

5. Cohen, F. B. (1986). *Computer Viruses*. Ph.D. dissertation, University of Southern California. Published in *Computer & Security* 8(4):325. A section of this paper appears as "Computational aspects of computer viruses" in Hoffman (see note 2, above), p. 324.

6. Gibbs, M. (1993). *The Computer Virus Threat: A Practical Strategy for Prevention and Cure*. Special Research Report (Patricia Seybold Group). This study of the virus problem includes a good historical review.

7. The story of the Creeper is found in note 13 of the Branscomb, A. W. (1990). Rogue computer programs and computer rogues: tailoring the punishment to fit the crime. *Rutgers Computer and Technology Law Journal* 16(1). Reprinted in Hoffman (see note 2, above).

8. Russell, D. & G. T. Gangemi (1991). *Computer Security Basics*. O'Reilly & Associates (Sebastopol, CA). ISBN 0-937175-71-4. This textbook has a good review of the virus problem in Chapter 4 (p. 79 ff).

9. Highland, H. J. (1988). The Brain virus: fact and fantasy. In: Hoffman (see note 2, above).

10. Highland, H. J. (1988). Computer viruses--a post mortem. *Computers & Security* 7(2):117.

11. Stefanac, S. (1988), Mad Macs. *Macworld*, November 1988. Reprinted in Hoffman (see note 2, above).

12. Tippett, P. S. (1991). The kinetics of computer virus replication. *Proceedings* of the Fourth Annual Computer Virus Symposium of the DPMA, New York, February 1991.

13. NCSA (1991). *Computer Virus Market Survey*. National Computer Security Association (Carlisle, PA).

14. USA Research (1992). *1992 IPA Computer Virus and Hacker Study*. Technology Company Information Reports, USA Research Inc. (Portland, OR).

15. Daly, J. (1992). Virus threat could be overstated: IBM researcher suggests sparse connectivity reduces virus contagion. *Computerworld* 26(37):16.

16. Haney, K. (1992). Viruses in an OS/2 environment: Remembrances of things past and a harbinger of things to come. *Proceedings* of the 1st International Virus Prevention Conference and Exhibition (NCSA), Washington, DC., October 1992.

17. Radatti, P. V. (1992). Heterogeneous computer viruses in a networked UNIX environment. *Proceedings* of the 1st International Virus Prevention Conference and Exhibition (NCSA), Washington, DC.

18. Solomon, A. (1992). Common viruses: a classification system. *Virus News and Reviews* 1(3):105.

19. Concerning the Columbus Day virus, see

    DROIS (1990). Security issues of 1989: a retrospective. Report #IS09-400-201 (p. 210 ff).

20. Concerning Michelangelo, see

    Alexander, M. (1992). This artful Michelangelo could unleash havoc: serious damage predicted for March 6. *Computerworld* 26(8):1.

    Alexander, M. (1992). No rest for virus defenders: little havoc wreaked by Michelangelo strain. *Computerworld* 26(10):1

    Bales, R. (1992). On-line with the Executive Director. *NCSA News* 3(2):2.

21. For more information on virus generators, see the following papers:

Solomon, A. & D. Stang (1992). Virus Creation Laboratory: a review. *Virus News and Reviews* 1(6):309.

Stang, D. (1992). The Phalcon/Skism Mass-Produced Code Generator 0.90b. *Virus News and Reviews* 1(7):383.

Schwartau, W. (1992). Virus Labs. *Security Insider Report* (Aug 1992):1.

22. The following recent articles deal with Macintosh viruses:

Schneier, B. (1994). Virus killers: Macworld Lab tests virus software and survives. Macworld 11(7):116

Hasson, M. (1992). Virus alert. MacUser 8(11):268

Norr, H. (1992). Trojan horse carries new MBDF A virus. *MacWEEK* 6(8):3

Norr, H. (1992). Cornell students jailed briefly, on virus, Trojan horse charges. *MacWEEK* 6(9):3

Norr, H. (1992). Misdemeanor plea for MBDF A authors. *MacWEEK* 6(32):147

Anonymous (1992) New virus: Virex user discovers new Macintosh virus. *EDGE: Work-Group Computing Report* 3(101):10

23. Bontchev, Vesselin (1991). *The Bulgarian and Soviet virus factories.* Paper circulated electronically. Downloaded from NCSA section on CompuServe.

24. For discussion of UNIX viruses, see

Anonymous (1992). Anti-virus protection for Unix. *Digital News & Review* 9(23):34

Sherman, M. (1990). Unix could be next target of growing virus invasion. *Government Computer News* 9(23):62

Palmer, S. D. (1989). Anti-virus wares may protect mainframes. *Federal Computer Week* 3(21):33

25. Concerning the Internet and the Internet Worm of 1988, see

Lynch, D.. & M. Rose (1993). *The Internet System Handbook*. Addison-Wesley (Reading, MA). ISBN 0-201-56741-5.

Quarterman, J. S. (1990). The Internet. In: *The Matrix: Computer Networks and Conferencing Systems Worldwide*, pp. 277-345. Digital Press/DEC (Bedford, MA). Reprinted in Datapro *Management of Data Communications*, report #CS10-650-101.

Spafford, E. H. (1989). The Internet worm incident. *Proceedings* of the 1989 European Software Engineering Conference (ESEC 89). Springer Verlag. Reprinted in Hoffman, note 2 above, p. 203 ff.

26. Recent reviews of anti-virus PC products gleaned through a quick search of Ziff-Davis Communications' *Computer Database Plus* via CompuServe. For convenience, these articles are listed in reverse chronological order rather than by author:

Ferrill, P., Mace, S. & Sercan, A (1995). An ounce of prevention. *InfoWorld* 17(7):84

Chowning, D. (1995). Anti-virus solutions for client/server - part 2. *Data Based Advisor* 13(1):102

Gann, R. (1994). Virus protection for PCs, servers and the network. *PC User* (249):111

Anonymous (1994). Virus-prevention NLMs: seven convenient and effective programs that defend against the threat of computer viruses. *Byte* 19(8):129

Anonymous (1994). Anti-virus NLMs. *PC User* (238):108

27. The following articles discuss the legal implications of the Internet Worm case:

Markoff, J. (1990). Computer intruder gets probation and fine but avoids prison term. The New York Times 139:1 (May 5, 1990).

Eckerson, W. (1990). Net managers favor jail term for hacker Morris. *Network World* 7(20):4

Alexander, M. (1990). Morris sentence spurs debate. *Computerworld* 24(20):128

Alexander, M. (1990). Justice failed in refusing to make Morris an example. *Computerworld* 24(20):23

Ubois, J. (1991). Supreme Court refuses to hear Morris case. *MacWEEK* 5(36):15

28. Kabay, M. E. (1993). Viruses should not be protected by First Amendment. *Network World* 10(9):27

29. Licenses for Patricia Hoffman's VSUM are available through the NCSA (717-258-1816) or directly from Ms Hoffman (408-988-3773).

<<end of text>>

LAST MODIFIED: February 1996
NCSA Guide to Enterprise Systems Security
FILE: CH_04_C.WPD
Chapter 4: Personnel and legal issues

After studying this chapter, the reader should be able to
1. define appropriate procedures for checking candidate background when hiring new staff.
2. recognize danger signals in the behaviour of employees.
3. define and enforce the separation of duties required for effective security.
4. terminate employment without compromising enterprise security.
5. develop a summary of legal liability issues affecting information systems.
6. define and justify a strategy for preventing software theft.
7. establish a policy for dealing with malfeasance by hierarchical superiors.

[A] Hiring

Crime is a human issue, not a technological one. True, technology can reduce the incidence of computer crimes, but the fundamental problem is that people can be tempted to take advantage of flaws in our information systems. The most spectacular biometric access control in the world won't stop someone from getting into your computer room if the janitor lets them in □just to pick up a listing.□

Hiring new employees poses a particular problem; growing evidence suggests that many of us inflate our resumes with unfounded claims. Be especially careful of vague words such as □monitored,□ and □initiated□--find out what the candidate did in specific detail, if possible. Be sure that references are followed up at least to verify that the candidate really worked where the resume claims they did.

Donn Parker cites the case of Eugene B. Slear, hired in January 1979 by a university hospital. Mr Slear had an impressive resume and a positive attitude. He was assigned responsibility for new accounts-receivable and billing systems. Over the next few years, he used the computer system to issue invoices to suppliers for imaginary data processing supplies. The suppliers were false fronts for himself. In this way, he embezzled $126,564. When his upper management announced that external auditors would be checking the records, he managed to convince them to delay the audit for seven months. When he could no longer delay the audit, he resigned. Coopers & Lybrand found the fraud and reported him. He was arrested, charged, and convicted of fraud. He spent 18 months in jail.

The irony of this story is that in 1973, Mr Slear had been convicted of embezzlement carried out through computer programming. The hospital would have avoided a good deal of trouble if it had checked his background more thoroughly.

Unfortunately, there is a civil liberties problem when considering someone's criminal record. Once someone has suffered the legally-mandated punishment for a crime (fines, community service, imprisonment), discriminating against them in hiring may be a violation of their civil

rights. Can you exclude convicted felons from any job openings? from job openings similar to areas in which they abused their former employers' trust? Are you permitted in law to require that prospective employees approve background checks? Can you legally require polygraph tests? Drug tests? You should consult your corporate legal staff to ensure that you know your rights and obligations in your specific legal context.

Even checking references from previous employers is fraught with uncertainty. Employers may hesitate to give bad references even for incompetent or unethical employees for fear of lawsuits if their comments become known or even if the employee fails to get a new job. Today, you can't even be sure you'll get an answer to the simple question, "Would you rehire this employee?"

Ex-employers must also be careful not to inflate their evaluation of an ex-employee. Sterling praise for a scoundrel could lead to a lawsuit from the disgruntled new employer.

For these reasons, a growing number of employers have corporate policies which forbid discussing a former employee's performance in any way, positive or negative. All you'll get from your contact in such cases is, "Your candidate did work as an Engineer Class 3 from 1991 to 1992. I am forbidden to provide any further information."

It is a commonplace in the security field that some people who have successfully carried out crimes have been rewarded by a "golden handshake" (a special payment in return for leaving) and even positive references. The criminals can then move on to victimize a new employer. For the same reasons that we cannot know exactly how many crimes are carried out, we can't tell how often this extortion takes place.

To work around such distortions, question the candidate closely about details their education and work experience. The answers can then be checked for internal consistency and compared with the candidate's written submissions. Liars hate details: it's so much harder to remember which lie to repeat to which person than it is to repeat the truth. Ask experienced employees to interview the candidate. Compare notes in meetings among your staff. I recall one new employee who claimed to have worked on particular platform for several years--but didn't know how to log on. Had he chatted with any of the programmers on staff before being hired, his deception would have been discovered quickly enough. Ironically, had he told the truth, he might have been hired anyway.

Before allowing new employees to start work, they should sign an employment agreement which stipulates that they will not disclose confidential information or trade secrets from their previous employer. Another clause must state that they understand that you are explicitly *not* requesting access to information misappropriated from their previous employer or stolen from any other source.
The Uniform Trade Secrets Act, which is enforced in many jurisdictions in the U.S., provides penalties which are triple the demonstrated financial damages caused by the data leakage plus attorney's fees.

Other clauses in the employment agreement which apply to termination of employment are discussed below in the section on legal issues.

[A] Ongoing management

Security managers don't have to be paranoid, they just have to act as if they're paranoid. Work with your colleagues to help you identify behaviour that indicates increased risk for your organization.

Treat people with scrupulously fair attention to written policies and procedures. Selective or capricious enforcement of procedures is harassment. If you allow some of your staff to be alone with the cheque run but force all others to be accompanied, the latter can justifiably interpret your inconsistency as an implicit indication of distrust. Such treatment may move certain employees to initiate grievances and civil lawsuits or to lay complaints under criminal statutes.

Inconsistency reduces your effectiveness. Suppose George is known for a no-nonsense, bluff manner. He sticks to technical issues with his staff; he rarely socializes with his colleagues and almost never talks about anyone's feelings. George discovers that his chief programmer, Sally, seems preoccupied and irritable lately. What is Sally to think when George suddenly enquires sweetly about how things are at home and whether she is under any strain? It would be easy for Sally to misinterpret George's apparent concern as either an unwarranted intrusion into her private life, a sexual come-on, or an accusation. George's unusual behaviour could trigger alarm bells even in innocent employees.

[B] Opportunities to use the system in unauthorized ways

What would you do if you discovered that an employee who used to occupy your current office still had the key? You would politely ask them to give it up. No one would question the reasonableness of such a request. However, when you remove access to the network server room from a system analyst who has no reason to enter that area, you may be treated to resentment, sulking and abuse. People learn about keys when they're children; they don't extend the principles to information security. People sometimes treat access controls as status symbols; why else would a CEO who has no technical training demand that his access code include the tape library and the wiring closet?

You can overcome these psychological barriers to better security by introducing a different way of looking at vulnerabilities. When you identify an opportunity to use the system in unauthorized ways, turn the discussion into a question of protecting the person against undue suspicion. For example, if one of your employees were found to have more access to secured files than required for her job, you could explain that having such capabilities put her at risk. If anything ever did go wrong with the secured files, she'd be a suspect. There's no need to frame the problem in terms of suspicion and distrust.

With these principles in mind, be alert to such opportunities as being alone in a sensitive area, having access to unencrypted backups, or being the only programmer who knows anything about the internals of the accounting package.

[B] Redundancy and security

For most areas of information processing, redundancy is generally viewed as either a Bad Thing or an unavoidable but regrettable cost paid for specific advantages. For example, in a database, indexing may require identical fields (items, columns) to be placed in separate files (datasets, tables) for links (views, joins) to be established. However, in managing personnel for better security, redundancy is a requirement.

Redundancy in this context means having more than one person who can accomplish a given task. Another way of looking at it is that *no knowledge shall belong to only one person* in an organization.

Unique resources always put our systems at risk; that's why companies like Tandem, Stratus and others have so successfully provided computer systems for critical-task functions such as stock exchanges and banking networks. Such redundant or fault-tolerant computer systems and networks have twin processors, channels, memory arrays, disk drives and controllers.

Similarly, a fault-tolerant organization will invest in cross-training of all its personnel. Every task should have at least one other person who knows how to do it--even if less well than the primary resource. This principle does not imply that you have to create clones of all your employees; it is in fact preferable to have several people who can accomplish various parts of any one person's job. Spreading knowledge throughout the organization makes it possible to reduce the damage caused by absence or unavailability of key people.

If a single employee is the only person who knows about a critical function in your organization, you are at risk. Your organization will suffer if the key person is away, and it may suffer if the key person decides to behave in unauthorized and harmful ways. Do you have anyone in your shop whose absence you dread? Are there any critical yet undocumented procedures for which everyone has to go ask Joe?

A client in a data centre operations management class volunteered the following story. There was a programming wizard responsible for maintaining a key production program; unfortunately, he had poor communication skills and preferred to solve problems himself rather than training and involving his colleagues. "It'll be faster for me to do it myself," he used to say. During one of his rare vacations, something went wrong with "his" production program, shutting down the company's operations. The wizard was in the north woods, out of reach of all modern communications; the disaster lasted until he returned.

Not only does your organization suffer, but also Mr/Ms Indispensable suffers from the imbalance of knowledge and skill when no one else knows what they know. Some indispensables are dedicated to the welfare of their employer and of their colleagues. They may hesitate to take

holidays. If their skills are needed from hour to hour, it becomes more difficult to allow them to participate in committee meetings. These are the people who wear beepers and cannot sit undisturbed even in a two-hour class. If the Indispendable's skills affect day-to-day operations, they may find it hard to go to offsite training courses, conferences and conventions. Despite their suitability for promotion, indispensable people may be delayed in their career change because the organization finds it difficult or expensive to train their replacement. In extreme cases, the newly promoted manager may find themselves continuing to perform specialized duties that ought to be done by their staff. I remember my amazement when the newly-promoted VP of information systems at a service bureau informed me that he was the only person on the technical support and operations team who was competent to reconfigure the mainframe computer.

Sometimes a person continues to be indispensable because of fear that their value to their employer resides in their private knowledge. Such employees resent training others. The best way to change their counter-productive attitude is to walk what you talk: share knowledge with them and with everyone else in your group. Make education a normal part of the way you work. Encourage cross-training by allocating time for it. Make cross-training a factor in your employee evaluations. Have discussions of current topics from the trade press and academic journals. Start a journal club where people take it in turn to present the findings from recent research in areas of interest.

Reluctance to explain their job to someone else may mask unauthorized or illegal activity. Take for example the case of Lloyd Benjamin Lewis, assistant operations officer at a large bank. He arranged with a confederate outside the bank to cash fraudulent cheques for up to $250,000 each on selected legitimate accounts at Lewis' branch. Using a secret code stolen from another branch, Lewis would scrupulously encode a credit for the exact amount of the theft, thus giving the illusion of correcting a transaction error. Lewis stole $21.3 million from his employer between September 1978 and January 1981, when he was caught by accident. For unknown reasons, a computer program flagged one of his fraudulent transactions so that another employee was notified of an irregularity. It did not take long to discover the fraud, and Lewis was convicted of embezzlement. He was sentenced to five years in a federal prison.

Since Lewis was obliged to be physically present to trap the fraudulent cheques as they came through the system, he could not afford to have anyone with him watching what he did. I doubt that Lewis would have been enthusiastic about having to train a backup to do his job. If anyone *had* been cross-trained, I doubt the embezzlement would have continued so long and been so serious.

[B] Problems with schedules

Lloyd Benjamin Lewis took his unauthorized duties (stealing money from his bank) so seriously that during the entire period of his embezzlement, about 850 days, he was never late, never absent, and never took a single vacation day in over two years. As a data centre manager, I would have been quite alarmed at having an employee who had failed to be absent or late a single day in more than two years. How would you know what would happen if Mr Perfect really *were* away? The usual rule in companies is that if an employee fails to use vacation days, they

can be carried over for a limited time and then they expire. This is supposed to be an incentive to take vacation time. For normal, honest employees it probably works fine. For dishonest employees who *have* to be present to control a scam, losing vacation days is irrelevant.

I recommend that every employee be required to take scheduled vacations within a definite--and short--time limit. No exceptions should be permitted. Excessive resistance to taking vacations should be investigated to find out why the employee insists on being at work all the time.

[B] Changes in behaviour

Any kind of unusual behaviour can pique the curiosity of a manager. Even more important, any *change* in behaviour should stimulate interest. Is Miss Punctual suddenly late--day after day? Did Mr Casual start showing up in hand-tailored suits? Why is Miss Charming snarling obscenities at her staff? What accounts for Charles' working overtime every day all of a sudden--in the absence of any known special project? Is Yosuf, that paragon of perfection, now producing obvious errors in simple reports? How is it that the formerly complaisant Waclav is now a demanding and bitter complainer?

Any radical change in personality should elicit concern, too. If the normally relaxed head accountant now has beads of sweat on her forehead whenever you discuss the audit trails, perhaps it's time to look into her work more closely. Mr Bubbly is now a morose whisky-swilling sourpuss: why? The formerly grim Schultz now waltzes through the office with a perpetual smile on his face. What happened? Or what *is* happening?

All of these changes alert you to the possibility of subterranean changes in the lives of your employees. Although these changes do indeed affect the security of your organization, they also concern managers as human beings who can help other human beings. Mood swings, irritability, depression, euphoria--these can be signs of psychological stress. Is your employee becoming alcoholic? a drug addict? abused at home? going through financial difficulties? having trouble with teenagers? falling in love with a colleague? Of course you can't help everyone, but at least you can express your concern and support in a sensitive and gentle way. Such discussions should take place in private and without alarming the subject or exciting other employees. If you feel out of your depth, by all means involve your human resources or personnel department. They will either have a psychologist or trained counsellor on staff or be able to provide appropriate help in some other way.

There are sad cases in which employees have shown signs of stress but been ignored, with disastrous consequences: suicides, murders, theft, and sabotage. Be alert to the indicators and take action quickly.

With so much of our organizations' financial affairs controlled by information systems, it is not surprising that sudden wealth may be a clue that someone is committing a computer crime. A participant in the *Information Systems Security Course* reported that an accounting clerk at a U.S. government agency in Washington, D.C. was arrested for massive embezzlement. The tipoff? He

arrived at work one day in a Porsche sports car and boasted of the expensive real estate he was buying in a wealthy area of the Capital region.

Not all thieves are that stupid. A healthy curiosity is perfectly justified if you see an employee sporting unusually expensive clothes, driving a sleek car after years with a rust-bucket, and chatting pleasantly about the latest trip to Acapulco when their salary doesn't appear to explain such expenditures.

The other kind of change may also indicate trouble. Why is your system manager looking both dejected and threadbare these days? Is he in the throes of a personal debt crisis? in the grip of a blackmailer? beset with a family medical emergency? a compulsive gambler on a losing streak? Again, on humane grounds alone you would want to know what's up in order to help. As a manager concerned with security, you have to investigate.

The manager's job is a tough one: you must walk the thin line between laissez-faire uninvolvement (and risk prosecution for dereliction of duty) and overt interference in the private affairs of your staff (and risk prosecution for harassment).

Written policies will help you; so will a strong and ongoing working relationship with your human resources staff.

[A] Separation of duties

The same principles that apply to the control of money should apply to control of data. Watch the tellers at a bank: when you deposit a large check, you'll see the teller going to a supervisor and having that person look the check over and initial the transaction. When bank tellers empty the automatic teller machines at night and fill the cash hoppers, there are *always* two people present. The person who creates a check is not the person who signs it.
In well-run information systems departments, data entry is distinct from validation and verification. For example, a data entry supervisor can check on the accuracy of data entry but cannot enter a new transaction without having their direct supervisor check their work. There is no excuse for allowing the supervisor to enter a transaction and then, effectively, authorize it. What if the entry were in error--or fraudulent? Where would the control be?

In quality assurance for program development, the principles of separation of duty are well established. For example, the person who designs or codes a program must not be the only one to test the design or the code. Test systems are separate from production systems; programmers must not have access to confidential and critical data which are controlled by the production staff. Programmers must not enter the computer room if they have no authorized business there; operators must not modify production programs and batch jobs without authorization.

When I was put in charge of operations at a service bureau, I trained two systems managers as soon as I could to take over the day-to-day management of the computer systems. When they were ready, I asked them to remove system manager capabilities from my account. I had no wish to intrude on their province of responsibility. My meddling with system parameters would cause

more trouble than it would solve. Were there to be an emergency, I could have been granted system management permissions and resumed my former role. This attitude exemplifies the concept of separation of duties.

In early 1995, the financial world was rocked by the collapse of the Barings PLC investment banking firm. The Singapore office chief, Nicholas Leeson, was accused of having played the futures market with disastrous consequences. The significant point in our context is that he managed to carry out all the orders *without independent overview.* Had there been effective separation of duties, the collapse would not have occurred.

[A] Firings and Resignations

The other end of the employer-employee relationship also deserves attention from a security-conscious manager. Taking our security mandate in the widest sense, we have to protect our employer and ourselves against potential damage from unethical, disgruntled or incompetent employees and against the legal consequences of improper firing procedures. Common sense and common decency argue for humane and sensitive treatment of people being fired and those who are resigning.

[B] Resignations

The potentially most dangerous form of employment termination is the resignation. The problem is summed up in the caption of a cartoon I once saw. A savage attack is in progress against a medieval town; a clan war chieftain confronts a singed and dirty warrior. "No, no, Thor! Pillage, THEN burn!" Like the warriors, employees rarely resign without planning. An employee may have an indefinite period during which he or she knows that resignation is imminent, whereas the employer may remain unaware of the situation. If the employee has bad feelings towards or evil designs on the current employer, there is a period of vulnerability unknown to management. Dishonest or unbalanced employees could steal information or equipment, cause immediate or delayed damage using programmatic techniques (the so-called "logic-bomb"), or introduce faulty data into the system ("data diddling").

The policies discussed above for ongoing management should reduce the risks associated with resignations. Your goal can be to make resignations rare and reasonable. By staying in touch with your employees' feelings, moods and morale, you can identify sources of strain and perhaps resolve problems before they lead to resignation.

[B] Firings

Firings give the advantage to employers. The time of notification can be controlled to minimize its effects on the organization and its business. For example, employers might find it best to fire an incompetent or no-longer acceptable employee before beginning an important new project or after a particular project has finished.

To reduce the psychological impact on other employees, it might also be best to fire someone at the end of the day before a long weekend, thus giving everyone a cooling-off period outside working hours. One hardly wants the buzz of conversation and speculation that often follow a firing to intrude on the work day.

A participant in my course told the following horrifying tale of a firing gone wrong: in a large company, the personnel department asked information security staff to suspend the access codes for more than 100 people who were to be fired at 18:00 on Tuesday. On Wednesday at 08:00, the security staff began receiving phone calls asking why the callers' logon IDs no longer worked. It turned out that the personnel staff had failed to inform the "victims" on time. The psychological trauma to both the employees who were fired and to the security staff was severe. Several security staff members had to be sent home to recuperate. The harm done to the fired employees was presumably even more serious.

[B] The fateful day

Let's suppose the time has arrived for the employee and the employer to part company. In both resignations and firings, security consultants unanimously advise instant action. Not for them the leisurely grace period during which employees wind down their projects or hand them off to other staff members. No, security officers are a hard lot, and they advise the following scenario: in a formal exit interview, and in the presence of at least two managers, an officer of the employer informs the employee politely that his/her employment is at an end. During the exit interview, the officer explains the reasons for termination of employment. The officer gives the employee a check for the period of notification required by law or by contract (e.g., the same period as that between pay checks) plus any severance pay due. Under supervision (preferably in the presence of at least one security guard), the employee is escorted to their work area and invited to remove all personal belongings and place them in a container provided by the employer. The employee returns all company badges, IDs, business cards available, credit cards, and keys. The employee is then ushered politely outside the building.

At the same time as all this is happening, all security arrangements must be changed to exclude the ex-employee from access to the building and to all information systems. Such restrictions can include:

- striking the person's name from all security-post lists of authorized access;
- explicitly informing guards that the ex-employee may not be allowed into the building, whether unaccompanied or accompanied by an employee, without special authorization by named authorities;
- changing the combinations, reprogramming access card systems, and replacing physical keys if necessary for all secure areas to which the individual used to have authorized access;

- removing or changing all personal access codes known to have been used by the ex-employee on all secured computer systems (microcomputers, networks, mainframes);

- informing all outside agencies (e.g., tape storage facilities, publications with company advertising) that the ex-employee is no longer authorized to access any of the employer's information or to initiate security or disaster recovery procedures;

- requesting cooperation from outside agencies in informing the employer if ex-employees attempt to exercise unauthorized functions on behalf of their former employer.

The task is made more difficult by seniority or if the ex-employee played an important role in disaster recovery or security. The employer should be assiduous in searching out all possible avenues of entry resulting from the person's position of responsibility and familiarity with security procedures.

In one story circulating in the security literature, an employee was fired without the safeguards suggested above. He returned to the workplace the next Saturday with his station wagon and greeted the security guard with the usual friendliness and confidence. The guard, who had known him for years, was unaware that the man had been fired. The ex-employee still had access codes and copies of keys to secure areas. He entered the unattended computer room, destroyed all the files on the system, and then opened the tape vault. He engaged the guard's help in loading all the company's backup tapes into his station wagon. The thief even complained about how he had to work on weekends. This criminal then tried to extort money from the company by threatening to destroy the backup tapes, but he was found by police and arrested in time to prevent a disaster for his ex-employee.

[B] Training replacements

One of the key organizational issues in planning or responding to termination of employment is training replacements for the departing employee. Such needs are voiced to justify policies allowing a more graceful, civilized and friendly approach to firings and resignations. It seems reasonable to encourage the departing employee to train the colleagues or new employees who will assume his or her responsibilities. However, cross-training should be part of the normal operations of all organizations.

[B] Psychosocial issues

What, no farewell party? Alas, security does interfere with the more obvious signs of friendliness. However, nothing stops a humane and sensitive employer from encouraging employees to arrange an after-hours party. If a resignation is on good terms, the employer may even arrange a celebration, possibly during working hours and maybe even at company cost.

A firing or a resignation on poor terms has two psychological dangers: effects on the individual concerned (embarrassment, shame, anger) and effects on the remaining staff (rumours, resentment, fear).

Both kinds of problems can be minimized by publishing termination procedures in organization documents provided to all employees; requiring all employees to sign a statement confirming that they have read and agreed to the termination procedures; consistent application of the termination procedures.

The personal shock of being fired can be reduced by politeness and consideration consistent with the nature of the reasons for being fired--although even nasty people should not be subject to verbal or physical abuse no matter how bad their behaviour; treatment consistent with that meted out to other fired employees (see "legal issues", below); and generous severance arrangements.

I once had to leave a wonderful company because of reasons beyond the control of the employer and myself. Neither the company nor I wanted to terminate my employment. The owner of the company offered to continue paying my salary until I found a job--and urged me to take all the time necessary to find a satisfactory job. His generosity eased the shock of having to leave my friends and colleagues.

Organizational turmoil can be reduced by convening organization-wide or departmental meetings to brief remaining employees on the details of significant termination; open discussion, including understanding how people respond to rupture of relationships. The remaining employees may have to suffer grief (a process, not a state).

Grief is a normal and healthy response to disruption of relationships (e.g.,death of a loved one, divorce, and even the loss of a co-worker). Some people value social relationships more than other aspects of their work and may be especially affected by firings. Grief involves stages of denial, anger, mourning and recovery. Trying to forestall such responses by denying that people legitimately have feelings is foolish and counter-productive. It is far better to encourage those who are upset to voice their feelings and to engage in constructive discussion.

[B] Style

The way an organization handles job termination affects more than internal relations. It also influences its image in the outside world. Prospective employees will think twice about accepting job offers from an organization that maltreats departing employees. Clients may form a negative impression of a company's stability if it abuses its own people. Investors may also look askance at a firm that gets a reputation for shoddy treatment of employees. Bad employee-management relations are a warning signs of long-term difficulties.

[B] Legal issues in firing people

There's another dimension to employment termination that depends on local laws and the litigation environment. The United States, for example, is said to be one of the most litigious

nations on the planet, perhaps because of the high number of lawyers per capita. Some guidelines for preventing legal problems related to firings:

- Build a solid, documented case for firing someone before acting. Keep good records, be objective, and get the opinions of several trustworthy people on record.

- Give the employee clear feedback long before considering firing.

- Offer the delinquent employee all reasonable chances to correct his or her behaviour.

Timing is important in employee relations, as it is in almost everything else we do. In particular, if an employee is found to be behaving improperly or illegally, there must be no marked delay in dealing the with problem. Such a person could sue the employer and individual managers. They could argue in court that the very fact that there was a delay in firing them was proof that the firing was due to other factors such as personality conflicts, racism, or sexism. A well-defined procedure for progressing through the decision will minimize such problems.

The critical legal issue is consistency. If rules such as those described above for the day of the firing are applied haphazardly, there could easily be grounds for complaining of unfairness. Those to whom the rules were strictly applied would justifiably feel implicitly criticized. How would we feel if we were singled out by having guards check what we took home from our desk--if everyone else got a party and two weeks notice? Such inconsistency would be grounds for legal proceedings for defamation of character. The company might lose and it might win, but what non-lawyer wants to spend time in court?

Another issue that arises in connection with firings and resignations is non-disclosure agreements. All such agreements must be included in a contract signed *before* the prospective employee begins work; it is impossible to force an existing employee to sign such an agreement. I remember one employer approaching me two years into my contract with them and asking that I agree that all patents I might develop--even those resulting from work at home in off-hours--would belong to the employer. I refused, and there was nothing they could do about it. Any attempt to threaten an employee with dismissal could result in a successful lawsuit for breach of contract and, if the threat were carried out, wrongful dismissal.
You, your legal department and your personnel department should study the necessity and feasibility of instituting a legally-binding contractual obligation to protect your company's confidential information for a specified period of time after leaving your employ. You cannot impose indefinite gags on people, but two to five years seems to be the common range. For this measure to be meaningful, you must include a clause in the initial employment contract that requires the departing employee to reveal his new employer.

Non-competition agreements require the employee to refrain from working for direct competitors for two to three years after termination of employment. Because this limitation can be an onerous impediment to earning a living, many jurisdictions will forbid such clauses.

My own view is that if a company is threatened by having an employee work for the competition, there is something seriously wrong with the first employer's security provisions.

[A] Legal liability in managing information

Given the immense cost of defending your employer and yourself against litigation, avoiding lawsuits is a necessary component of your security planning. Cooperate with your legal staff to determine your liability to lawsuits by employees, customers, third-party "data subjects" and "stakeholders.'

Suppose you fail to provide adequate disaster prevention, mitigation and recovery plans and procedures and your company burns down, stops functioning and loses all its clients, or gets shut down by regulatory agencies. You could be sued for damages by many people for the consequences of failing to exercise due care in your responsibilities. Employees could sue for recovery of lost wages or employment opportunities. Customers could sue for breach of contract such as failing to supply parts and therefore causing *them* to incur penalties from *their* customers.

Data subjects are the people about whom you store or manipulate information. A credit-rating company could be sued if its data are corrupted by programmatic error or malfeasance by its employees. A hospital information systems manager could be sued for allowing patient data to be leaked to a newspaper or to blackmailers. A human resources department could be sued for failing to protect the confidentiality of employee records.

Stakeholders include shareholders and users of the organization's services. If incompetent security managers in a publicly-traded company allow secret data about a merger escape to stock brokers and thereby cause stock manipulations, shareholders damaged by the premature disclosure could sue for damages to the value of their portfolios. In the U.S., the Securities and Exchange Commission would also be very interested in the case: such activities contravene the federal Foreign Corrupt Practices Act, which stipulates that company information affecting stock prices must be protected against premature disclosure.

Another thorny issue is the privacy of electronic mail. Many organizations make prospective employees or employees who begin to use electronic mail sign an agreement which states that the email system is to be used for company business only and that duly authorized staff members may investigate the content and use of company email at any time. Other employers treat email like phone conversations; all email is explicitly treated as private to the parties involved. In these organizations, systems staff are not allowed to read other employees' email.

A participant in one of my security courses told us that one morning she came in to work and found a passionate love letter in her email in-basket from a manager to someone else in the company. The writer had accidentally sent the email message to an extensive distribution list instead of only to the intended participant. Even more unfortunately, the writer was a married man. So was the intended recipient.

[A] Software theft

Recently I was downtown in Montreal and noticed a store advertising a software library. Curious, I went in and found an entire wall unit filled with programs of all kinds--databases, spreadsheets, games, communications packages, financial systems, engineering software, fourth-generation languages, compilers and so on. All the big names were there in their original boxes: LOTUS, Ashton-Tate, Walker Richer and Quinn, Aldus.... Each software package was plastered with a sticker so it could be borrowed by a user. The cost of borrowing the package was about 10% of the original cost of the software. The advertising flier disclaimer said

> The sole purpose of the club is to assist members in evaluating software before purchasing the original software at discounted prices. All evaluation rental fees are applied to purchases of original software.
>
> Members must be aware that the copyright laws of Canada expressly forbids [sic] duplication in whole or in part of the original software rented for evaluation.

What we had here was a full-fledged software piracy gang.

[B] Help from the SPA

I contacted the Software Publishers' Association (SPA) in Washington, DC for information on what could be done about the pirates. They sent me two folders full of interesting information I'd like to share with you. Fittingly for a section about copyright violations, I do have permission from Peter Beruk, their very helpful litigation manager, to quote extensively from their documentation.

Having earned my living as a programmer (long ago), I have never been very keen on software piracy. True, at one time in my youth I myself (blush) modified the code of a proprietary package so I could keep using it when my new employer wouldn't buy it. I regret having done that (I tell you about it to avoid being labelled as holier-than-thou) and have never done it since. Why have I come round to the view that unauthorized software copying is bad?

[Excuse me while I climb into the imaginary pulpit here....]Ahem. In the pamphlet entitled, "Software Use and the Law," the SPA writes,

> ...the problem of software theft has developed and threatens to impede the development of new software products. Romantically called "piracy," the unauthorized duplication of software is a Federal offense that affects everyone: large and small publishers and legitimate users. Even the users of unlawful copies suffer from their own illegal actions. They receive no documentation, no customer support, and no information about product upgrades.

The pamphlet goes on to make the following points:

- Title 17 of the U.S. Code forbids unauthorized copies of copyrighted material.
- Individuals have the right to make a backup copy of their software. All other copies are illegal.
- Educational institutions do not have any special right to copy software; however, many software publishers do offer special discounts or special (limited) educational versions of their products.
- User groups have no special right to share copyrighted software. Both the user group and the owner of the meeting place where illegal copying takes place may be prosecuted (hotel owners beware).
- Corporate users must not place single-user versions of software on their local area networks.
- A toll-free number (1-800-388-PIR8) is available to report software theft.

Before you go out and report your employers and colleagues to the SPA, though, it would be a very good thing to tell your manager (or your manager's manager if necessary) about the dangers of stealing software. You can point out that the illegality could easily be reported at any time by a disgruntled employee. Stealing software, like any other criminal action, lays a company open to blackmail. If someone hassles you for pointing this out, you should be aware that there are laws in effect in the U.S. to protect "whistle-blowers" (those who report unsafe or illegal activities in the workplace) against harassment.

[B] Sample terms for employee agreement

The SPA Self-Audit Kit included the following sample corporate employee agreement where "(Company/Agency)" represents the name of your company, agency, or department):

COMPANY/AGENCY POLICY REGARDING
THE USE OF PERSONAL COMPUTER SOFTWARE

1. Company/Agency) licenses the use of software from a variety of outside companies. (Company/Agency) dos not own this software or its related documentation and , unless authorize by the software developer, does not have the right to reproduce it.
2. With regard to use on local area networks or on multiple machines, (Company/Agency) employees shall use the software only in accordance with the license agreement.
3. (Company/Agency) employees learning of any misuse of software or related documentation within the company shall notify the department manager or (Company/Agency's) legal counsel.

4. According to the U.S. Copyright Law, persons involved in the illegal reproduction of software can ben be subject to civil damages of as much as $50,000 and criminal penalties, including fines and imprisonment. (Company/Agency) does not condone the illegal duplication of software. (Company/Agency) employees who make, acquire or use unauthorized copies of computer software shall be disciplined as appropriate under the circumstances. Such discipline may include termination.

I am fully aware of the software use policies of (Company/Agency) and agree to uphold those policies.

_____

Employee Date and Signature

I recommend that every employee (including top-level managers and officers) sign an information security agreement every year. Requiring such signed agreements ensures that

- no one in your organization can claim that they didn't know about the policy forbidding software theft;
- no employee can be bullied by a manager into breaking the law;
- your organization can prove that it actively opposes software theft if an action is launched by an aggrieved software vendor.

This last point warrants additional comment. According to the information I have received from lawyers, case law in both the U.S. and Canada includes precedents where firms have been found guilty of tolerating or encouraging unlawful activities because corporate policies were sporadic, half-hearted, or otherwise unconvincing. An organization must not only spout the letter of the law; it must actively

- disseminate information about corporate policy;
- support the acquisition of legal copies of required software; and
- apply appropriate penalties to employees who break the law.

A stated policy to prevent software theft is useless if employees are allowed to use stolen software openly. Many companies have an explicit policy that includes a commitment to obtain a legal copy of software that is necessary for employee effectiveness. An appropriate penalty might be to deduct the cost of a legal copy of a pirated package from both the employee's salary and from his or her manager's.(d)SPA Self-Audit Kit

The SPA Software Self-Audit package came with several simple tools for reducing software theft. Perhaps the simplest was a pair of metallic stickers with the anti-piracy hotline phone number in red. Putting such a sticker on every computer in the company; it is a useful reminder of corporate policy.

The SPA included two audit sheets to copy. The Audit Tally Sheet is to be used by individual computer users and it looks roughly like this:

COMPUTER PROGRAM	COMMERCIAL	ACCOMPANYING DOCUMENTATION?	PROOF OF PURCHASE?

The Audit Summation Sheet is for management to see the global results, including cost of compliance with copyright laws. It looks something like this:

A PRODUCT	B PUBLISHER	C #COPIES FOUND	D #COPIES PURCH	E = C-D SHORTFALL	F RETAIL PRICE	G = ExF VIOLATION

Upper management might be shocked to discover the extent of software theft in their own organization; even results of incomplete audits would likely be illuminating.

[B] SPAudit software

Finally, the SPA Self-Audit Kit came with a PC diskettes with auditing software. SPAudit was written by Softguard Systems and reproduced by The Software Factory as part of the SPA anti-theft project. It has a list of reserved filenames for over 650 known proprietary software products. It works simply by scanning all directories on each system for files with the reserved names. Users can print a report for each system; if the same diskette is used for several systems in turn, one can print a global summary at the end of the audit.

A Macintosh version is also available.

The documentation points out that because the product works with filenames only, it may fail by

- missing products whose files have been renamed;
- mis-identifying non-proprietary files as products because of coincidental choice of filename.

SPAudit users are asked to contribute information to the SPA about both classes of error.

As pointed out by the SPAudit pamphlet, this product cannot possibly prove that any given package has been stolen. It merely identifies which packages reside on a given system. It is then up to the people responsible for the audit to follow up with detailed verification of the legitimacy of the copies.

[A] Blowing the whistle

What would you do in the following situations?

- you observe someone in another department asking an employee for their password.
- your own manager asks you to enter dummy quality assurance approvals on your own work by using their user ID and password.
- your manager orders you to make an illegal copy of a software package despite your objections.
- you're invited to collude in a scheme to defraud a client by charging them for non-existent expenses or imaginary services.

What would people in your organization do? Do your corporate security policies cover these cases clearly? Are your employees trained to make the right decisions about ethical issues? Do your managers provide support for obeying the law in the face of direct and indirect pressure to bend the law?

This section looks at the many facets of a complex and difficult issue: fighting crime within an organization.

[B] Case study: General Dotan and General Electric

In the early 1980s, General Electric (GE) landed contracts for assemblies in the Minuteman missile. By the mid-80s, cost overruns were causing major problems for the corporation. A senior manager from headquarters in Fairfield, CT sent a blistering memo to the Philadelphia plant warning that people would be fired unless the overruns were contained. The terrified managers decided to invent a fraudulent research and development project to which they charged $800,000 of the Minuteman cost overruns. The Department of Defense paid the fraudulent charges.

In another case, corporate headquarters sent memos ordering plant managers to realize a 15% profit on a particular government contract; unfortunately, the contract limited profit to 8%. The managers met their profit quota illegally by billing the government over $21 million on parts of an Army computer system.

As a result of the 1985 prosecution based on the Philadelphia fraud, John F. Welch, Jr, the Chairman of GE, set out on a crusade to bring ethics back to his company. GE set up extensive

training programs, active ethics committees, and hotlines for reporting problems both internally and to external law enforcement authorities. The company entered an era of voluntary disclosure in which its own lawyers investigated suspected infractions and reported them to a special Pentagon investigative unit based in Philadelphia.

Regrettably, the Chairman's zeal for ethics was not matched by appropriate changes in the corporate culture at GE. Employees and ex-employees reported that throughout the 80s, GE continued to use systems of reward and punishment which pushed its executives toward the edge of legality. Bonuses and career advancement depended on short-term profits. Welch himself came in for criticism because his confrontational style led some managers to suppress anything that would disturb the corporate Party Line.

In 1987, Chester Walsh was moved to the Israeli offices of GE. He quickly discovered a systematic fraud involving GE employees and an Israeli air force general, Rami Dotan, to steal $30 million from the U.S. military assistance program to Israel. Walsh determined that the corruption extended up the corporate ladder to the highest levels of the engine division both in Israel and in the U.S. Fearing to blow the whistle internally while he was still in Israel.

In 1989, Walsh left Israel and moved to the Swiss offices of GE. He reported his suspicions to his replacement and to two colleagues. They informed headquarters and the Israeli office was examined by an engineer from the Evandale, OH engine plant. Almost immediately, Dotan demanded that GE suspend the enquiry. Because of Dotan's power to allocate $600 million of contracts, two top engine-group executives called off the investigation. These two executives were later accused of having colluded in the fraud and were fired by GE.

Meanwhile, Chester Walsh filed suit against GE under the False Claims Act, which allows individuals to sue federal contractors and protects whistleblowers against harassment. The Act also provides for a minimum 15% of whatever fines are collected by the government as a result of their prosecution.

GE's reaction was to put Walsh on administrative leave, threaten to fire him, and threaten to sue him for not having worked within the company to fight the fraud. According to some GE spokespersons, Walsh's four-year delay in launching the suit was a crass ploy to profit from penalties on an even greater dollar amount than would have accumulated if he had stopped the scam earlier.

Walsh is understandably bitter about his treatment, especially in light of the conviction of Rami Dotan in Israel. The ex-General was sentenced to 13 years in jail for fraud and also for conspiracy to commit murder. He had arranged to have an Israeli executive assassinated in New York. The executive had threatened to reveal Dotan's fraud.

[B] Analysis of the Dotan case

The story presented above is based on the gripping account of the events by Steven Pearlstein of the Washington Post. Pearlstein pointed out that GE's corporate culture contributed to several

instances of fraud. It looks as if the demands on lower-level managers for predetermined profits led to intolerable pressure. Pearlstein quotes Ed Zittlau, a prosecuting attorney in the 1985 fraud case: "The managers feared for their jobs.... [T]he mischarging looked like the lesser of two evils.'

My interpretation of the story is that Walsh realized that the corruption he encountered in the Israeli operations of GE's engine division went very high in the corporation. He feared for his job and possibly for his life if he revealed the fraud while in the power of the criminals. He therefore waited until he could escape to Switzerland before telling three other staff members of the problem. As a result of his intervention, GE began an investigation. As soon as Dotan and his collaborators in the U.S. found out about the internal investigation, they applied pressure to stop it.

GE's reaction to Walsh's civil suit (blaming him and threatening to sue him for damages) looks like denial. The contrast between the public posture and reality was so great that top management drew together to protect their Chairman's self-image. Pearlstein wrote perceptively, "For Welch, who has been lionized by the business press and held up as a model by business schools nationwide for his success in transforming GE's stodgy bureaucracy into a fierce global competitor, such problems represent a huge professional embarrassment.'

[B] Doing the right thing vs minding your own business

Why should anyone report breaches of security, ethics, or the law? People have many motives for reporting crimes; few of the motives are mutually exclusive.

One motive is to protect corporate interests. Reporting irregularities can stop the immediate loss and prevent further damage. The damage can include more than material threats: stopping a crime can prevent damage to client interests and client relations. Stepping in to stop a fraud can help prevent a public relations disaster. And it can prevent financial or operational catastrophes.

Stopping a crime can protect you in your career; being convicted as an accessory to a crime is not great recommendation for future employment. If enraged stakeholders sue managers for dereliction of duty, it would be nice to be one of the good guys; if the government prosecutes in criminal court, it would be much more fun being a witness for the prosecution than for the defence. And even if there never is any personal danger, personal integrity and standing by your principles lets you look yourself in the eye without cringing.

People also report crimes for other, somewhat less savory reasons: social approbation, fame, and interest in financial rewards. Some may even feel the glow of self-righteous glee as their colleagues march off to jail. Perhaps a few decide to report only people they dislike.

On the other hand, there are many reasons why people might not report a crime. People may fear social disapproval of breaking explicit or implicit group bonding (perhaps based in memories of school yard taunts, fraternity oaths, military solidarity, and grade-B crime movies with tight-lipped gangsters sneering at stool-pigeons). The social disapproval may extend to blacklisting the

whistle-blower both within the organization and perhaps even in the field. In the television-ridden, recessionary atmosphere of late twentieth-century America, there may even be a legitimate fear of physical attack.

Another reason for doubts about reporting crimes is anomie. People sometimes just don't care. They don't care about their employer, they don't care about their colleagues, they may not even care about themselves. Under these circumstances, fishy dealings will continue until external forces respond.

In my opinion, it is highly appropriate for management to make whistle-blowing part of the official escalation path for reporting dangerous or illegal behaviour. An organization that makes sure everyone knows they are subject to reporting for illegality demonstrates its commitment to the highest standards of business ethics.

CHAPTER NOTES

1. Parker, D. B. (1983). *Fighting Computer Crime*. Scribner's (New York). Reprinted as □Computer crime methods□ in *Datapro Reports on Information Security* report #IS09-200-101.

2 Van Duyn, J. (1985). *The Human Factor in Computer Crime*. Petrocelli Books (Princeton, NJ). ISBN 0-89433-256-2.

3 Kabay, M. E. (1990). Security policy: personnel hiring and training. *INTERACT* 10(6):78).

4 Sherizen, S. (1986). The role of management in computer security. *Datapro Reports on Information Security* report #IS09-300-101. Dr Sherizen discusses in detail the personnel-related issues and parallels between traditional business controls and information systems controls.

5 Gilman, J. B. (1990). When an employee leaves, make sure his knowledge stays. *Systems Integration* 23(12):15

6 Anonymous (1990). Apple tightens security screws. *MacWEEK* 4(7):74

7 SOFTWARE PUBLISHERS' ASSOCIATION / 1101 Connecticut Avnue N.W., Suite 901 Washington, DC 20036. Tel: 202-452-1600 / Fax: 202-223-8756 / Hotline 1-800-388-PIR8

8 Pearlstein, S. (1992). Israeli military aid scandal jolts GE; company to settle fraud charges, defends ethics program. *Washington Post Newswire* (July 20,1992).

Chapter 5: Physical security

M. E. Kabay, PhD, CISSP < mkabay@norwich.edu >

Associate Professor of Information Assurance
Dept of Computer Information Systems
Norwich University, Northfield, VT

1 Objectives:

After studying this chapter, the reader should be able to

1. evaluate the physical security of existing or planned computer facilities.

2. identify and correct building construction and design flaws which impair information security.

3. evaluate the security implications of information systems support equipment.

4. judge and improve the suitability of physical access control systems.

2 Building location and design

If you're planning to build a new computer center or relocate your existing equipment to an existing building, you have an opportunity to make your building work for you instead of against you. By picking the right combination of location, structure and layout, you can decrease your vulnerability while increasing the usability and maintainability of your equipment.

2.1 Natural risks

If you're starting from basics, you can consider the geographical location of your new site. Study long-term weather patterns, including frequency of heavy winds (e.g., tornadoes, hurricanes, and monsoons), snow, and lightning. Unless you're devoted to a life of great excitement, the likelihood of earthquakes should play a role when siting a major data center.

2.2 Neighborhood risks

If it weren't for personal experience, I'd be embarrassed to remind you not to situate your data center in a dangerous place. Sounds like motherhood-and-apple-pie. But consider the following:

One fine spring day, as I drove to a data center where I was due to start a security audit, I noticed a field of enormous storage tanks on my left. It looked like a science fiction movie: row upon row of spheres and cylinders holding millions of liters of gasoline, diesel fuel and home heating oil. I was startled to find, upon following my directions, that the data center was directly across the road, no more than 200 meters away.

As I parked my car, I noticed a freight rail road crossing diagonally immediately behind the building. The tracks were still bright, so the railway was still in active use.

Copyright © 1996, 2000 M. E. Kabay. *All rights reserved.*

Finally, just as I was about to enter the building, I heard a passenger jet screaming across the sky just above, flaps out, heading for a landing at the regional airport.

Now that was a poorly situated data center.

Before choosing the building which will hold your corporate offices or data center, examine the neighborhood. Avoid

- flight paths for the local airport
- nearby chemical or explosives plants
- neighboring elevated highways
- railway freight lines.

Look out for

- mine shafts
- toxic waste dumps
- sources of dust and smoke (e.g., industrial incinerators)
- new or planned building activity (the vibration of pile drivers will harm your systems).

How easy would it be to reach the site in an emergency?

- is there redundant road access?
- are there several sources of help to fight fires?
- is there police support and emergency rescue within easy reach?

Examine the socio-economic profile of the proposed location.

- Are there poor areas around the site?
- What's the crime rate?
- Is it improving or declining?

A participant in the January 1993 session (New York City) of the NCSA's Information Systems Security course reported that their corporation decided to move their headquarters one day after the new CEO took over.

He had been shot at in the parking lot on his first day at work.

Whatever you decide, be sure to re-evaluate your physical location periodically. Maybe you can avoid being shot.

Copyright © 1996, 2000 M. E. Kabay. *All rights reserved.*

2.3 Building construction and design

In the March 1993 session (Atlanta, GA) of the Information Systems Security course, a participant reported that a major company installed millions of dollars of computer equipment, electrical power conditioners and air conditioners on the 11th floor of an office tower. One Monday morning, the staff arrived to discover no 11th floor--and no 10th floor--and no 9th floor. The company had neglected to consult a structural engineer before loading the building with all that equipment. Luckily, no one was hurt in the collapse; however, damages ran over $100 million.

2.4 Location within building

Access to the computer center should allow easy installation of equipment yet protect that equipment and its operators against physical assault. The ground floor seems too easy to attack; underground is susceptible to flooding. In the movie Die Hard, we see a Hollywood conception of a computer center: at the top of an office tower and entirely surrounded by glass. Since some computer equipment (or support equipment such as large-scale air-conditioning units) is larger than freight elevators can handle, the units have to be lifted into place using building cranes. The higher the computer center, the more expensive the crane. In case of fire, there may be a longer lead time for your staff to shut off the equipment and make their way to safety than if they're high up in a sky-scraper.

The second floor seems like a good compromise.

Place the computer room far from hazardous areas. One story circulating in the security field tells of a security auditor in the U.K. who wondered about the vibrations he felt in his feet every now and then. “Oh that?” responded the data center manager, “That's just the lorries with the petrol.” The computer room was directly over the passageway through which trucks carrying fuel oil regularly rumbled.

High security vaults are required by law to have no external walls. That is, they are completely inside their building with corridors completely surrounding them. This design makes it much more difficult to punch holes into the data center without having anyone notice. And in case you doubt that a frontal assault on a computer center is likely, some automatic teller machines have been removed holus-bolus by thieves operating back-hoes and forklifts (it does make one wonder about why no one thought it odd to see a forklift trundling along with an ATM in the middle of the night). When I was teaching in Africa in the 1970s, I recall thieves simply ramming their way into houses with trucks or cutting through the roof to enter secured buildings. And as I was editing this chapter in the Spring of 1995, one of the participants in an online Computer Crime and Countermeasures Course told us about how a series of smash-and-grab attacks had been made on a local company known to have installed large numbers of new workstations. The criminals simply crashed through the wall and made off with the equipment in the minutes before the police could respond to building alarms. Maddeningly, the criminals apparently watched and waited until the victims had replaced all the equipment--and did it again! They were dissuaded from further repetitions by having a 24-hour mounted on the site.

Make that perimeter tight and strong.

Copyright © 1996, 2000 M. E. Kabay. *All rights reserved.*

Once you've built the computer room, be sure the local fire department knows exactly where it is. Keep your plans, including layout, up to date and coordinate with the fire marshals in your municipality.

However, there is no reason to mark the computer room with special neon flashers that read, "THIS WAY TO MILLIONS OF DOLLARS OF VULNERABLE EQUIPMENT." When I visited the headquarters of EDS Inc. in Dallas, I was much struck by the anonymity of the equipment rooms. We'd be walking through endless corridors with identical, boring metal doors, each marked with a numbering scheme. They all looked as if they could be broom closets. Then we'd open one up and find vast gleaming, sterile chambers of white tiles with silent titans standing in rows with unblinking red and green eyes.

Anyone who needed to know where the computers were knew where they were; why help anyone else?

2.5 Layout

Within your data center, try to put separate functions in different compartments. For example, keep printers away from consoles, disk drives and processors (the paper is a fire hazard and the paper dust gets into your air filters). Put tape vaults and data safes far away from the disk drives (although you can have a local fire-proof safe or vault for the convenience of operators if the tapes stored there are not your latest backups). Put your access control equipment into a separate, high-security area, not with the rest of the computers. Keep your phone switches away from the computer room so that a single attack cannot put your entire operation into jeopardy.

The lower the traffic through a secure perimeter, the higher the security. Accordingly, try to keep your personnel inside the secure areas surrounding your equipment; for example, include rest rooms, eating areas and office space within a tightly-controlled space.

2.6 Walls

When you build an enclosure for expensive and critical equipment, be sure they're substantial walls, not mere partitions. Reinforced concrete that runs from slab to slab is best. Allow no crawl spaces around the wall above a drop ceiling or below a raised floor.

Check your plans and forbid any closets in the walls; they are weak spots and also provide concealment should anyone decide to burrow through the wall.

Finally, if you're really paranoid, discuss the design of the outermost walls of your building. Avoid chases (decorative indentations on the side) and other features such as rusticated stone that could allow assailants to use mountain-climbing techniques to climb your building.

2.7 Doors

Have as few doors as possible. You must know and obey all the safety regulations which mandate the number of exits you must include for protection of human life. Your architect will know what the law requires. However, only one door should be used for entry. All the others should be used as emergency exits only. All doors should be equipped with crash bars and alarms and decorated

Copyright © 1996, 2000 M. E. Kabay. *All rights reserved.*

accordingly. You can even buy signs that read, "DOOR IS ALARMED," which always makes me want to pat the door and reassure it.

Choose heat-resistant doors (solid metal or thick metal with structurally-sound core) and avoid any glass if at all possible. If safety regulations require glass panels to prevent smashed noses, insist on multiply-laminated bullet-proof, shatterproof small panels. Glass is a weak point anywhere in the secured area.

Installing a door that would make your local bank proud will be pointless if the frame is so weak that it--and the door--can be pried out of the wall with a crowbar. Door frames should be anchored solidly in the wall; if possible, bonded to the structural members of the wall. Door hinges should be on the inside of the secure area so they can't be dismantled. Choose hinge pins that are welded into place--not the ones that can be unscrewed and removed by anyone with a home tool kit.

Protect door locks with astragals (a lovely word meaning the edge-plates that prevent nasty folk from inserting credit cards, screwdrivers and chisels into the latch and forcing the door open). I have seen many sites which use astragals which extend from top to bottom of the door to provide maximum protection.

Don't use motion or simple proximity sensors to unlock or open doors into secure areas. Sliding doors controlled by such sensors--like those used in many public buildings--can be opened from the outside simply by pushing a sheet of paper through the rubber gaskets and waving it about.

2.8 Windows

Don't put windows in your data centers. I've already pointed out that there should be no outer walls in your computer room, let alone windows. Windows are physically weak; their frames are weak; and they let too many people see how you've laid our your equipment--including your security equipment.

I recall one manufacturing site where I stopped next to the floor-to-ceiling windows around the computer console room and stared at the 5 meter banner on the wall. It had huge numbers printed on it. I asked, "That's not the main modem number, is it?" Yup. So much for dial-in security.

Unfortunately, many executives who worked with computers in the 1960s and 1970s still think that "vision panels" make their data center look more impressive. If you are faced with this retrograde attitude, try a graduated approach to getting rid of these vulnerable spots in your defenses. Offer the decision makers a choice between, say, concrete, brick or bullet-proof safety glass. Alternatively, you can strap the executives down and force them to watch endless loops of Bruce Willis surviving the destruction of the Glass House in the movie Die Hard.

If you cannot get approval to remove the windows in your computer room, install vertical blinds and keep them closed all the time except when there are important official visitors pressing their noses to the glass. Install security glazing (shatterproof metal-reinforced glass), and perhaps gratings securely attached to the walls. Install breakage sensors and connect them to the main building alarm systems. Aim motion sensors and closed-circuit television cameras at the windows. Move equipment whose presence should be secret away from the windows. Install a few dummy security cameras and motion sensors just to keep spies and intruders guessing.

Copyright © 1996, 2000 M. E. Kabay. *All rights reserved.*

2.9 Ceilings and floors

Practically all offices have drop ceilings; i.e., acoustic tiles are suspended from the actual ceiling. This design provides for a place where electrical and communications wiring can be laid out of sight. This crawl space must not extend without interruption into the data center. Within the data center, the drop ceiling should include smoke, heat and water sensors.

Most data centers have raised floors because of all the cabling and power cords required for processing equipment and peripherals. The floor tiles are laid on a framework about 18 inches (~50 cm) off the actual floor. These tiles must be fire-resistant, easy to keep clean, and strong enough for the loads that will be placed on them. For access to the underfloor area, the tiles are raised using suction cups. Perforated tiles are part of the air-conditioning and fire-suppression systems and are raised using hooks.

The underfloor area must be kept scrupulously clean. Halon and other gas-based fire-suppression systems discharge high-pressure gas through the underfloor. If that area is dusty, the entire computer room will be filled with a cloud of dirt when the gas discharges.

In some cases, operators have used the underfloor as a storage area, usually for things that don't belong in the computer room at all (e.g., soda pop). Such foreign objects interfere with the air-conditioning system and cause access problems in emergencies.

3 Computer center equipment

In recent years, computer equipment has become increasingly tolerant of environmental conditions. Midrange and many mainframe computers are now air-cooled, survive temperatures from cold to hot, and run on regular 110V current. Nevertheless, some people abuse their systems. I mentioned in Chapter 2 that while I was hanging my coat in a hall closet one day on a visit to a client, I noticed blinking green and red lights down among the boots and galoshes. I moved some heavy winter coats out of the way and discovered a network server. Startled, I asked my host what it was doing in an unprotected hall closet. It seems that they ran out of room in the computer center and the server was installed in the hallway. “It doesn't need special conditions,” he chirped. No, but its on/off switch was open to anyone who wanted to try bringing the network down.

In many smaller organizations, I have noted with dismay that electrical power cord extensions are looped helter-skelter around the bottoms of desks and partitions. If someone trips over these cords, they can not only unplug somebody's computer, they can hurt themselves too.

Sometimes people plug their computer systems into a power bar in their neighbor's cubicle without informing anyone. When the neighbor innocently cuts the power on their own system by hitting the main switch on the power bar, the electricity-borrower has a power failure too.

3.1 Electrical power supply

According to recent research by field service organizations, almost half of all service calls on PCs are related to bad electrical power. Power fluctuations such as brownouts (transient low voltage), spikes (transient over?voltage) and line noise (waveform deformations) can physically damage sensitive electronic equipment. Even surges on phone lines can damage modems and PC boards.

Copyright © 1996, 2000 M. E. Kabay. *All rights reserved.*

Power outages cause down time, but the more serious threat is that power interruptions during a critical phase of posting data to disk will cause data corruption. If a disk drive goes down while data are being written into a file, one or more records can be damaged. Parity checks or cyclic redundancy codes on the disks can usually pick up and sometimes correct errors. However, if the computer is updating a directory structure when the power disappears, there can be serious trouble. Directory structures include database or file indexes and system directories such as the DOS File Allocation Table (FAT). Damaging even a small part of these structures may make large amounts of data inaccessible. Recovery of data may require painstaking retrieval of section (cluster, sector) after section of individual files.

Midrange and mainframe computers have long had their own internal electrical-power conditioners and uninterruptable power supplies (UPSs) or standby power supplies (SPSs). Less powerful, less expensive systems did not. However, users have placed critical applications on servers, work stations and microcomputers; alternative power supplies and line conditioners are now required components for most production systems.

UPSs run the mains power into a transformer which keeps batteries charged; output power comes from direct current (DC) rectifiers which convert the battery power into alternating current (AC). UPSs provide excellent-quality power and good insulation from power-line fluctuations.

SPSs switch from the mains to battery power within a few milliseconds; they are adequate for PCs and servers, which usually come equipped with capacitors that allow at least 15 milliseconds power interruption without harm to the system.

For PCs, work stations and servers, SPS or UPS units in the 0.4-1.2 KVA (kilovolt-ampere) range are sufficient. In 1993, SPSs ranged in cost from about $200 to over $1,000. UPSs are about 1.5 to 2 times more expensive for the same power load. Keep in mind that you have to plan for peak loads, not just the average power drain. Laser printers, for example, can run at 700 watts while warming up yet function on standby at a mere 100 watts. Older, physically larger disk drives take much more power while spinning up than while running normally. However, modern tiny, ultra-dense drives (e.g., 20 Mb on a 1.5" spindle) require so little power anyway that they're no longer an issue.

Speaking of printers, many people will deliberately exclude their printers from the calculations for their proposed SPS or UPS. They can live without the printer when it loses power. At worst, they may have a single damaged page to reprint.

The size of the batteries and the drain by your systems determine how long the SPS or UPS can keep your system going. At a minimum, you need time for a graceful shutdown; 5 minutes is ample to allow you and your users to exit from application systems and shut down all peripherals and processors. If there is a reason to continue operating your system during a power failure (e.g., to protect the security computer that controls your physical access control systems), you may have to order extra batteries (for hours of operation) or a generator (for continuous operation as long as the fuel lasts).

For larger, more critical applications, you should evaluate large-scale UPSs which can be hooked into your office or building electrical system. Systems for loads ranging into the hundreds of KVA can cost from $2,000 up into the $100,000 range. Some units include gasoline or diesel generators and heavy-duty flywheels or large isolation transformers to smooth out the rough waveform of the

Copyright © 1996, 2000 M. E. Kabay. *All rights reserved.*

generators' output. Never run electronic equipment directly from generators without checking the power quality carefully. Ordinary household generators of the kind sold in hardware stores for your country cabin can destroy your computer equipment within seconds.

In a related issue, common sense (as well as workplace safety regulations) dictates that you install adequate emergency lighting for all work areas and escape routes. After the bombs exploded in the World Trade Center in New York in February 1993, thousands of people had to feel their way through smoke-filled, pitch-black stairwells. It seems the emergency lighting system was controlled by computers that had been blown up by the explosion in the parking garage. Independent lights with their own batteries would have saved time and reduced injury in that disaster. Portable flashlights supplied to emergency marshals would have helped, too.

Now that you've spent all this money on electrical power equipment, how about protecting it all from tampering? Keep all electrical junction boxes, breaker panels and main switches under lock and key. If you have to install additional power cables, ensure that they're pulled through protective ducts or manifolds, not left lying about in the suspended ceilings where anyone can get at them. And document all the switches and breakers correctly and readably so that people can make intelligent decisions in an emergency.

Label SPS and UPS plainly with warning signs to prevent unauthorized equipment from being added to the circuits. In one of the May 1993 Information Systems Security courses (Toronto, ON), a participant reported that an operator plugged a vacuum cleaner into the nearest electrical outlet and took down the LAN for a few minutes. That nearest outlet happened to be in the server's UPS.

Be sure that there are at least two "panic buttons" in your computer room: one at each end and both near exits. The panic button cuts off all power to everything in the computer room except the lights. These switches should be protected against accidental use; for example, you can choose switches covered with a spring-loaded flip-top cover or models with the button at the bottom of a one-inch finger-sized tube. Install a phone within reach of each panic button for rapid communications in an emergency. Put a long extension cord on the handset of that phone or provide a cordless phone for use only in an emergency (cordless phones are not secure and should not normally be used for business communications).

In my own apartment building, a visitor had trouble opening the electrically-operated door and therefore pulled the nearest handy lever--the fire alarm. To prevent this sort of error, label the panic switches clearly; e.g., "MASTER POWER CUTOFF."

Keep fuses handy in all the right sizes for all your electrical gear, including the power supplies.

Every time you order modifications to the electrical system or find out that your building is having such modifications, be sure to check that the grounding is correct. Especially when your midrange or mainframe systems use three-phase power, it's crucial that the correct wires carry the ground. While you're at it, verify that your building is properly grounded in case of lightning strikes. This precaution is especially important throughout the great plains of North America.

If someone were in the process of being electrocuted in your computer room, what would you use to move them off the live wires? You're supposed to use a non-conductor such as wood or plastic. Some data centers have a wooden cane for this purpose hung on the wall along with fire

Copyright © 1996, 2000 M. E. Kabay. *All rights reserved.*

extinguishers and other emergency equipment. Don't forget to train your staff, though, or the cane will simply sit on the wall while several people electrocute each other in turn.

If you want to shut off your computer equipment remotely or start it up remotely, you can install inexpensive switches to do both. There are switches with serial ports that allow a computer (e.g., the batch file that handles your backup procedures) to send a signal which will power down all systems on the switch. Thus your system could shut itself off at the end of its nighttime processing. Contrariwise, there are switches that sit on the phone line; when they sense a modem or FAX signal, they can turn on the power to whatever equipment you connect to them. For those people who insist on powering off their equipment overnight, some switches can even be programmed with a timer so that your system can be up and running in the morning when you arrive at work. If your AUTOEXEC.BAT file (or equivalent on other systems) is properly programmed, you could have your electronic mail ready as you arrive with your morning coffee.

Do it right and you could have the morning coffee ready, too.

3.2 Air conditioning

Concentrations of computer system equipment (host processors, LAN servers, disk drives, system printers, tape backups, multiplexors, and so on) can use so much energy that regular office air-conditioning (A/C) fails to dissipate the heat. Ideally, temperatures in your computer center should be 66-73 F (19-23 C). Midrange and mainframe systems still produce so much heat that A/C failure can rapidly lead to high temperatures.

Each component of your computer system usually has its own temperature sensor that can cut off power at the upper end of the temperature range. In addition, computer rooms have their own global thermostats and cutoff switches.

In the data center where I worked in the mid-1980s, an A/C unit failed one day. A new operator noticed the rising temperature but didn't realize the cause. He looked about for the room thermostat and noticed a temperature dial in the ceiling. It was set at 90 F (32 C). He turned it down to 70 F (21 C) and immediately lost power all over the computer room. He had changed the overtemp power cutoff.

That day, we labeled every single dial and switch in the computer room.

Relative humidity should be maintained from about 45 to 55% to prevent static electricity buildup (if too dry) and condensation or curling paper (if too humid).

Air pressure in the computer center should be slightly higher than in surrounding office areas so that air tends to flow out of the equipment area when doors open (positive pressure helps keep smoke and dust away from the electronics).

The computer room A/C should be separate from that for the rest of the building. You need to be able to control ambient conditions yourself under normal circumstances. You want to keep smoke and dust out of your computer center in an emergency.

Protect the external air intakes to reduce the risk of a gas attack or tampering with you're a/C. Make sure that the ductwork is non-combustible and that it does not provide a crawlspace for

Copyright © 1996, 2000 M. E. Kabay. *All rights reserved.*

unauthorized access to your computer room. Sometimes it seems that every movie involving penetration of a secured area includes an obligatory scene in which heros or villains crawl undetected through the A/C ducts.

Link you're a/C units to the fire-suppression control systems. The panic button that cuts power to your computer equipment should include the A/C equipment. In case of a fire, the last thing you need is the A/C continuing to pump fresh air into an enclosed area at risk.

The perforated tiles in your raised floor are part of the A/C system and fire-suppression systems. A/C engineers lay these tiles in patterns that control air flow within the computer room. These tiles must not be displaced at random. In some data centers, operators move the tiles about without considering the effects on air flow; in one case reported in the Information Systems Security course, operators decided they didn't like the tiles, so they moved them all over to the far corner of the computer room. This spontaneous redesign of the A/C system produced Arctic conditions in one area and tropical temperatures in the other. The operators were on their way to generating a model of the global atmospheric wind patterns.

As discussed below in the section on fire suppression, chlorofluorocarbons (CFCs) such as Halons have been banned in the U.S.. McLachlan (1992) has pointed out that, in consequence, some A/C equipment may have to be replaced instead of repaired. Data center managers will have to budget for increased A/C expenses over this phase-out of CFCs.

3.3 Electromagnetic fields

Computers, like gods, are omnipresent. Therefore anything that interferes with computers can cause problems in applications ranging from the homely to the extreme. For example, two workers in Japan were crushed by a drilling machine when radio waves interfered with its computer-based controller. A drilling rig in the North Sea went for a random walk looking for a positioning signal when a portable radio transceiver disrupted its satellite link. Telephone switches, which are really specialized computers, have failed during electrical storms, when electromagnetic interference can be severe.

Electromagnetic interference (EMI) and radio frequency interference (RFI) are terms applied to any disruption caused by electromagnetic waves. RFI usually applies to disturbances of radio and television, whereas EMI is a broader term that includes RFI.

Newly-installed IBM 4381 mainframe computers at the London Air Traffic Control Center at West Drayton, near Heathrow Airport, have been severely affected by RFI. In May 1993, several U.S. airlines announced a complete ban on using electronic equipment (including portable computers and video games) in airplanes at any time. I personally spoke with a pilot who had a horrifying experience when a portable computer being used in the first-class compartment interfered with his plane's avionics so severely that he had trouble landing safely.

Electromagnetic fields are generated by the flow of electrons through conductors. Any time electricity flows through a wire, it induces a corresponding magnetic field. Any time a magnetic field moves through conductors, it induces a current.

Copyright © 1996, 2000 M. E. Kabay. *All rights reserved.*

The earth generates an enormous magnetic field and is surrounded by clouds of moving charged particles. Together, these factors determine the earth's magnetosphere. Our sun spits out torrents of fast-moving charged particles (the solar wind) which interact with the magnetosphere. The polar lights (aurora borealis and aurora australis) are the result of the collisions between the solar wind and the magnetosphere.

As you can imagine, with all these fields and currents, the planet is sizzling with natural EMI and RFI. Sometimes, especially when the 11-year solar sunspot cycle is at its maximum, natural EMI disrupts radio communications worldwide. Sunspots are cooler areas of the sun's outer photosphere; they are often many times larger than the earth's diameter. Sunspots are associated with intense magnetic fields. Sometimes sunspots throw out such enormous electromagnetic pulses that our planet's electrical-distribution grids act as antennae and generate huge waves of high voltage. One such incident caused a cascade of tripping circuit breakers in the Province of Quebec and turned the lights off in Quebec and several New England states.

However, natural sources of EMI are not the worst threat our electronic equipment faces. Almost all modern consumer electronics broadcast EMI. The exceptions are devices made to tough U.S. government TEMPEST standards. TEMPEST stands for Transient ElectroMagnetic Pulse Emanations STandard and is designed to prevent eavesdropping. TEMPEST designs include thorough shielding and cladding using metal (EMI cannot propagate through such layers).

Cellular telephones, walkie?talkies, FAX machines, computers and video-film players and recorders all produce RFI. Processors using fast clocks and high-density integrated circuits (e.g., 80486 chips running at 66 MHz) produce the most disruptive high-energy RFI. Not only do these fast-running, powerful chips generate noise; they also show the greatest sensitivity to neighboring devices' noise. The new processors use subtle differences between the 0 and the 1 state; they also have tiny connectors which can serve as antennae for precisely the high-frequency, short-wavelength RFI which they themselves emit.

It isn't easy to protect electronic equipment against EMI. For example, the US Army spent $175M protecting Black Hawk helicopters from EMI. Organizations have been forced to spend enormous sums replacing old unshielded wiring and replacing it with shielded cables. When the Civil Aviation Authority (CAA) in the U.K. realized that the flickering on their video display terminals was due to RFI, they surrounded them with Faraday cages (shielding). Unfortunately, the flickering got worse. According to Tony Collins, writing in 1990, CAA engineers found that the Faraday cages acted as antennae, amplifying the RFI instead of excluding it.

Standards bodies are still debating the details of appropriate levels of required attenuation. At some point, we should see new requirements for manufacturers to protect their equipment against RFI and also to prevent their products from broadcasting these pesky signals.

In your own environment, there are some simple principles to help avoid problems from RFI:

o do not allow magnets such as degaussers to be brought near your processors, disk devices, and tape units.

Copyright © 1996, 2000 M. E. Kabay. *All rights reserved.*

o have your main supplier (or a specialized consulting firm) measure RFI everywhere you have computer equipment in your facility and ascertain that you are within tolerances for both incident radiation and radiation emitted from your equipment.

o do not permit the use of cellular telephones and walkie-talkies within your computer room.

o be especially careful to monitor EMI if you see microwave or radio transmitters near your building. Ask to be informed if a nearby broadcasting station increases its power.

3.4 Fire

Fire is the chief physical threat to your information systems.

3.4.1 Prevention

As mentioned in the section on air conditioning, you should keep your data center separate from the rest of the building if possible. Ideally, you should have your own data center electrical and alarm systems as well. Check your walls to be sure they are non-combustible. Restrict the number of openings in your walls, including spaces for electrical wiring, air ducts and water pipes. All ductwork and conduits should be cemented into the walls with fire-resistant materials and should be as airtight as possible. Doors, the largest holes in your walls, should be equipped with self-closing fire exclosures (insulated, metal-sheathed doors that roll shut to delay smoke and fire as long as possible).

Floors should be fire-proof; keep suction cups for emergencies in a fixed place in your computer room and don't allow them to be taken for daily use. Make sure your underfloor areas are clean and not used for storage.

Keep combustibles out of the computer room. Don't store paper or solvents near your equipment. Keep backup tapes away from the processors and disk drives they're backing up.

3.4.2 Detection

Be sure your fire detection systems are approved by the local fire authorities before installing them. Select detection systems which integrate information from multiple sensors rather than setting off alarms if a single sensor malfunctions. Place heat and smoke detectors in several places in your data center, including above the hanging ceiling and below the raised floor. Your goal is to provide precious extra minutes to your staff and the fire-fighting team in case of an emergency.

Mark the positions of all fire, smoke, heat, and water detectors so they can be found easily when you check the alarm system.

3.4.3 Suppression

Until recently, Halon 1301 has been the method of choice for suppressing fires in computer rooms. The heavy chlorofluorinated hydrocarbon is non-combustible and displaces oxygen, thus snuffing out fires immediately. Unlike carbon dioxide, it does not kill people in the concentrations required for fire suppression.

Copyright © 1996, 2000 M. E. Kabay. *All rights reserved.*

Unfortunately, Halon, like other chlorofluorocarbons (CFCs), destroys ozone and thus contributes to the depletion of the ultraviolet-blocking atmospheric ozone layer. In 1987, the U.S. and Canada signed the Montreal Protocol which mandates the elimination of CFCs by the year 2000. In 1991, the U.S. Environmental Protection Agency set an earlier date of January 1, 1995 for this phase-out, which is now well under way. Many organizations have been tearing out their existing Halon-based systems and replacing them with new gas-based or water-based fire suppression systems. There is now a thriving new industry devoted entirely to collecting, recycling and disposing of Halons and other CFCs.

The National Fire Protection Association standard NFPA-2001 provides for eight alternative gases to replace the Halons. The current DuPont candidate to replace Halon 1301, which was the gas of choice for fire suppression, is FE-13. Unfortunately, this gas requires larger storage tanks and thus leads to expensive retro-fitting. North American Fire Guardian (Vancouver, BC) makes NAF S-III which is claimed by the maker to be a perfect replacement for Halon 1301 and requires only a change of nozzles.

Until more effective substitutes are found, fire suppression will depend on water sprinklers and on carbon-dioxide, chemical foam, and chemical powder extinguishers.

The best system for controlling water above your computer equipment is dry-pipe sprinklers. Their pipes have valves outside the walls of the protected area; when the fire-detection system triggers the sprinklers, water enters the pipes but the sprinklers don't release the water until heat trips the triggers. Newer sprinklers release a fine mist that uses only 10% as much water as conventional models. In-cabinet and under-floor carbon dioxide systems help suppress fire at the source.

3.5 Water

Data center managers used to view sprinkler systems with horror, but today's electronic equipment is far less sensitive to water than older technology. A participant in the April 1993 session of the Information Systems Security course reported that a plumber cut the wrong pipe one day and flooded the computer room with three feet of water. The staff did not even have time to hit the panic button and so all the power stayed on. The staff spent three days with fans and hair dryers working on the sodden equipment to dry it out. Everything worked except one tape drive.

Despite this heartening story, mixing water with live electrical circuits is not a good idea for either equipment or people. As mentioned above, be sure there are panic buttons easily accessible in case of emergency.

Install water detectors in the ceiling areas under areas that appear to be likely conduits for water leaking from the storey above your equipment or from plumbing in the ceiling space. Examine the concrete ceiling carefully for tell-tale areas of mineral encrustation and check the acoustic tiles in the suspended ceiling for stains of any kind. I have seen concrete buildings in which low-level leaks have gone on for so long that there are actually tiny stalactites hanging down from the ceiling. Some data center managers have noted condensation from uninsulated pipes carrying cold water through the space above their million-dollar investments; insulate the pipes. In all such cases, see if the problem can be fixed; if not, you may have to invest in the equivalent of eaves-troughs to guide stray water droplets away to drainage pipes. All such potential leakage areas should be equipped with water detectors that are linked into your center and building alarm systems.

Copyright © 1996, 2000 M. E. Kabay. *All rights reserved.*

If a major leak or accidental discharge of sprinklers should occur, you want to protect the equipment against the spatter of water. On a visit to the New York Stock Exchange, I was pleased to see fire-resistant plastic sheeting stored at the sides of the huge computer room; staff are trained to draw the sheeting over the equipment in case of a water or fire emergency.

Water has to go somewhere if it does enter your computer room. Ensure that the under-floor has adequate drainage. Place water detectors in strategic spots under the raised floor. The electrical cables supplying your equipment are waterproof; it's the connectors that cause problems in water. To give yourself the maximum time before rising water shorts out your electrical connections, place junction boxes a couple of inches off the ground by putting them on raised cable trays--or, in a pinch, on top of bricks.

4 Physical access controls

To reduce the risks of sabotage, theft, and spying, you have to prevent unauthorized access to your computer equipment. Normally, there should be a single controlled and monitored access point in your security perimeter. Your physical access controls should be flexible to meet changing needs. There should be an audit trail which records all traffic into and out of the restricted areas.

4.1 Policies

Access controls may seem like a nuisance to employees and others who are inconvenienced by security requirements. It's important to present these controls and other security precautions in a positive light. In your policy development and security training programs, emphasize that such measures protect employees against the disruption, loss of business and even loss of employment that could result from sabotage or from accidental damage caused by untrained employees or visitors. Audit trails protect the innocent by excluding them from suspicion.

All employees must be trained to wear an identifying badge and to challenge anyone not wearing an appropriate badge. In some centers, I have been amused to see guards assigning badges to visitors when no one else wears any. If all that's required to be part of the crowd is to remove your badge, there will be no effective identification of intruders. In larger workplaces, badges are color-coded to indicate to which areas they give authorized access; e.g., a blue badge might restrict its wearer to the factory floor and administrative areas; a red badge might be required for access to the network control center.

Ideally, badges should include a clear picture. If possible, include the access cards used for electronic security systems as part of the badge. Badges can be equipped with clips (most useful for people wearing jackets or shirts with pockets or buttons) or hung on light chains or cords and worn around the neck. With time and proper enforcement, putting on your ID card becomes as natural as putting on the your clothes before going to work. Some people may find themselves putting their badge on weekends if they're not careful.

In high-security areas, all visitors must be accompanied by authorized staff at all times. In my local bank, for example, a visitor who needs to use a toilet is accompanied to the basement; the bank employee is required to wait until the visitor comes out of the lavatory.

Copyright © 1996, 2000 M. E. Kabay. *All rights reserved.*

It takes training to convince most people to stop unaccompanied visitors or people who are not wearing the right badges in a restricted area. We are brought up to be polite to strangers or to ignore them (depending on whether you come from an area with low population density or from a big city). Train your staff to approach the visitor or unknown, unbadged person politely and to enquire, AMay I help you?' Usually, there will be no problem guiding a visitor to the proper area. An unbadged employee may make a fuss if the security policies are unclear or poorly enforced. A criminal may try to bluff his or her way out of the situation. If there is the slightest doubt about their safety in approaching a potential intruder, employees should call the security guards at once for help.

It is critically important to apply security policies even-handedly. Any allowance or exception casts doubt on the integrity of the rest of the staff who must obey these irritating rules. It is especially dangerous to give the impression that immunity to security policies is a perquisite of power. For example, the CEO does not need and should not have access to the network control center; a manager does not need unsupervised access to her employees' locked desks. Any deviation from this principle results in a scramble for the invisible badges of authority as people try to show how important or powerful they are by flouting security rules that apply to ordinary people.

When you train your staff to apply security rules, be prepared to back them up if they get into a conflict with other employees. In my data center, we trained a young operator as usual to restrict access to the computer room to authorized personnel. One weekend, the CEO appeared unannounced to show an out-of-town visitor the computer room. The operator politely but firmly refused to allow these unknown, unbadged, unauthorized people in; he offered to call his supervisor for instructions, but he resisted all attempts to override the rules. The CEO got a little irritated at first, but on reconsideration, he wrote a letter of commendation to the young man on Monday morning.

4.2 Guards

A well-trained, motivated security guard can be the most sophisticated access-control system in the world. Who else can smell alcohol on the breath of a visitor and watch more carefully, notice a chair moved out of place in an area that's supposed to be empty, verify the expiry date of a proffered driver's license, or notice that someone is wearing the ID of an ex-employee?

One evening I was stopped on my way out of the building by John, the friendly guard with whom I had chatted over the years every time I left after hours. He asked me what was in the large carrying-case I had in hand. It was a computer I was taking home for the weekend. Unfortunately, I had forgotten to get an authorization slip signed by my boss allowing me to remove equipment after hours. John made me put the system back. I thanked him and sent his boss a letter praising his professionalism.

Three weeks later, John stopped another businessman on his way out with a computer. This time, the “businessman” dropped the computer and ran. John had stopped a theft in progress and saved a Compaq portable computer for a firm in the building.

In contrast, untrained or incompetent guards are worse than useless. I have seen guards waving people through who weren't even wearing passes, guards watching television shows instead of monitoring the building status. I have also waited for guards to return to their post from some

Copyright © 1996, 2000 M. E. Kabay. *All rights reserved.*

unknown errand so I could enter or leave a secured area. Such guards merely give the organization a misleading sense of security.

You can hire security guards or you can rent them from security services. In both cases, check their backgrounds carefully. Criminals have been known to infiltrate organizations by working as guards. You can require that a security firm post a bond for its employees; putting up thousands of dollars as proof of their confidence in their agents encourages thorough verification.

Security guards can be imbued with a sense of team spirit if you work at their training. Introduce new security guards to the information systems staff. Take them for a tour of the facilities. Explain how important it is to prevent unauthorized access. Show them the security policies that all employees have to follow. Provide them with clear, unambiguous written instructions on exactly what you want them to do for you. Assure them that they will be backed up when they apply the rules fairly. Explain how they can get authorization for exceptional or emergency cases.

I was impressed by the professionalism of guards at the Central Mortgage and Housing Corporation of Canada. They were using training films dealing with information security and were learning how to recognize diskettes, portable disks, digital audiotape (DAT) cassettes and magnetic tape reels. They were alert, friendly and firm in the way they handled visitors.

These ways of welcoming guards and including them in the team apply to employees of security companies, too. However, you must negotiate with their employer to be sure that everyone agrees on the terms of the guards' functions.

A guard station usually includes provision for telephone access (guards often answer the phone and transfer calls after hours), emergency intercom (for communications throughout the building if the phone system breaks down) and public-address system (to warn occupants of the building in case of emergency). The station usually includes the central alarm panel, showing where and what kind of alarms have been tripped. Many buildings include closed-circuit television (CCTV); the monitors are placed so that the guards can see everywhere within and around the building. Usually there are door lock releases at hand so that the guards can let employees into the building or secured area from a distance (it's safer than having the guards physically move to the doors). Some security guards are authorized to carry hand-guns.

There are normally at least two guards for every guard station. While one guard is away (patrolling, on break, dealing with emergencies) the other can stay at the station. Two guards also improves security in case one of them is dishonest or incompetent.

Guards are especially useful in preventing unauthorized use of someone else's access privileges. For example, they can monitor entrances to prevent piggybacking (having two or more people enter using a single authorization) and passback (passing an access card back to another user to enter a secured area).

Guards can check identity papers of all visitors before issuing visitors' passes. At the Canadian Government Print Center (formerly the Queen's Printer) in Hull, Quebec, guards require visitors to leave some valuable piece of identification (e.g., a driver's license, credit card or employer-supplied ID card) behind when signing in. Assuming the ID is genuine, this practice ensures not only that the visitor returns the visitor's pass but also that visitors sign out correctly. Anyone who does leave the

Copyright © 1996, 2000 M. E. Kabay. *All rights reserved.*

building without retrieving their IDs behind may have been doing Bad Things (or may be terminally absent-minded). There should be no way of leaving a secured area that is guarded by security personnel without having to pass their command post and sign out.

The signature log is not a mere formality. It provides an audit trail that may protect hundreds of innocent employees from being suspected of wrong-doing. The log may help police identify chief suspects in cases of sabotage, theft, arson, and assault. In an emergency, the log could be used to help fire-fighters know how many people are trapped in a burning building by comparing who got out with the list of who were inside.

Finally, there may be legal requirements for you to have guards on duty. For example, if you run a night shift with a single operator, it may be illegal to permit that person to be alone in the building. What if they had a heart attack? broke their leg and couldn't reach a phone? fell and struck their head? A patrolling guard or a regular CCTV scan monitored by a guard can save someone's life.

What if someone went berserk and started taking an axe to your computer systems? A properly-trained guard would call the police and then take measures to distract, delay or disable the attacker. Such action could save you several times the guard's annual salary in a few minutes.

4.3 Mechanical locks and keypads

All locks used for protecting sensitive corporate areas should be chosen with their high-security function in mind. It's quite funny seeing homes which have impressive armored doors, peep-holes and chains and yet have flimsy locks that a child could break with a good kick. Be sure that any locks offered by your contractor or locksmith have solid components, deadbolts that extend at least an inch into the door frame, and protection against being dismantled. As mentioned in the section above on doors, you may wish to install an astragal to protect your locking mechanisms.

Locks that use metal keys and require a locksmith to change are unacceptable for securing busy areas with normal traffic. At best, they will do for small sites with a few employees, and even then only for doors that are used only two or three times a day. Anything more frequent than that, and the doors will end up with tape on the latches or wedges holding them open.

Unless you use special locks with restricted distribution of the key blanks (e.g., ABLOY locks), any key can be duplicated. Don't count on stamped warnings such as, “DO NOT COPY” to prevent anyone from getting a duplicate key. In my experience, confirmed by my locksmith, even registered locksmiths will not respect such a stamp; the local store operator with a key grinder in the corner will almost certainly pay no attention to the warning.

Because of the insecurity of physical keys, you will have to change the locks every time you fire someone or an employee leaves. To change the locks, a locksmith has to dismantle each one and create new keys. This is a tedious and expensive business (according to my locksmith, this cost could range from about $5 to over $100 per lock) (not to speak of the waste of metal in throwing away all the old keys). Each key costs at least $2. Multiply the frequency of departures by the number of people whose keys have to be replaced and you get a sense of the nuisance and cost involved.

Copyright © 1996, 2000 M. E. Kabay. *All rights reserved.*

According to a participant in the June 1992 Information Systems Security course in Montreal, an area hospital spent C$150,000 in a single year changing locks because the directors insisted on having master keys--and there were three different directors who came and went in that year.

An inexpensive alternative to key-locks is the push-button lock. However, these units often have only 5 buttons. If the buttons can punched only once and not in combination, that makes a total of only 235 unique 5, 4, 3, 2 or 1-key combinations. If the buttons can be punched in combination as well, then there can be an additional 26 combinations. To try 261 combinations at 30 seconds per combination would take about two hours of steady, if boring work. If the combination were somewhere around the middle of the sequences, it might take about an hour. If the people who manage the push-button lock fail to reset the factory pre-set combination, it might take 30 seconds. I have personally tested locks at client sites and found the same factory pre-set as at other locations.

Another problem with push-button locks is that people are often careless in their use. Employees often stand at one side of the lock as they push the buttons; this position makes shoulder-surfing (spying out confidential codes) easy for onlookers. If you must use such primitive locks, at least provide a protective sleeve which makes it awkward for observers to tell what the combination is.

Mechanical locks still have to be physically manipulated every time the combination has to be changed. Even though there are no locksmiths required, it is still a nuisance. Adding to this nuisance is the difficulty of informing everyone who shares the combination that there has been a change. Employees who have not been informed waste time and become frustrated as they wait for entry. in time, administrators may forget to change those locks when employees leave the organization.

Finally, such mechanical locks fail to provide an audit trail of entry and departure of personnel.

The concept of trying to secure an area by using a shared combination is itself ludicrous. I saw two delivery youths punching in the combination to a secured area at a paper company where I was on contract. I asked the manager whether they were employees. “Naw,” he answered with a shrug. “We got tired of having to open the door for them every day, so we just gave them the security code for the lock.”

4.4 Electronic systems

Electronic systems offer far more control than mechanical locks for high-security applications. For example, there's the possibility of improving the latching system. Magnetic locks consist of electromagnets on the door frame and metal plates on the door. These devices can require greater tension to break apart the seal than the door or frame themselves can withstand.

Ken Shoopman, an Albuquerque, NM expert in counter-surveillance security and a participant in the April 1993 Information Systems Security course in Denver told the class that too many electronic door locks have vulnerable wiring. By shorting out the unshielded wires, anyone can open such a door. Be sure your contractor uses physically shielded conduits to make the criminal's job harder.

To use electronic access control systems, every authorized user receives an access token, usually a card. Each card is uniquely recognized by the system. Security administrators configure the system to reflect their control requirements. Certain cards confer the right to enter certain areas but not others. There may be time restrictions; e.g., a certain card may not work at all after normal business

Copyright © 1996, 2000 M. E. Kabay. *All rights reserved.*

hours. All of these restrictions can be changed by interactive dialogue with the security system control computer, usually a PC.

Electronic access control systems can be as sophisticated as you require. The more features you use, the more serious about security your organization will be seen to be. Disregarding for the moment the physical token that lets you into a secured area, you will have to evaluate the following features:

o Antipassback: the system remembers who's in the secured area. Passing an access card back to someone else won't work unless the owner uses it to exit first. Makes card sharing very inconvenient. Audit trails could highlight unusual behavior such as entering, leaving three seconds later, and entering again five seconds later. Such apparent behavior could signal misuse of access cards.

o Time-open limits: an alarm rings or a security violation is noted when a door is held open too long. This feature interferes with people who jam doors open in contravention of the security rules.

o Duress signal: if the card is used in a particular way, it lets the user in but triggers an alarm or a display at the guard station. This mechanism allows an employee who is under duress (e.g., being threatened by a terrorist or in trouble but unable to reach a phone) to signal for help. Be aware that newcomers to your system may set this off several times before they get the hang of using their access card.

o Degraded mode: what happens if the power fails? Will all the doors open? Not a good idea. However, safety regulation require you to provide a means for emergency exit, so you should have a panic bar or manual override on the door to let people out of the secured area. To allow emergency entry, you can place a key in a glass case beside the door. What if the access control computer fails? Some systems allow anyone with an access card to open any door under such circumstances.

o Audit features: This feature uses the security computer to keep a trail of all movements and violations in the system. Ideally, you should have a permanent paper record printed out at the same time as data are written to a disk file. Courts have been hesitant at times to accept electronically-recorded data as evidence (because of the fear of undetectable data diddling). You need the electronic version, though, so that you can conduct rapid electronic searches. If the security software produces standard flat files, you will be able to import the data into any modern database system for proper exception reporting. The security system itself may also include a set of reports. *Exception reporting* means that you can ask for summaries of anomalies, rather than the thousands of lines of unexceptional and unexceptionable events.

o Alarms: you will want to evaluate your need for audible and visible alarms in case of intrusion or other security violations. Consider linking your access control computer to the central guard station and ensuring that all alarms are audible in the computer room as well as in the building.

Copyright © 1996, 2000 M. E. Kabay. *All rights reserved.*

4.5 Security cards

Another question is the type of card the system uses. The easiest tokens to use are proximity or "reflected frequency" cards. These cards reflect radio-frequency pulses from wall-mounted readers that are usually built invisibly into the wall near a door. A user with the right card can unlock a door simply by walking up to the hidden reader. One participant in the May 1993 Information Systems Security course in Toronto told us that a friend of hers startled her by throwing what appeared to be a karate kick at the reader in the wall--and opening the door. It turned out that he had been forgetting his card at home too often for convenience. Since he always wore cowboy boots to work, he got into the habit of putting the card down the side of his boot. Anything for kicks, I guess.

Wiegand cards use embedded metal fibers which respond to the magnetic fields in special readers; they are difficult to counterfeit. Ordinary magnetic stripe readers are inexpensive but easy to duplicate. Infrared-readable patterns are harder to counterfeit but cost more.

In the December 1992 Information Systems Security course, I was amazed to have in the class two security experts with 25 years of experience each (they were looking for teaching techniques and material). One of them pointed out that in the first week after installing any kind of access control system, you should program the computer to give all cards access everywhere except the most secure areas. This plan will help prevent frustration due to the inevitable errors in planning, implementation and communication of the new security routines. The same principle applies to the duress signal: be accepting and understanding when you get errors at first.

Finally, when you plan the placement of your card readers, don't forget the special needs of handicapped people. Proximity sensors, for example, can work on cards that are anywhere within a couple of feet of the wall panel--ideal for people sitting in wheelchairs or who have limited mobility.

4.6 Biometric devices

Instead of making people carry unique tokens showing that they are who they claim they are, why don't we just recognize individuals and determine if they're authorized to use their IDs? Biometric methods do precisely that. Such methods are based on the hope that the variability in biological or behavioral characteristics of an individual will be less than the differences among individuals. In addition, we need characteristics that are relatively stable over time.

Biometric methods offer the convenience of never being without your identification and authentication (and if you should lose various bits of your anatomy, being rejected by the access control system will be the least of your troubles). All these methods require the prospect to initialize the system with some preliminary measurements or recordings.

A relatively primitive biometric method is the height/weight cabinet. This apparatus consists essentially of a small cubicle into which only one person can (decently) fit. The cubicle is equipped with a scale to measure weight and lights and sensors to estimate the height of the occupant. The combination of height and weight is supposed to allow unique identification of each person registered in the computer system that reads and interprets the data.

The utility of such a method depends on the stability of weight and height and on the tolerance for deviations. I leave it to the reader to imagine the consequences of imposing overly stringent

Copyright © 1996, 2000 M. E. Kabay. *All rights reserved.*

limitations on acceptable weight deviations... say, after the Christmas holidays.... It would take only a few embarrassing incidents ("Did you hear about Susan? She got rejected by the height/weight cabinet: that means she gained more than 15 pounds!") to cause a revolt among the staff. Additional difficulties for the height/weight cabinet: high heels, carrying a heavy briefcase and wearing a beehive hairdo.

Hand geometry measurement devices are another biometric method available for identifying individuals. The lengths and thicknesses of fingers and the angles between the fingers at maximum extension of the hand are sufficiently different among people that they can be used to screen imposters.

Voice verification systems attempt to identify and authenticate a person by recording baseline voice prints for a specific phrase and then asking the person to repeat that phrase when trying to gain access. This method doesn't work well when people develop head colds, are under the effects of medication or drugs which affect speech, or suffer damage to their vocal cords. However, it is very capable of rejecting imposters. To prevent the use of recordings, the system can be primed with several phrases and can prompt the candidate with a question or challenge randomly selected from the list originally prepared by the authorized person. For example, the system could be primed with questions such as, AWhat was the most enjoyable course you ever took in high school?' An imposter would find it hard to search through a tape looking for the answer to one of a number of questions.

Keystroke dynamics recognition systems keep track of the millisecond delays between characters when people type familiar phrases such as their own name. Anything that affects this pattern will cause false negatives. For example, tiredness, stress, coffee, alcohol and other conditions and drugs could cause a false alarm (rejection of an authorized user). It would also be important to retrain the system for anyone learning to type better. However, as in the case of voice verification, this approach is good at spotting imposters.

Signature dynamics depends on a special stylus equipped with accelerometers that can measure movement forward and back and left and right. The sequence of movements that one person uses in signing their own name is unrepeatable by anyone else.

Retinal scan devices use a low-power laser to read the patterns of blood vessels in a person's eye. These patterns are as characteristic of the individual as fingerprints. In addition, changes in retinal patterns may indicate pathology, so the scanners could serve incidentally to identifying users with eye problems. A retinal scan system has been successfully used in Illinois' Cook County Jail to process thousands of prisoners since October 1990; it successfully stopped over 40 attempted impersonations in the first six months of 1991. However, I suspect that it might be a little harder to convince your staff to use a device that beams lasers into their eyeballs than imposing it on prisoners was.

Fingerprints have been a method of choice for the unique identification of people for centuries. By the mid-nineteenth century, it was established that no two human beings have exactly the same fingerprints--even identical twins have minor but recognizable differences. With advances in the performance of inexpensive computers, automated pattern recognition has become feasible even for civilian applications. Fingerprint recognition devices require a specific finger to be inserted into a measuring chamber and pressed against a glass surface. A laser beam records the pattern of ridges and digitizes the information for pattern recognition and transmission.

Copyright © 1996, 2000 M. E. Kabay. *All rights reserved.*

In January 1993, Digital Biometrics (Minnetonka, MN) announced that it had won a $5.2 million contract with the Internal Services Department of the County of Los Angeles for a "live-scan" fingerprint system. The system allows fingerprints to be registered electronically and instantly dispatched anywhere in the network of 100 units, where they can be reproduced by laser printers with full fidelity.

Systems are available at much less than $50,000 per unit, although you should still expect prices in the $1,000 range.

As you have probably gathered, biometric methods are still either too imprecise to depend on as primary methods of identification and authentication or they cost too much for ordinary use. However, for specific applications such as factory data capture where every second counts or where there are hundreds of interactions with a computer system per day per person, biometric systems may be cost effective. One way of avoiding high costs for ultra-precise systems is to combine two or more methods of identification and authentication. The probability that both methods will fail to identify an imposter is the product of the individual failure rates of the separate methods.

5 CHAPTER NOTES

5.1 Several good books include reviews of physical security:

Garfinkel, S. & G. Spafford (1991). Practical UNIX Security. O'Reilly & Associates (Sebastopol, CA). ISBN 0-937175-72-2. Chapter 19, APhysical security.' Available from the NCSA. Also reprinted as APhysical security: the basics' in Datapro Reports on Information Security report #IS41-050-101.

Russell, D. & G. T. Gangemi (1991). Computer Security Basics. O'Reilly & Associates (Sebastopol, CA). ISBN 0-937175-71-4. Chapter 9, APhysical security and biometrics.' Available from the NCSA.

Wood, M. B. (1982). Introducing Computer Security. National Computing Center (Manchester, UK). ISBN 0-85012-340-2. Chapter 3, APhysical security.'

5.2 On computer room design and infrastructure:

Welch, D. E. (1994). A room of one's own: Design tips for the server room: raised flooring, custom-fitted racks and a cool climate never go out of style. LAN Magazine 9(12):65.

Hassett, J. (1992). The basics of data center site design. Datapro Reports on Information Security report #IS41-140-101.

Strauchs, J. (1986). Designing the computer room for security. Datapro Reports on Information Security report #IS40-050-101.

A later version of this report is:

Strauchs, J. (1991). Security design considerations for computer rooms. Datapro Reports on Information Security report #IS41-150-101.

Copyright © 1996, 2000 M. E. Kabay. *All rights reserved.*

Brill, K. G. (1990). Ensuring Facility Infrastructure Reliability: Making Computer Environmental Systems Fault Tolerant. ComputerSite Engineering (Danvers, MA). Reprinted as "Designing fault tolerant environmental systems" in Datapro Reports on Information Security report #IS41-100-101.

Anonymous (1989). Controlling the computer room environment. Datapro Reports on Information Security report #IS41-700-101.

5.3 Recent (in 1995) articles and reviews dealing with power conditioning equipment:

Deixler, L. (1994). We got zapped! Teleconnect 12(11):84

Hassett, J. (1992). Understanding power quality and conditioning. Datapro Reports on Information Security report #IS41-110-101.

Anonymous (1992). No?fault insurance for the rest of us. Computer Shopper 12(6):215 (June 1992).

Levine, R. (1992). Power on! DEC Professional 11(6):38 (June 1992).

Smith, G. (1992). Prepare your PC for the worst: eight precautions to take before your system crashes. PC?Computing 5(5):146 (May 1992).

Anonymous (1992). Intelligent Power Module puts your PC to bed after hours. Computer Shopper 12(4):851 (April 1992).

Rosch, W. L.(1992). PC power when you need it: power directors, backup power, and surge suppressors keep the juice flowing. Computer Shopper 12(2):528 (Feb 1992).

Panchak, P. L. (1991). PCs and LANs: Power Protection. Modern Office Technology 36(11):40 (Nov 1991).

Dern, D. P. (1991). Keeping your computer safe for business. Home Office Computing 9(7):46 (July 1991).

Taylor, W. (1991). Don't allow electronic hazards to zap your PC. PC?Computing 4(6):240 (June 1991).

Rowinsky, W. (1991). Power directors: convenience plus protection: overview of 16 evaluations of power conditioning devices. PC Magazine 10(2):305 (Jan 29, 1991).

Derfler, F. J. Jr. & P. Ferrill (1990). LAN Server UPSs: overview of 26 evaluations of uninterruptible power supplies for local area networks. PC Magazine 9(20):321 (Nov 27,1990).

5.4 Good articles on EMI/RFI:

Lineback. J. R. (1994). Europe's EMI immunity rules spark concern, unease at OEMs. Electronic Business Buyer 20(8):29

Betts, M. (1994). FDA seeks Rx for radio wave ills. Computerworld 28(25):1

Copyright © 1996, 2000 M. E. Kabay. *All rights reserved.*

Collins, T. (1990). Deadly waves that spell disaster: Electromagnetic interference affects all kinds of computer and microprocessor?based systems. Computer Weekly (1221):18 (July 5, 1990)

Rosch, W. L. (1989). Unwanted emissions: EMI and RFI. PC Magazine 8(18):140 (Oct 31, 1989)

5.5 On the banning of Halon and alternatives for fire prevention and suppression:

Anonymous (1994). CFC policy goes into effect. Chilton's Hardware Age 231(5):30

Sullivan, C. C. (1994). Halon: CFC's cousin. Buildings 88(4):72

Anthes, G. H. (1992). Data centers get the halon out of there: Fire retardant alternatives not always good solutions. Computerworld 26(30):82 (July 27, 1992).

Bennett, C. (1992). Net closes in on CFC users: Legislation will be passed outlawing use of ozone-damaging chemicals such as chlorofluorocarbon. Electronics Weekly (1602):32 (June 24, 1992).

McLachlan, G. (1992). Computer room politics: And another thing... ozone depletion. HP Professional 6(5):88 (May 1992).

Corby, M. J. (1992). Managing disaster recovery testing. Datapro Reports on Information Security report #IS38-450-101.

Brown, R. (1991). Case study: the Steinberg fire. Datapro Reports on Information Security report #IS38-920-101.

Betts, M. (1991). EPA official: Halon phaseout to accelerate. Computerworld 25(49):1 (Dec 9, 1991)

Forsythe, J. (1991). Halon--still a burning issue: Finding another alternative besides halon to fight data center fire. Information Week (325):28 (June 17, 1992).

Betts, M. (1989). Data-center showers may be halon option: Computer center fire fighting equipment. Computerworld 23(27):1 (July 3, 1989).

5.6 Closed circuit television systems:

Newton, M. (1994). Picturing the future of CCTV. Security Management 38(11):60

Meley, M. S. (1991). Closed-circuit television (CCTV) systems: Overview. Datapro Reports on Information Security report #IS41-250-101.

5.7 On physical access control and biometrics:

Bowers, K. (1995). Seeing is believing. Doors and Hardware 59(3):46.

Zunkel, R. L. (1994). Palm reading for protection. Security Management 38(11):87

Harowitz, S. L. (1993). Biometrics: more than meets the eye. Security Management 37(2):24.

Copyright © 1996, 2000 M. E. Kabay. *All rights reserved.*

Duncan, R. J. (1992). Physical access control systems: Overview. Datapro Reports on Information Security report #IS42-001-401.

Duncan, R. J. (1992). Physical access control systems: Comparison columns. Datapro Reports on Information Security report #IS42-001-408.

Daly, J. (1992). Fingerprinting a computer security code: Biometric devices secure computers beyond a reasonable doubt using personal characteristics no one can steal. Computerworld 26(30):25 (July 27, 1992).

Booker, E. (1992). Retinal scanners eye-identify inmates: PS/2-based biometric devices keep track of prisoners at Chicago's Cook County Jail. Computerworld 26(12):28 (Mar 23, 1992).

Bass, Brad (1991). Strict FBI specs spook would?be NCIC players: The US Federal Bureau of Investigation's National Crime Information Center 2000 procurement. Federal Computer Week 5(34):1 (Nov 18, 1991).

Richardson, J. (1990). Sandia tackles biometric inertia: Sandia National Laboratories' Safeguards and Security Group evaluates biometric verifiers and other entry monitoring devices. Federal Computer Week 4(30):1 (Aug 20, 1990).

Toigo, J. (1990). Security: biometrics creep into business. Computerworld 24(24):75 (June 11, 1990).

<<end>>

Copyright © 1996, 2000 M. E. Kabay. *All rights reserved.*

LAST MODIFIED: April 18, 2020

NCSA Guide to Enterprise Systems Security

FILE: CH_06_C.WPD

Chapter 6: Identification, authentication and authorization

Objectives:

After studying this chapter, the reader should be able to

1. choose suitable composition and length of passwords.
2. define acceptable lifetimes for passwords.
3. explain who should choose passwords and how.
4. explain why passwords must not be shared.
5. guard against disclosure of stored passwords.
6. protect passwords against disclosure during entry.
7. define an acceptable period of use after which re-authentication should occur.
8. choose additional methods of authenticating the use of an ID.
9. discuss the advantages and disadvantages of the single logon in a multiple-system environment.
10. decide whether hand-held password generators and smart cards are suitable for a particular situation.
11. understand and apply methods for authorizing access privileges.
12. solve the problem if someone forgets a crucial file password.
13. follow security applications of artificial intelligence.

[A] The fundamentals of access controls

Identification, authentication and authorization are at the heart of access controls. A human being (or another computer system) is *identified* by a user-ID. User-IDs confer privileges on a computer system: *authorization* to access specific resources such as files, databases, phone lines, printers, tape drives, and disk drives. Access to buildings, services or computer systems depends on either what one knows (combinations, secret passageways, passwords, influential names) or what one has (keys, explosives, money, weapons). The user-ID is usually *authenticated* when its user knows a secret password or in some other way indicates that the user really is the person authorized to use that ID. The challenge is to select and manage passwords so that they cannot easily be discovered by unauthorized users and are not compromised by naive users.

This chapter begins with a look at the ways that passwords can be compromised and then summarizes how to use passwords securely. It ends with a discussion of how to manage user IDs and passwords when users have to access many systems.

[A] Attacks on passwords

How could someone determine a secret password?

[B] Borrowing

The consultant strides into your cubicle. "Hi Bob, could you log on to your account for me?" You answer irritably, "What, again? Here--why don't you just use my ID and password yourself for now. I'll change it later." And there we are: a password is no longer secret. From this point on, you can no longer affirm that an audit trail kept by the computer security software is correct: a logon under your ID may or may not represent your activities.

Even *asking* to borrow someone's ID and password is a breach of security.
Sharing a password with someone for momentary convenience compromises security. The lender may forget to change that password, providing an open door until the next change. Users who choose passwords badly (see below) may reveal patterns or preferences which make it easier for the borrower to guess subsequent passwords; e.g., if a poorly-chosen password is "FEB02MYPASS" in February, what do you think the password for March might be?

A borrower may abuse your confidence. What will you do when an abusive email message is circulated to top executives under your user ID? How will you feel when a critical and sensitive spreadsheet is "shared" with your competition? What will happen when an ID-borrower contravenes Securities and Exchange regulations against insider-trading?

Lending someone your user-ID and password is exactly equivalent to lending them your bank card and personal identification number. For Canadians, it's like giving them your medical card.

Naive users often protest that others have to share their own password "because there's no other way to get the work done." *This assumption is absolutely, categorically, universally wrong.* I put it this strongly because the assumption is so widespread. If a user needs to share files or other resources with another user, both should ask the person who administers security on their system for help. Security systems for multi-user computers *will* provide for access to private resources if they are used correctly. Anything that an individual user-ID can do can be accomplished by another user given appropriate permissions or capabilities. For example, many electronic mail (email) systems include features to allow someone's secretary to read, print and even reply to the principal's mail; however, all such transactions are recorded correctly in the audit trail with the secretary's ID, not the principal's. Replies are also unambiguously "signed" correctly with the secretary's name.

If the current security system makes controlled access difficult, you can replace the security system. Even a single-user computer's security can be upgraded to allow more flexibility.

Some people make ill-considered end-runs around their security systems. For example, if two users need read-access to a file that doesn't change, the file owner can make a copy. The problem is that the borrower of the copy may not respect the security restrictions on the original file. If the file changes, the borrower will have out-of-date data. If the users both need read/write capability, they *must* use a locking system to avoid overwriting each other's changes. Consult your system administrator to avoid blunders that could cost your employer money and yourself your job.

[B] Theft

Some people write their password down. Security auditors look for the yellow Post-It (TM) note stuck behind the monitor / under the keyboard / on the underside of the mouse pad (and so on and on) when looking for passwords. So do password thieves.

Computers with complex system-logon scripts sometimes include passwords in the logon procedure. A thief who steals such a computer may acquire automatic access to one or more networks. The logon script should require either manual input of passwords or a key (password) to decrypt the script itself.

[B] Guessing

Many users choose passwords with personal associations. On systems where the passwords are not encrypted, administrators have noticed unusual passwords: names of dogs, sports teams, cars, children and spouses (and even non-spouses); words from hobbies; favourite obscenities; ordinary words spelled backwards. The infamous *Joe* logon is one whose password is the same as the ID; e.g., logging on as HOSKINS and having the password HOSKINS.

A password guesser would be interested to know that Ruth's ruling passion is bingo. Bob's infatuation with Gillian might suggest some likely passwords. Samid is a fanatic player of voluntary taxation (lotteries); his latest get-rich-quick scheme is to "invest" $10 a week in the Grand Blotto game. Any of these titbits of information might help crack these people's passwords--if the passwords were poorly chosen.

Password guessers can gently quiz friends or fellow workers to find out intimate details of their target's life. Security folklore even includes seductions arranged in order to extract confidential information usable for cracking passwords. Such manipulation is known as *social engineering.*

[B] Dictionary

If ordinary words are permitted in passwords, a guesser can systematically try to guess those passwords by using entries in an online dictionary. If a password file is encrypted using a known one-way encryption algorithm, a password-guessing program can try every word in the dictionary to see if their encrypted forms match the values in the password file.

[B] Brute force

The method of last resort for a password guesser is the brute-force approach. Is the password A? B? C? AA? AB? AC? If the rules restricting choice of password are known, the search can concentrate on the appropriate lengths and composition. The difficulty of the search depends on the *keyspace,* which is the total number of possible passwords which conform to the rules.

For example, a single-character alphabetic (letters only) case-insensitive password has a keyspace of exactly 26. If the length of an alphanumeric password (letters and numbers) is 6, the keyspace is 36^6 or about 2 billion. If a 6-symbol alphanumeric password forbids repeated symbols, there will be 36x35x34x33x32x31 or about 1 billion different passwords in the keyspace.

On average, a systematic search through the keyspace will take half the keyspace to locate a randomly-chosen password. Thus cycling through AAAAAA through ZZZZZZ looking for a six-character alphabetic sequence might take about a billion tries on average to locate an unknown password.

The success of a brute-force attack depends on how fast one can try passwords. If trying means logging on, the response of the system under attack will be the most important determinant of speed. If trying means matching values in a file, the speed of the computer system doing the matching will determine how long it takes to crack a password.

[A] Password hygiene

Having explored the methods used to guess passwords, let's summarize the defensive mechanisms you can use to protect yourself against involuntary disclosure or discovery of your passwords.

[B] Composition and Length

The ASCII character set includes 26 upper-case letters, 26 lower-case letters, 10 digits, and 26 other "special" (non-alphanumeric printable) characters (excluding the space character):

! " # $ % & ' ( ) * + , - . / : ; < = > ? ` { | } ~

In theory, if all of these characters are permitted in a password, the keyspace for a single-character password is 88. A double-character password has a keyspace of 88^2 = 7744 and an n-character password has keyspace 88^n.

In order to have a keyspace of, say, 1 billion (10^9), you need to define a minimum password length of 5 such alphanumeric and special characters.

In contrast, if the password composition is limited to uppercase letters and numbers only, there are only 36 possible values for one character; the keyspace for n characters is thus 36^n.

In order to have a keyspace of 1 billion, you need passwords at least 6 characters long with uppercase letters and numbers.

If you stick only to uppercase letters, you are limited to 26 characters; to have a keyspace of at least 1 billion, your passwords have to be at least 7 letters long.

Completely random passwords are difficult to remember. How would you like to deal with A#U8^3+14? Much easier is to build syllable-like passwords; e.g.,

BOLACIRY NALUDOPP VROGATUEE.

The limitation on choices in each position reduces the total keyspace, however, so it is wise to include numbers and special characters as well:

BO3LA@CIRY 8NA(LU!DOP+P V3RO^GA-TUE$E.

In practise, upper-case letters, numbers and even special characters are easy to remember when there's a syllable-like structure. However, varying upper-case and lower-case letters in passwords makes them very difficult to remember:

BO3LA@ci7rY 8nA(lu!dOP+p V3ro^Ga-TuE$e.

Such passwords are so easy to forget that many users will write them down--thus increasing the likelihood that the passwords will be stolen.

Another method for generating easy-to-remember, hard-to-guess passwords is to use letters from familiar phrases or rhymes. MHALL (from Mary Had A Little Lamb) is a good start for a password like M*HA3L!L. Users can use any rule they like as long as the results are gibberish.

I quote (with a few minor punctuation changes) a recent IBM corporate password policy from the *IBM UK Information Network Newsletter*. It summarizes some of the key points made above as well as some not-so-obvious risks:

- A password will be disallowed if its length is not at least six characters and satisfies the length rules specified by the installation.

- The first character must be alphabetic.

The following strings cause the new password to be disallowed:

- the year number for this year, last year, and next year;

- three-character abbreviations for the months of the year, regardless of the current month;

- three or more characters in ascending or descending sequence from the alphabet or numbers;

- four or more characters in horizontal sequence in either direction from the keyboard;

- any complete match with an 8-byte string in a table (variable *invword*) of passwords previously found to be frequently used; this test involves a compare with the full password (sub-strings are not considered);

- at least four characters in the same relative positions must be different from the current password;

- any three-character string from the old password, if present;
- any string of three identical characters;
- any string of three characters repeated or reversed;
- any character repeated more than twice;
- the user identification or any three-character sub-string thereof;
- all initials appearing together will be disallowed, and if more than two exist then the first and last will be disallowed when used together;
- the surname, or any four-character sub-string thereof;
- the RACF Groupname, also in reverse.

[B] Automatic screening of user passwords

One approach to making passwords harder to crack is to check every password when it is proposed by a user at password-changing time. The operating system or other security software can enforce the rules by parsing the proposed text; e.g., verifying that at least one character is non-alphabetic, ensuring minimum length and so forth. In more sophisticated approaches, the security software can verify that the proposed password is *not* found in a dictionary of forbidden words. However, if a large dictionary is simply used as a lookup table, processing time can become significant. To speed up the analysis, Stallings (1994) describes how to use Bloom filters (a method for computing hash functions of all entries in a dictionary and rapidly evaluating whether a proposed password is in that dictionary) for screening passwords.

Another problem is that dictionary lookup does not catch simple variations on common words (e.g., what4). Davies & Ganesan (1993) presented a paper at the 16th National Computer Security Conference and won an award for their innovative approach to qualifying proposed passwords. The strategy they implemented in *BApasswd* (so named because it was developed at Bell Atlantic) is to look at the transition probabilities for each letter or number in turn. This means that when a user proposes, say, "googol3" as their password, the algorithm "uses statistical tests to determine, with a high degree of confidence, whether that password could have been generated by the same ... process" that accounts for all the words in the dictionary. The extra "noisy" character (3, in our example) does not interfere with the software's ability to reject a poorly-chosen password.

[B] Lifetime

On the theory that all passwords can in theory eventually be compromised, security policies dictate that passwords have a maximum period of use or lifetime.

One writer (Leichter, 1991) thoughtfully questions the basis for the belief that frequent password changes are necessary or even useful. He points out that these policies may have originated in the

military, where several people often share a single user-ID and password. Therefore the risk of leakage is greater than if a single person uses a password. With only one ID for many people, the only way to revoke access privileges is to change the password and tell only the remaining staff what the new code is. However, with one-password per person, there are easier ways to revoke access privileges. Finally, Leichter suggests, shared passwords are often spoken out loud, increasing the chances of a security breach.

Leichter suggests that there are only two reasons for changing passwords: to respond to a known breach of security (e.g., someone has been shoulder-surfing as you enter your password) and to prevent unknown leakage of your password.

In Leichter's opinion, policies which mandate frequent (by which he means more often than twice a year) password changes are quasi-religious rituals designed to give the illusion that security is tight--regardless of whether the practice is necessary.

I have been quizzing participants in the *Information Systems Security* course for years about the lifetime of their passwords. Almost no one changes their passwords more often than once a month or less often than once a quarter. The problems caused by frequent password changes (forgetting the new password) are easily prevented by appropriate choice of password.

No one would dispute that you must cancel user-IDs or change their passwords immediately upon firing their user. If there is any question about what other passwords the departed user may have known, those should be changed too.

Warn users that their passwords will expire. For example, let the security system announce that a password will expire in 10 days... 9 days... 8 days... and so on. On the last day, users will be unable to continue their work until they change their passwords.

When this system is first imposed, there may be a surge on the last day in the number of phone calls you receive as system administrator to reset forgotten passwords. However, some users will naturally change their passwords at the first warnings; others will wait until they are forced to change. This difference of style has an advantage for system administrators: requests for password resets will eventually be spread out over the entire password lifetime.

Every security system should include a password history to preclude reuse of favourite passwords. The history file should be configurable to permit at least 13 entries to prevent month-oriented passwords such as JANMYPASS, FEBMYPASS, MARMYPASS and so on. Although 13 entries in the history will discourage most people from changing their password back to the same old value, it cannot stop the determined rule-breaker. I have had one report of a user who actually cycled through 25 passwords in order to return to his familiar, years-old password. One approach to this problem is to prevent more than a single password change per day.

[B] Source

Who or what creates passwords? On most systems, the user chooses passwords. On more secure systems, the system provides a generated password or a menu of possible choices. In all cases, acceptance of the password should be conditional. Conditions should include minimum length and composition. If numbers and special characters are not required in the password, it is a good idea for the password-checking algorithm to check the proposed password against a dictionary of ordinary words: ordinary words won't do.

Remember that canonical passwords are a problem everywhere. Canonical passwords are those that are the same from system to system. Change all vendor-supplied passwords to conform to your standards.

When you define a new password or reset a password for a user, the security system should limit this value to a single use--enough to allow the user to change the password to a secret value.

[B] Ownership

As mentioned above, passwords should be uniquely assigned to an individual human being. "Shared password" is an oxymoron.

Employees' security agreement must include clear language prohibiting the disclosure of passwords. Improper use or protection of passwords (e.g., lending or displaying a password) should lead to disciplinary action; in the extreme, repeat offenders should be fired.

[B] Entry

Practically every software package in use today blanks the entry field for passwords. It is unthinkable to allow passwords to appear on screen when they're being entered. Those still using printing terminals must ensure that any request for password entry includes a series of overstrikes that create an unreadable area where the password may be typed; a common series is MMMMMMMM ^H^H^H^H^H^H^H^H WWWWWWWW ^H^H^H^H^H^H^H^H XXXXXXXX (where ^H represents the backspace character).

Users must be trained to guard against observation while they log on. If necessary, users should ask a visitor to look away during password entry. When I visit a customer site, I turn away physically while a user is logging on in my presence. In a world where social conventions have caught up with technology, it will be as shocking to find someone watching as you enter a password as to find them watching when you use a toilet.

I have encountered sites where users were permitted to define one-character passwords. Anyone interested in learning such a password need merely find out that it is single by watching the user--even from a distance--and then can try all possible characters in a few minutes.

To foil automated password guessers, you should enforce a delay of at least a few seconds after an incorrect password before asking for the next attempt. After about three errors, you should configure a delay of at least a few minutes before allowing that access port or user ID to try logging

on again. At some point in a sequence of errors, your system ought to inactivate the ID until further notice. However, if you can manage it, the system would ideally allow the intruder to continue guessing at passwords--it just wouldn't recognize even the correct password. This delaying tactic might give you a chance to determine where the attack was coming from.

A security audit trail includes the time of every incorrect logon. Exception reporting provides you with only those cases where the number of errors exceeds a threshold. It should also allow you to see a summary of those IDs which have the highest frequency of errors. Either the user has picked or been assigned a bad password (one that's hard to remember) or someone is trying to crack their password.

As a mechanism for self-auditing, some security software posts a notice about the last successful logon and the last unsuccessful attempt to log on. Any discrepancy should be reported to security at once. "Hey, I never tried to log on at 03:30 Sunday morning!"

Should repeated errors during logon cause cancellation of the ID in question? Such a policy ensures that an ID under attack cannot be used by the attacker but it inconveniences the legitimate owner of the ID. Theoretically, someone who knows the IDs in use on your system could lock everyone out by systematically attacking each ID with bad passwords. Such an attack would surely include standard IDs for system supervisors. Supervisors could find themselves incapable of logging on to reset the locked IDs.

I feel that the disadvantages of blocking IDs under attack outweigh the benefits. However, if your policies require IDs under attack to be disabled, supervisory IDs should have special mechanisms in place to prevent the deliberate or even accidental lockout of system managers.

If your software allows it, you can set up a system which notices repeated attacks on supervisory IDs. The system can then terminate access to the access port until further action is taken. Such a system will work when the attack is from outside your network and uses a modem connection; it is much more difficult to arrange if the attack is on a Local Area Network.

[B] Storage

Passwords *must* be stored in *encrypted* form on any computer system. Systems which store plaintext (readable) passwords anywhere on disk or in main memory are vulnerable to attack. Anyone having access to the stored passwords has the capacity to impersonate any user on the system.

One-way encryption routines convert an entered password into gibberish--but it's always the same gibberish for a given password. Therefore when a user next enters the password, the security software converts it to the encrypted form and compares that gibberish with the stored gibberish. When the two values match, the system assumes that the entered password must have been the same as the original password.

Unfortunately, even such a system is vulnerable to cracking. If the algorithm is known or if the attacker can observe the encrypted form of large numbers of passwords, the attacker can generate a

list of encrypted versions of known passwords. Any encrypted forms that match the existing list of passwords tells the attacker the original version of the password.

It follows that your security scheme must protect the password files or other structures against disclosure even if they are encrypted. For example, backups that contain the password lists must have as much protection as the disks they backup.

[B] Authentication period

Once someone has successfully logged on to the system, their session is vulnerable to piggybacking. If the authorized user leaves their session unprotected, someone else can use their session for unauthorized purposes.

Many systems allow you to configure a tolerance for inactivity in a session; after this time limit, an inactive session is locked. The authorized user need merely re-enter their password to resume at the same point they left off. Screen savers on PCs provide this function.

Some host-based security systems try to provide the same functionality; however, even if they monitor both *keystroke* and *CPU* activity, they are subject to error. For example, if a user is in block mode, their keystrokes are invisible to the host processor and they are using no CPU at all during data entry. A short tolerance for inactivity could cut someone off right in the middle of working on a complex screen.

A re-authentication procedure should not log someone off after a short period of inactivity; it should simply ask for the correct ID and password. However, if inactivity persists, logoff may be required to free up system resources. For example, if the backup procedures require all files to be closed, sessions left with open files will have to be aborted to be sure everything gets backed up properly.

Before implementing such a forced-logoff procedure, you should verify that the operating system (OS) can handle such aborts without causing file damage. This precaution is especially important if database programs allow transactions to be interrupted by human intervention. For example, if a database transaction affects several files, it could be disastrous to abort a session that had made a few changes and then paused with the database in an inconsistent state.

[A] Alternative methods of authentication

There are alternative mechanisms for detecting fraudulent use of a password. In a previous chapter, I reviewed access control devices based on biometrics--the measurement of a user's structure or function. The same devices used for controlling physical doors using computers can defend the computer systems themselves. For example, in addition to entering the logon ID and a password, users might have to insert a finger into a fingerprint reader before being permitted to access their files. In a flash of imagination, I can see such a system being equipped with a finger lock to trap password thieves (and in the next flash, I can imagine how irritated the users would be if the security program made a mistake!).

Another approach to authentication is to define a database of confidential information that only the official user of an ID should know. Typical questions include knowledge that is not part of the public record; e.g., pet names of family members, stories from the user's family or personal history, names of childhood friends, colour of the car the user learned to drive in, the name of the first piano teacher, the user's favourite book, and so on.

The questions in this *personal profile* are usually framed secretly by the user during an initialization phase and then encrypted. Alternatively, the security manager can define the questions. The user's answer to each question is one-way encrypted. During logon, one or more questions is decrypted and presented to the user, who answers easily because the knowledge is supposed to be intrinsic. Any error immediately suggests that the user is an imposter.

Be very careful to explain to your users that they are *not* to try any fancy tricks with the personal profile; one of my system managers locked himself out of a system by giving false answers to the profile questions and then, naturally, forgetting them.

[A] Multiple systems

One user in the April 1993 session of the *Information Systems Security* course in Denver reported that certain programmers in his shop required 16 different logons to support all the systems and networks in his organization.

Now, programmers may be able to handle 16 different logons, but ordinary users will revolt at having to do so. They'll write them down or program them into their access software.

There are two approaches to handling the password problems of multiple systems: the single logon and hand-held password generators.

[B] Single logon

Suppose you have several networks, PCs and mainframes in use. Could you define a single logon ID and password for each user? Yes, but it's a devil to manage.

If all the systems are separate and have different OSs, you may have trouble finding an acceptable single ID and password pair. This system uses 8-digit alphabetic IDs; that one uses 6-digit alphanumerics. This system forces you to use special characters in the password; that one doesn't allow them.

Even with the same OS, separate systems will require separate password changes to stay synchronized. Either the users will have to change their passwords multiple times (and they'll inevitably forget) or you'll have to provide a facility for automatic password changes on all the systems they use. Such a facility will have to be protected against disclosure of the old and new passwords, providing yet another headache for overworked security administrators.

There *is* a hardware mechanism to provide a single logon to multiple systems: the data switch or front-end processor (FEP). These devices provide access control and then allow authorized users to link to whichever system they require, usually invisibly. Value-added networks (VANs) such as CompuServe do this all the time: once a user has logged onto the VAN, there are no further logons required even for access to other host systems such as those that provide online databases.

The FEP must be secured as thoroughly as the hosts to which it provides access. If passwords are stored on the FEP they must also be encrypted and secured. The FEP security system should include the same level of audit facility that the hosts require.

Host security must not be compromised by lowering the barriers to unauthorized access. Even if a FEP handles access security, it would be a mistake to weaken security on the host--it could be defenceless against an attack that bypasses the FEP. In addition, protect hosts against physical disconnection from their FEP.

[B] Hand-held password generators

There's a different approach to access controls which depends on tokens (e.g., physical keys). These devices make it unnecessary to remember passwords at all.

Most computer systems have provisions for passwords, but there are circumstances in which tokens have advantages. For example, a high-security research project might need measures that make passwords difficult or impossible to guess or to steal. The theft of a physical token is easier to spot than the theft of a password. In organizations such as the military, distribution of physical passes and keys may be easier to regulate and monitor than knowledge of a password. On the other hand, a token can be lost just as a password can be forgotten.

For those sites preferring to include tokens as part of their security systems, a hand-held password generator may be useful. To give you a sense of how these work, I present a detailed analysis of a particular product.

I routinely capture news-wire reports touching on information systems security through the CompuServe *Executive News Service,* and I in 1992 I spotted a news release about a major contract for security products from VASCO Corporation's ThumbScan line. On May 5, 1992, VASCO announced that ThumbScan's SOFTBoot and Access Key products would be incorporated into "The Resource Center (TM)" from Resource Computer Systems. This integrated, briefcase-sized unit combines cellular phone, fax, computer, printer, modem and battery. Thumbscan's cellular data-encryption product, Scramble, is also available in The Resource Center.

ThumbScan, Inc. was founded by members of the University of Illinois groups in computer technology and electrical engineering in 1985. ThumbScan acquired Gordian Systems, makers of the hand-held password generator called the Access Key. Over 100,000 Keys have been sold worldwide.

ThumbScan's Extended User Authentication systems are based on the Access Key, a domino-sized, self-contained unit containing a custom microprocessor, optical sensors, clock, liquid-crystal display (LCD), and five-year lithium battery. Interlocks on the unit disable it if the seals are broken. Each Key is programmed with a particular base number--loaded either at the factory or by the ThumbScan Keycutter System available to institutional purchasers. In use, the system, using special routines provided by ThumbScan, generates a pattern on screen which is read by the Key; this pattern is the input prompt or challenge in the challenge/response process. The Key generates one of 16,777,216 different alphanumeric responses as a function of time and input; the value generated changes from moment to moment throughout the day but can always be processed by the host-resident algorithm to determine which Key generated the value in response to a prompt.

The Key must be physically in contact with the display screen in order to be used; this requirement precludes collusion in which a Key-holder could receive a prompt by phone from a confederate, enter it manually into a Key, and read the generated code back over the phone to the confederate. With this Key, if the correct access code is entered, the Key must be present at the terminal or work station. No alibis are possible.

The Key is used in an Access Management System (AMS) that can either be installed as part of a package or included into the customer's own software using a library of function calls. AMS provides identical functionality across a wide range of OSs and platforms. The software will interest users of personal computers (PCs), UNIX systems, LANs, HP3000s, IBM mainframes running MVS, CICS, and TSO (AMS can also enhance ACF2, RACF, and TOP SECRET), SUN work stations, and DEC VAX machines.

The description of SOFTBoot for Windows will serve as an overview of the general features of the entire AMS family. The use of the Key is optional and can be specified anywhere a password is demanded. Passwords can be specified for boot-up (cannot start the system at all without authorization). User IDs can be restricted from accessing any or all directories and sub-directories while minimizing the number of passwords in the system. This feature gives PCs the same powerful access controls we are used to with more evolved OSs. If fixed passwords are used, they can be forced to expire after a specified interval; they are stored only in encrypted form on the system. Repeated password failures can trigger suspension of logon privileges. The trigger count is user definable. System administration can force four levels of authentication:

- user ID only
- user ID and password
- user ID and Key
- user ID, password, and Key.

Future levels currently in development are

- smart-card token

- fingerprint scan
- voice scan.

Four security levels of users exist:

- users: allowed to change their own passwords, if any;
- admin: change their own password, list users under their authority, enrol and edit user characteristics, manage security configuration settings as permitted by owner and super levels;
- owner: install and remove the security system, enrol admin and users, change all user passwords, change all user configurations, alter global security configuration;
- super: all of the above privileges, plus automatic enrolment on all systems in an installation.

It is possible to implement time filters similar to those of large-system security tools; thus a PC might be accessible only from Monday to Friday and 07:00 to 18:00, making illicit operation outside normal office hours more difficult.

Device filters are also available: one can allow or restrict access to hard disks, floppy drives, serial ports and parallel ports on a user-by-user basis.

Anti-virus features at the DOS and BIOS levels are designed to prevent virus attachment. Prevention is the key term here. A combination of floppy disk encryption and virus protection *prevents* viruses from entering the system. In addition, the restrictions keep users from loading unauthorized software from floppies.

One can put a PC into an idle state (processor suspends) or a screen lock (keyboard and screen locked but processor continues its work). This suspension can be on user request or by timeout after a configurable period of inactivity.

Encryption is a favoured method of protecting sensitive data. SOFTBoot provides encryption facilities that can be tied to a specific Key, thus eliminating the dreaded problem of the forgotten encryption key. On the other hand, one faces the dreaded problem of the lost Key. The superuser installation allows the user who has lost the Key to gain access to the system by contacting the Help Desk and obtaining a one-time access code until the Key is replaced.

Encryption can be applied to entire disks or to directory structures. Encryption is automatic and invisible to the user and can be extended to floppy disks.

One of the most important features is the audit trail, which includes up to 24 violation types, each with time and date stamp and user ID. These violations include errors in logging on, attempting to access restricted directories, and violations of time restrictions. There are 4 levels of severity: fatal (security package fails), severe (invalid user ID), normal, and warning (e.g., idle followed by 1 password error). Unfortunately, there is no detailed record of file accesses. The manufacturer explains that logging normal events makes the log files grow excessively. Administrators will have to make do with the records on unauthorized directory accesses.
With a new option, called SOFTBoot with Scramble, access to encrypted files is audited. Scramble is designed to allow any DOS file to be encrypted and sent over any transmission medium to another SOFTBooted PC or UNIX machine set up with the Scramble software tools. The initial version uses a proprietary algorithm; however, the company plans to offer the Data Encryption Standard.

SOFTBoot for Windows 3.x and up requires a maximum of 46K RAM, of which all but 2.4K can be moved out of low memory if the PC is equipped with QEMM-386 or 386-MAX memory managers for the Windows 3.x environment. DOS a5.0 load to Hi Memory will move all but 800 bytes of the security system to high memory. At most 600 Kb of disk space are required.

A DOS version of the Windows product provides identical functionality without the icons.

The Key Cutter consists of a frame for programming up to 5 Keys at a time, a circuit board that fits into an 8-bit PC slot, and software for programming the Keys. The Cutter is itself protected by Keys, so unauthorized personnel cannot use it to generate their own Keys, and neither can anyone else. The Cutter is primed with a unique identifier at the factory, and so no two Cutters can generate identical Keys. Not even ThumbScan can duplicate a client's Keys. The database containing relevant security information used in programming the keys can and should be encrypted and Key-protected.

An Access Key costs about $75 for 1-49 keys and less for larger quantities (down to about $50 for up to 5,000 units). The Key Cutter costs about $3000 for end users and less for software manufacturers and resellers. Keys are available in stock, although enormous orders will require notice to prevent inconveniencing other purchasers. UNIX software tools cost about $2,000; large-system versions run about $5,400.

[B] Smart cards

Smart cards are tiny computers which store information about their user and interact with other computers. Applications of such cards include providing medical information about their users to all hospitals, clinics, physicians and pharmacists. For example, patients could have their most recent medical history and pharmaceutical purchases recorded on their card, thus contributing to reduced fraud and abuse of the medical system.

Such cards raise the hackles of many who are concerned with privacy. They see these devices as providing an excuse for a universal identification card that would permit increased surveillance of a country's citizens.

Security applications include secure authentication. At the National Institute of Standards and Technology (NIST), engineers have developed a smart card which implements the Data Encryption Standard (DES) and the newer Digital Signature Standard (DSS).

In a typical application, the Advanced Smart Card Access Control System (ASACS) card is placed in an external I/O device connected to a computer system using a regular serial data communications port. Special host software interrogates the smart card and the two computers talk to each other until the authenticity of the card is established. This interaction is different every time the card is used; it is therefore impossible for someone to record the dialogue and then play it back later to gain unauthorized access.

Once the ASACS has been validated by one computer, the NIST software allows the ASACS user to access other computers in the network. The current host communicates with the new host to establish the *bona fides* of the user. This system resembles the Kerberos protocols discussed below in that a trusted agent (the software on the system where a user is already authorized) communicates with another copy of itself on a remote computer and passes on information that may authorize the user to access the second system.

In addition to providing single-logon features, ASACS also allows files to be "signed" using the DSS. The ASACS card can generate such a signature using a *private key.* This system allows the recipient to confirm the originator of any signed message. The ASACS allows the recipient to decipher signatures on files that are received; it does so by using a published *public key* assigned to the sender. As discussed in the chapter on encryption, this is an example of a public key encryption system.

One of the most important features of the smart card is that it can demand a personal identification number (PIN) from its authorized user and check it on the spot. Thus a smart card stolen by a thief who doesn't know its user's PIN is useless. The smart card communicates with the computer system which authorizes access; it can therefore be inactivated by the host computer if there is reason to believe the device has been stolen.

[B] Kerberos

At the Massachusetts Institute of Technology (MIT) in the early 1980s, project Athena aimed to wire the entire campus. As the network moved towards integrating LANs with the original IBM and DEC UNIX hosts, security became a nightmare. The computer scientists at MIT developed Kerberos (named after the three-headed dog guarding the gates of hell in classical mythology) as a way of controlling access to multiple systems and resources.

Kerberos puts the power of authorizing logons in a security program running on a central system, the *Kerberos Server,* which stores encrypted passwords for all authorized users in the entire network. This server provides a mechanism for any *Kerberos-equipped* computer system on the network to authenticate a request for specific services (e.g., logon, file access privileges, use of peripherals).

When you log on to a work station, it sends your ID to the Kerberos Server, which checks its list of IDs to see if you are allowed to logon at all. The Server then issues a *Ticket* that is unusable without the password that you supplied at logon time. Because the Ticket is encrypted, an eavesdropper cannot do anything with the stolen ticket unless they can guess your password. Your work station decrypts the encrypted Ticket and stores the contents of this Ticket for future use. You are now logged on to your work station.

The contents of the logon Ticket include a special *Session Key* and a *Ticket-Granting Service Ticket* (TGS Ticket). The latter is permission to use the Kerberos *Ticket-Granting Service* (TGS) which runs on the Kerberos Server. The TGS is responsible for authorizing access to any protected service on the network (e.g., access to your own files on the file server).

During your logon, the Kerberos Server sent an encrypted Ticket to the TGS containing your user ID and the Session Key.

When you try to use your files, your work station sends its TGS Ticket to the TGS asking for permission to use the File Server Service. The TGS recognizes a valid TGS Ticket and returns a special Ticket for the File Server Service. This Ticket is valid only for the requested service and only for a certain length of time.

From the legitimate user's point of view, all of this frenetic exchanging of tickets is invisible. However, Kerberos is a real pain for the nasty unauthorized user. Since there is never any exchange of unprotected, readable information among the components of the Kerberos-protected systems, there is no opportunity to pretend to be the authorized user. Because the Tickets expire (by default, after eight hours), copied Tickets are no good after a reasonable period of use. The TGS rejects any attempt by a work station that does not have the correct combination of network address and Session Key.

Kerberos provides the opportunity for secure access to multiple systems if they are all running Kerberos software (available in source code from MIT and also in various commercial OSs).

Garfinkel and Spafford (1991) point out that Kerberos is not perfect. A user who obtains a valid password can impersonate its legitimate user without any interference from Kerberos. This is not Kerberos' fault--it's true of any system which does not provide additional authentication functions such as biometric verification or extensive private-information profiles.

[A] Authorization

Once a user has logged onto a system, how are resources protected by the OS or by add-on security packages?

All security systems define various operations which are controlled. For example, file security software can restrict read (get information from a file), write (modify a file), append (add to the file), lock (flag a file to control concurrent access), execute (loading a program to run it), and save

(creating a new file) functions. Such privileges can also apply to devices such as tape drives, entire disk drives or partitions, communications ports (e.g., modem pools), printers, and so on.

[B] Security matrix

Many OSs and security programs protect files against unauthorized access with a security matrix. For example, under the MPE OS of the HP3000 midrange computer family, users logon as *user.account,group* (I write these terms in italics to distinguish them from the normal meanings, including "user," which refers to the human being using the *user.account* ID). The *user* ID is associated with a specific *group* in a particular *account*. Files reside in *groups.* These terms are equivalent to directory *(account)* and subdirectory *(group)* in other OSs such as DOS, OS/2 and UNIX.

To logon to an *account*, the user must choose a *group*--either the *user* ID's *home group* (if one has been specified) or some other *group*. By default, if the user does not specify a *group* at logon time, the *user* will logon in its *home group*.

At logon, each *user* is defined as qualifying as an ANY *user* for all *account*s on the system, as an AC *user* with respect to its logon *account*, and as a GU *user* with respect to its logon *group* and also its *home group.*

In addition to relative categories such as ANY, AC and GU, *user* IDs are also assigned capabilities such as *account manager* (AM), *account librarian* (AL), and *group librarian* (GL).

Each *account*, *group* and file has a security matrix which specifies what each type of *user* can do within or to it. For example, *account*s can allow read (R), write (W), append (A), lock (L) and execute (X) functions to specified *user* classes. An *account* which specifies R,W,A,L,X:AC permits only *users* which have logged onto that *account* to do anything at all to the files in the *account's groups.* An *group* with security matrix R,L,X:ANY;W,A,S:GU permits any *user* logged onto the system to read, lock and execute files in that group but allows only a *user* actually logged into that particular *group* to modify or create its files.

By having permissive screening at a higher level of the directory hierarchy and more restrictive conditions at lower levels, it is possible to control access to specific *groups* within an *account* and certain files within a *group.* For example, by default, MPE defines a PUB *group* in every *account.* PUB, by default, has a security matrix of "R,L,X:ANY; W,A,S:GU." The SYS account on every HP3000 has an *account* security matrix of "R,L,X:ANY; W,A:AC." Therefore any file left in PUB.SYS can be read by any *user* on the system. I am amazed and amused at how often I have found batch job files containing logon passwords in PUB.SYS in systems I have audited. Security specialists fight a constant battle against storing passwords on disk in any case, but leaving them in a public *group* is just silly.

This security matrix system is pretty limited in the discrimination among *users.* You're either an AC *user* or an ANY *user.* If you have to allow access to a specific file by *users* logged into certain *accounts* but not to others logged into different *accounts,* you're out of luck. Similarly, if you want

to allow access by only certain *users* logged into the *group* where they've all logged on, you can't do it using the security matrix.

MPE includes several mechanisms for getting around this problem. It is possible to assign a specific class-identifier called a *local attribute* to each *user* and then programmatically check this value when the *user* tries to open a specific file. However, the *local attribute* is difficult to administer and is rarely used. Another approach uses the *lockword,* which is simply a password applied to each file that requires special protection. The *lockword* is a clumsy mechanism that requires human intervention or special programming.

The *creator* of a file (the *user* which first saved the file on disk) can release that file from its security matrix. Forgetting to secure released files is a common source of compromised security.

MPE includes a design decision that allows inference about what a *user* normally works with: anyone can list the names and size features of any file on the system. Most other OSs show this security flaw, too. Ideally, it should be possible to restrict how much information can be obtained about areas of the system to which a *user* is supposed to have no access.

[B] Access control lists

A different and much simpler approach for securing resources uses *access control lists* (ACLs). These are lists that the security software maintains for every file, database, or device. Suppose you want to control access to a specific printer used for payroll. You define a *user* called PRTCHECK in the ACCTG *account.* By assigning that printer an ACL of "W:PRTCHECK.ACCTG," you ensure that only that *user* can write to the printer. If file GENDATA has an ACL of "R,W:@.ENGNG; R:SUPV.@" (where @ is a wild-card symbol meaning, in this context, all *accounts*), then every *user* logged onto account ENGNG can have full access to GENDATA. In addition, any *user* called SUPV in any account can also have read-only access to GENDATA.

ACLs thus provide much more subtle discrimination among *users* than the security matrix described in the section above.

On the HP3000, there's an additional permission that addresses the issue of inference. The RACD flag grants a specific *user* or group of *users* the right to read the ACL (called access control definitions under MPE) of a specified file. Otherwise, no one but system supervisors can read ACLs.

[B] Access limitations

Some systems further restrict what a user can do on the system after logon. For example, you can prevent access for any individual user ID or group of IDs as a function of any combination of access port, terminal or network ID, time of day, day of week, and company and legal holidays. For example, it may be acceptable for any of the accounting staff IDs to logon only from 07:00 to 18:00 Monday to Friday on terminal ports numbers 32 through 46.

[B] Process controls

At a deeper level of the OS, security must apply to regions of memory and to drivers used for controlling peripheral devices. What is to stop a program from reading from and writing to any sector on a disk drive regardless of security restrictions? How does a multi-user OS prevent concurrent users from reading and writing in each other private memory work areas? The answer resides in the kernel (central code) of the OS.

In the simplest implementation, there are two *modes* of functioning; e.g., user-mode (less powerful) and kernel-mode (more powerful). Kernel-mode is also called *privileged* mode. Certain *objects* are classified into *protection domains*. When an ordinary program is executed, the OS creates a *process* (the unique execution of a particular program at a particular time by a particular *user* on a specific processor) which is tagged with the user-mode flag. If the process tries to read or write objects in the protection domain restricted to kernel-mode processes, the OS refuses access. When the user-mode process calls system routines, the OS temporarily assigns kernel-mode privileges to the process; thus a user program can nonetheless call privileged routines such as database-access functions or hardware drivers without putting the system at risk.

More sophisticated security schemes have more than two levels of security. MULTICS, for example, was designed with up to 64 *rings* of process domains.

One of the most serious problems with MS-DOS and the Macintosh OS is that they were never designed with multiple processes in mind. They therefore lack process-level security controls. It is this historical accident that has allowed so many viruses to spread among microcomputers.

When managing multi-user OSs, it is critically important to prevent users from acquiring privileged mode unless they are entitled to supervisory rights. For example, under MPE, each process has a *capability mask* that resides in a section of its private work area (stack) in memory. A user who acquires privileged mode can modify anything in memory, including her own capability mask; thus any user with privileged mode can acquire system manager rights.

[A] Security software

Each platform requires its own security software. Proprietary OSs have security features, but many users have chosen to supplement the basics with third-party security software.

Here are features that count in security software:

- Switch-on protection: forces the software to be invoked at boot time and prevents someone from bypassing security by booting from a floppy drive instead of from the hard disk. Some products disable the Control-Alt-Del key combination. Several microcomputer products include a hardware device that is installed inside the processor cage. Mainframe and midrange security systems are tied to the OS autologon features that invoke programs when a user logs on.

- Logon restrictions: exclusion after repeated errors.
- Password management: configurable length, content, pattern exclusions, expiration, one-way encryption.
- Audit trail: records of all logons and logoffs, file opens and closes (including failed attempts to open files that are restricted).
- Access rights: controls on reading and writing files, file groups, subdirectories, directories, and partitions.
- Selective access by user, function, or file.
- Copy protection: preventing files from being copied to or from diskette.
- Screen locking: including automatic and manual lock-setting options.
- OS access control: restrictions on reaching the OS prompt keep users in selected applications and utilities.
- Number of users: options on how many people are permitted to have user IDs for a specific microcomputer.
- Dual passwords for users and system administrators: emergency and supervisory access in case of irregularity or emergency.
- File encryption: ability to make files unusable without knowing a secret encryption key.
- NIST Digital Signatures: ability to authenticate documents using the DSS encryption algorithms.
- Documentation.
- Ease of use.
- Ease of administration: installation, configuration.
- Cost and value for money.

[A] Forgotten passwords

Even the best-trained staff can make a mistake. What happens if you forget the system supervisor password? One approach is to keep a secure copy of the password in escrow. You write down the password, store it in an opaque, envelope, and lock it up in a corporate safe or a bank vault.

Arrange to have procedures in place so that at least two top officers be required to sign for the password to be released.

Another approach is to use password retrieval software. Several packages provide protection against the irritation of losing the encryption key for word-processing documents and spreadsheets. Other utilities allow access to secured Novell NetWare LANs. Naturally, it is critically important not to allow unauthorized users to use such software. You might even consider making unauthorized *possession* of system-cracking tools to be a serious breach of security at your sites.

[A] Artificial intelligence

When authorized users gain access to the system, they usually perform predictable chores. The finance department users tend to work in the payroll and accounting databases. It would be highly unusual for such a user to attempt to obtain root or supervisory privileges or to scan files to look at their security status. Artificial intelligence (AI) programs can be designed to warn supervisory personnel that something odd is going on in a session. AI is already being used successfully by phone companies to help trap misuse of customers' telephone services. If no one at a specific company ever calls, say, Baluchistan, then a spate of calls to Baluchistan from the customer's phones will spark a warning call from the telephone carrier to the account manager. Yet another application of AI to security involves using neural networks to form models of typical typing style (transition times between letters) for authorized users and then monitor how actual users of a computer are typing in their pass phrase. Even if the pass phrase is known to an unauthorized user, they won't get access to the system.

It will be interesting to see when such software can adapt to the many duties of the programming staff and keep a watchful eye on our systems without squawking out excessive false alarms.

CHAPTER NOTES

1. Recent readings on password policies:

Anonymous (1991). Secure networks: Baseline Software's Password Coach screening software for Novell NetWare. *MIDRANGE Systems* 4(21):38

Anonymous (1992). IBM explains how to avoid an obvious password--it's as easy as one two three. *Computergram International* #CGI06190013

Anonymous (1992). NIST proposes new standards for creating secure passwords. *Government Computer News* 11(23):6

Barkes, K. G. (1992). Common-sense security. *DEC Professional* 11(4):94

Berndt, R. (1991). On guard: DataLynx Guardian security system offers painless password and profile control. *DG Review* 12(4):33

Bishop, M. (1992). Foiling password crackers: often the weakest link in the security chain, passwords need to be carefully chosen to make them uncrackable. *UNIX World* 9(3):85

Davies, C. & R. Ganesan (1993). BApasswd: a new proactive password checker. *Proceedings of the 16th National Computer Security Conference* (Baltimore, MD, Sep 20-23, 1993). National Institute of Standards and Technology & National Computer Security Center. P. 1.

Duncan, T. (1991). Password Coach secures login procedure; random number generator creates hard-to-guess, easy-to-remember passwords. *LAN Times* 8(17):42

Ehrmann, D. (1992). Securing applications: how you can implement password protection and keep track of who's using your Paradox application. *DBMS* 5(3):17

Jainschigg, J. (1994). The unbreakable password: how to defend yourself against voicemail predators. *Teleconnect* 12(10):172.

Leichter, J. (1991). VMS mythconceptions: passwords. *VAX Professional* 13(4):23

Miller, D. B. (1991). Sleep tight: Monterey Software's SAF/3000 lets MPE system managers rest easier. *HP Professional* 5(12):24

Nieland, M. E. (1992). VMS password security: The password security features n VMS version 5.4 and creation of a VMS password policy. *DEC Professional* 11(6):24

Riley, W. D. (1992). Safe as a bank: network security. *LAN Technology* 8(5):29
Rosch, W. L. (1992). Security is best achieved with multilevel passwords: Software Buyer's Guide--LAN Email. *PC Sources* 3(11):476

Salamone, S. (1991). Hard-to-guess passwords a critical key to security. *Network World* 8(42):21

Simpson, C. (1991). The enemy within: Software Review--Penta's Auto Sign-Off, Auto Passwords, and Auto Log security softare for the AS/400. *MIDRANGE Systems* 4(22):35

Stallings, W. (1994). Password generation by Bloom filters. *Dr. Dobb's Journal* 19(8):119

Vaughan-Nichols, S. J. (1991). Unix security: tighten any loose bolts. *Computer Shopper* 11(11):742

Weibel, B. (1993). Batten down your Mac: security is essential. *MacWEEK* 7(30):63

2. On a clever technique for temporarily saving and then restoring a user' password on OpenVMS systems:

Seshadri, S. (1993). A utility to save and restore a user's passwords. *Digital Systems Journal* 15(2):16

3. About multiple systems, single logons and hand-held password generators:

Cummings, J. (1991). Firm offers pack to ease system access across nets: Pyramid Development Corp.'s Single Sign-On data security software. *Network World* 8(50):13

Foster, E. (1992). A log-on by any other name would be just as confusing. In: Enterprise Computing--An Editorial Supplement. *Infoworld* 14(12):S74

Hinners, B. (1991). Changing passwords on multiple servers. *LAN Magazine* 6(7):18

Krill, P. (1995). NLM to link NetWare 3.x, DCE; IBM device will provide single log-in. *InfoWorld* 17(17):60

Lewis, J. (1995). Single log-in solutions elude network developers. *PC Week* 12(12):N32

Power, K. (1993). Smart cards and public keys unlock crypto's potential uses: More powerful microchips let agencies move away from simple passwords. *Government Computer News* 12(3):75

Smalley, E. (1993). IBM packages internetwork security technology. *PC Week* 10(50):37

Weitz, M. S. (1991). An overview of handheld password generators. *Datapro Reports on Information Security* report #IS36-001-301.
Willett, S. (1994). Proginet will bring NDS to mainframes in 1994: to give NetWare PCs single log-on. *InfoWorld* 16(12):43

4. Recent analyses of Kerberos:

Anonymous (1992). Kerberos adds install script. *Digital News & Review* 9(20):21

Anonymous (1992). Kerberos software: OCSG/Kerberos, authentication software from the Open Computing Security Group. *LAN Computing* 3(10):54

Bobrowski, S. (1994). Database security in a client/server world. *DBMS* 7(10):48

Fisher, S. (1992). Kerberos: network-security ally: but too few versions exist to tell whether interoperability problems will arise. *CommunicationsWeek* (387):45

Garfinkel, S. & G. Spafford (1991). *Practical UNIX Security.* O'Reilley & Associates, Inc. (Sebastopol, CA). ISBN 0-937175-72-2. Appendix D: "How Kerberos Works', p. 445 ff.

Haber, L. (1992). Needed: security battle plan: Distributed computing architectures are proliferating without a master plan and standards for security. *CommunicationsWeek* (408):42

Harrison, B. T. (1991). Securing with Kerberos. *DEC Professional* 10(9):106
Harrison, B. T. (1992). Opening the gates on Kerberos: while Kerberos has earned its reputation as an excellent security system, PKC is being championed as an alternative. *DEC Professional* 11(6):46

Kay, R. (1994). Distributed and secure. *Byte* 19(6):165

McNutt, D. (1992). Who are you? Kerberos system's authentication processes. *UNIX Review* 10(11):46

Morgenstern, D. (1994). AuthMan opens Mac door to Kerberos security. *MacWEEK* 8(23):10

Muftic, S. & S. Morris (1994). Security architecture for distributed systems. *Computer Communications* 17(7):492

Padovano, Michael (1990). Kerberos software guards your network. *Systems Integration* 23(10):29

Ratcliffe, M. (1993). Open Computing unleashes Kerberos on Mac networks; Security system patrols TCP/IP. *MacWEEK* 7(11):20

Schoeniger, E. (1992). The MultiNet safety net: with support for Kerberos, TGV's MultiNet provides VMS users with secure access to TCP/IP-connected hosts. *DEC Professional* 11(6):16

Scott, K. (1991). Encryption schemes put safety first: Analysis of the Kerberos and RSA Cryptosystem encryption schemes. *Data Communications* 20(4):17

Stallings, W. (1994). Kerberos keeps the enterprise secure. *Data Communications* 23(14):103

Sjogren, S. (1992). A bite out of LAN crime: LANs, MIT's Kerberos security system. *LAN Magazine* 7(7):S21

Taber, M. (1993). Can Kerberos really make UNIX secure? *Datamation* 39(1):59

Violino, B. & Klein, P. (1994). A dogged security model. *InformationWeek* (466):42

5. For understandable introductions to operating systems security theory and implementation:
Tanenbaum, A. S. (1987). *Operating Systems: Design and Implementation.* Prentice-Hall (Englewood Cliffs, NJ). ISBN 0-13-637406-9. xvi + 719. Index. Section 5.5, "Protection Mechanisms," p. 289 ff.

6. Reviews of platform-specific security packages or operating system features that confer access privileges to files:

Annesley, A. (1991). Security software: Buyer's Guide. *PC User* (154):125

Anonymous (1992). Save hosts from unnwanted guests: security. Software Buyer's Guide: Remote Control Communicatons--Putting you in control. *PC Sources* 3(5):513

Appleton, E. L. (1993). Network security: Is your LAN a sieve? *Datamation* 39(17):79

Cobb, S. (1991). Security software: Buyers Guide. *Which Computer?* 14(9):64

Conliffe, A. (1992). Who goes there? Test team finds only a few access controls products measure up to user needs. *Network World* 10(1):37

Dennis, K. (1993). The Windows Sources catalog: Buyers Guide. *Windows Sources* 1(3):483

Dern, D. P. (1992). Who's using your LAN? Local area network security products Buyer's Guide. *Datamation* 38(12):104

Eckhardt, R. C. (1991). Solving your security worries: Buyers Guide. *Macworld* 8(6):122

Graham, M. (1991). Methods for controlling access to LAN Manager; share-, user-level security provide different services. *LAN Times* 8(19):49

Grevstad, E. (1993). Mission critical: disk, file and data-saving utilities: Buyers Guide. *Computer Shopper* 13(3):586

Heim, J. (1991). Antivirus and security products: Buyers Guide. *PC World* 9(7):245

Horner, S. (1994). Safety in numbers. *DEC User* (April 1994):23

Lindholm, E. (1994). Tools for remote LAN access. *Datamation* 40(7):66

Matthews, N. (1992). Security programs help stamp out snoops: Four shareware security utilities. *San Jose Mercury News* p. 3F (Nov 8, 1992).

Schreiber, T. (1991). VMS kernels: access modes. *VAX Professional* 13(5):34

Wasson, G. (1992). Crime stoppers: Security shareware and freeware Buyers Guide. *MacUser* 8(3):112

Stevens, L. (1994). Software helps net admins balance security and access. *MacWEEK* 8(22):35

Weibel, B. (1993). Batten down your Mac: security is essential. *MacWEEK* 7(30):63

Whitehorn, M. (1992). Security software: Buyers Guide. *PC User* (177):116

7. What to do if a user loses a password:

Anonymous (1991). MasterKey utility unlocks passwords: New Visions Unlimited Partnership's password recovery utility. *MacWEEK* 5(10):6

Anonymous (1992). Password recovery: NTPASS password recovery program from AccessData for the Netware network operating system is a NetWare Loadable Module. *LAN Computing* 3(9):49

Cummings, S. (1992). Locked out of your Network? AccessData holds the key. *LAN Times* 9(21):89

McCormick, J. (1991). Cracking that lost password easy as 123: Access Data Recovery Service's WPPass, 123Pass and XLPass. *Government Computer News* 10(3):17

Meneses, P. (1993). Bypass your password: How to bypass the password to a Windows screen saver. *PC-Computing* 6(4):260

Parkinson, K. L. (1992). Utilities open password-protected data files. *MacWEEK* 6(28):16

8. Interesting articles on pattern recognition for identifying potential breaches of security:

Eliot, L. B. (1995). Typing your ID via AI. *AI Expert* 10(1):9

Eliot, L. B. (1994). Data highway needs fuzzy logic. *AI Expert* 9(1):9

LaPlante, A. (1993). Bank's expert system acts as fraud watchdog in currency exchange. *InfoWorld* 15(4):54

Newquist, H. P. (1994). Weathering the test of time. *AI Expert* 9(10):42

Wallace, B. (1992). Xiox wields AI in war on toll fraud. *Network World* 9(43):1

Zeichick, A. L. (1992). Is that really you, Dave? *AI Expert* 7(8):5

<<end of chapter>>

LAST MODIFIED: May 22, 1995
NCSA Guide to Enterprise Systems Security
File: CH_07_C.WPD
Chapter 7: Backups and data integrity

Objectives:
After studying this chapter, the reader should be able to
1. Estimate the costs of backups.
2. Determine optimal frequency for backups.
3. Use calculations of expected value in judging backup strategies.
4. Decide how long to keep backups in archives.
5. Select appropriate software and hardware for cost-effective backups.
6. Evaluate the importance and quality of offsite storage.

[A] Introduction to Data Integrity

Data integrity is at the core of enterprise systems security. If data are corrupt, why bother running programs, generating reports, and paying information systems staff?

On a visit to a client, I had to wait for a few minutes before being admitted. I chatted with the secretary. "How often do you do backups," I asked, in my continuing informal survey of operations practices. "What are backups?" she asked. "Uh, you know, where you make a copy of files in case you have problems." "Oh, that!" she exclaimed in relief. "The computer does them for me." Imagining that she meant there was an automatic backup, I enquired, "Oh? How does it do that?" "It always makes .BAK files when I save something," she answered cheerfully. "How long have you been using this computer," I asked. "Two years." "And what will you do if the hard drive breaks?" Stunned, she gasped, AIt can break?@

Data can be damaged by

- users (e.g., a user destroys a block of text and overwrites the original file)
- operators (e.g., an operator restores old files on top of the current versions)
- software (e.g., a bug in an application program adds the wrong increment to a field in 20,000 records)
- hardware (e.g., a disk head crashes into the disk surface)
- disasters (e.g., a tornado steals your disk drive).

Here are two more case studies. I watched as a PC user copied a file to a diskette and then erased the hard-disk copy. "Where's your backup?" I asked. "Right here," he answered confidently. "No, I mean where's your backup? Where's the second copy? You just destroyed the original and now you seem to have only one copy. Therefore it's not a backup any more." "What do you mean?" he asked in perplexity. "This is my backup because it's on a floppy. What do you mean by backup?" Turned

out the technician who had trained the poor fellow had simply told him that a backup was any copy on a floppy but had never explained why to make backups.

Incidentally, this case illustrates how important it is to give users sound reasons, not rote formulas, when explaining procedures such as how to do backups. Without a conceptual schema to make sense of copying information to floppy diskettes, the user--not a stupid man by any means--simply never grasped the purpose of his actions. Making a backup had become a ritual with unclear purpose.

As a systems engineer, I sometimes had to help users recover from major system problems by recommending a reload. This meant copying all the disk files to tape, reformatting the disks, and then restoring the files. Many times, I had to remind system managers to make double backups before wiping their disks. Otherwise, as they realized when I pointed it out, they would be at the mercy of their tape drives. One error could cost them a file; several errors could wipe out their only copy of their system.

[A] Definitions

For the record, here are some plain definitions:

- a backup is a second copy of programs and data.
- a full backup copies the entire contents of data storage.
- an incremental backup copies all the files which have been modified since a specific date--usually the date of the last full backup.

[A] Cost/benefit analysis

Operations managers should be able to answer at once when upper management asks the following questions:

- How often do we take system backups?
- How much system availability do backups cost?
- How much do our backups currently cost us?
- If backups are so important, why don't we backup more often?
- If backups are so expensive, why don't we do them less often?
- How long do we keep backups? Why not longer? Why not discard them sooner?
- Where do we keep backups? Are they safe? How much does storage cost us?

Backups require tapes, cassettes or optical disks. For simplicity, I'll refer to tapes throughout. So in addition to tapes, backups also take tape storage, tape drives, operator time, and system down time. The following table shows a typical calculation of backup cost for a medium-sized data centre. The details of specific cost are not important; you should estimate your costs and fill them into an equivalent spreadsheet model yourself.

Cost Factor	Estimate	Notes
Tape Costs		
Tapes/Backup	12	2.6 Gb @ 6250 bpi
Purchase Cost/Tape	$10.00	2400 Ft Reels in Bulk
Storage Cost/Tape	$3.00	Including Rack, Floor Space
Tape Cost/Backup	$156.00	Total Cost * Number of Tapes
Backup Cycles Saved	31	6 From Current Week Each Saturday Set 2 Months Month-End for 12 Months Each Year-End for 5 Years
Cost of All Tapes	$4,836.00	Sets * Total Cost
Time Costs		
Hr/Tape for Backup	0.2	
Hr/Backup Total	2.4	
Cost/Hr for Operator	$10.00	(Salary + Benefits)/Hr
System Cost/Month	$30,000.00	Purchase, Finance, Maintenance, Floor Space, Electricity, Air Conditioning, Insurance, System Management Services, Software Licenses and Maintenance
Days Used Per Month	26	
Hr/Day Availability	22	
Cost/Hr System	$52.45	
Time Cost/Hr Backup	$62.45	
Total Cost/Backup	$218.45	Tapes + Time

Annualized Costs

Backups/Yr	312	26 Days/Mo * 12 Mo
Total Backup Hrs/Yr	749	
Time Cost/Yr	$46,760.73	
Total Investment/Yr	$51,596.73	Tape Costs + Time Costs

[A] Frequency

If you have never calculated the cost of your backup strategy, the above exercise may be a shock. Now that you know roughly what backups cost, you can address the issue of backup frequency.

In the example used above, the hypothetical data centre performed a daily full backup. What if there were only one full backup every two days? One a week? One a month? The total number of tapes used and stored would decline, as would the labour and computer costs. The next chart shows the summary cost for our example as a function of interval between backups in days.

Frequency	Annual Cost
Daily	$51,597
Every Other Day	$28,216
Once A Week	$12,030
Once A Month	$6,634

The cost of backups naturally falls as the frequency declines, although not linearly. So why not reduce the number of backups to, say, one per year? Intuitively, we answer, "Because the risk would be excessive." We balance risk and cost to find the optimal backup strategy. Most of us have no idea how to calculate the optimal backup frequency, and that's what we are about to do in the following discussion.

A measure of value that integrates risk is known to statisticians and MBA graduates as the "expected value" of a strategy. The principle of expected value is used all the time by familiar institutions such as insurance companies and lotteries. The expected value is the average gain (if it's a positive quantity) or loss (if it's negative) that participants will incur in a process that involves random events.

For backups, the principle is summarized by the following equation:

$$E(x) = P(y) * C(y) - P(n) * C(n)$$

where

x is some particular strategy such as doing a daily full backup

E(x) is the expected value or cost of the strategy

P(y) is the probability of having to use the backup; e.g., 1 chance in a 1000 or 0.001

C(y) is the money saved by not having to redo all the work that would otherwise be lost if there were no backup; e.g., the cost of paying for 30 people's time for 3 hours @ $10/hr each as they input the previous day's data ($900)

P(n) is the probability of not having to use the backup = 1 - P(y) = 0.999

C(n) is the cost of doing backups that aren't used (e.g., $218.45).

The expected value of doing a single daily full backup (using our figures) is

E(x) = 0.001 * $900 - 0.999 * $218.45 = ($217.33).

In other words, the daily full backup has an average cost of about $217 per day when the likelihood of its use is factored into the calculations.

Suppose you backed up only once a month under the same circumstances. What would the expected value of your strategy be?
The first problem is that you have been told the probability of disaster only for a single day. To calculate the likelihood of at least one disaster in any given period of days, you can use the following reasoning:

The chance of a disaster in a single day is P{1}.

The chance of not having a disaster in a single day is therefore 1 - P{1}.

The chance of having no disasters in all n days of a period is (1 - P{1})^n.

Therefore the chance of having at least 1 disaster during a period of n days is [1 - (1 - P{1})^n].

In our example, where P(1} was taken as 0.001, the probability of at least one diaster during a 30-day period is 1 - 0.999^30 = 1 - .970430 = 0.03

As a simplification, pretend that the cost of recovering the work of 30 days of work were simply 30 times the cost of recovering a day's work (i.e., 30 * $900 = $27,000). Then the expected value for the monthly backups is

E(x) = 0.03 * $27,000 - 0.97 * $218.45 = $810 - $211.90 = $598.10

In other words, on average, the once-a-month backup strategy will save you almost $600 per month when the cost of recovery is factored into the equations.

Not surprisingly, the less often we do backups, the less they cost us. At some point, the quantities become zero and then become positive, as in our example. You can't expect to make money by using backups, but you can at least make these often-hidden costs conform to the rest of your insurance expenditures (including maintenance fees). You can get an idea of the minimum backup frequency by finding the interval between backups that results in a zero expected value.

These examples illustrate the reasoning which allows us to weigh alternative backup strategies. However, no one can actually estimate precisely how much a disaster costs nor compute precise probabilities for something as nebulous as "disaster." Nonetheless, the figures provide a ballpark figure with more credibility than the usual lame explanations of backup strategy.

People choose to do backups more frequently than a strict minimum for many reasons, include the following:

- custom (daily backups are a fact of life at many institutions)
- irrecoverable data (e.g., real-time data capture during scientific experiments or high-volume order entry)
- legal liability that could bankrupt the organization (e.g., loss of data at a service bureau resulting in punitive damages by hundreds of different clients)
- severe disruption with long-term consequences to the organization (e.g., loss of registration data for 20,000 students in a university at the end of a long day assigning classes).

In many organizations, the volume of changes follows a seasonal pattern. For example, 80% of all orders taken might come in two two-month periods spaced half a year apart. Registration for colleges occurs mostly in the autumn, with another bulge in January. Boat sales and ski sales follow seasonal variations. Despite this obvious variability, many organizations follow the same backup schedule regardless of date.

It makes sense to adjust the frequency of backups to the volatility of your data: more backups when there are lots of changes and fewer when the data are relatively stable. Perhaps you should do a full backup twice a day during the really heavy season.

Because different applications may have different seasonal patterns, some operations managers carry out application-specific backups. In large data centres, it is commonplace to backup an entire database before launching batch jobs which update records. If the system crashes in the middle of the update, the database will be corrupted--but the backup means you can just start over by restoring the initial conditions and launching the batch job again from the beginning.

[A] Logging

Even if you're not doing massive batch updates, you may want to carry out more backups more frequently on your more active files than on the system as a whole. The problem is that most backup methods lock your files so the users can't get at them while they're being copied to tape or other medium.

A transaction is a set of changes that must all be completed to make sense. For example, if a data entry clerk receives an order from a new customer, the transaction may consist of adding the customer information, creating an order-header, and adding the detail lines for the order. If the system or program were to fail in the middle of such a transaction after the customer were added and just as the order header were being added, the database could contain a fragment of the information required. To minimize the window of vulnerability, DBMS usually include a two-phase commit. First the user prepares a complete transaction and checks it; then the DBMS writes all the changes quickly into the database.

But what happens if the system crashes right in the middle of the quick update? The database will be logically or physically corrupt. The database is logically corrupt when all the information can be found correctly by the DBMS but it doesn't make sense (e.g., the total cost for an order might not match the actual sum of the costs of line items). The database is physically or structurally corrupt if the DBMS itself cannot find its data correctly (e.g., you could get line items from different orders mixed up together in a printout of a single order).

One solution is transaction logging and recovery. You start with a synchronization step in which you shut off access to your database, copy the database to a backup medium, initialize a log file and a launch a logging process. When you enable access to the database, the logging process intercepts all calls to the system routines which write to (modify) the database and copy information about the changes into the log file. This process is usually invisible to users and programmers alike; in many database management systems (DBMS), logging requires no changes to the application code. Logging can handle more than one database at a time simultaneously, so interrelated databases are usually no problem to log and recover.

What happens if the system does crash? You restore the initial conditions: copy the backups you made in the synchronization step back to disk, and then start reading the log file to know what to change to bring the system up to the last complete transaction. Roll-forward recovery marks the beginning and end of transactions in the log file. The recover program looks ahead to see if there's an end-marker to match a beginning-marker; if the transaction is complete, the changes are rolled into the database. If there is no end-marker, though, it means the system crashed in the middle of that transaction; therefore, the steps that were taken are not forced on the database.

If there's a long time between synchronization steps, the log file (or files) can represent many transactions. Recovering all these changes through roll-forward methods can take a long time. Therefore, another approach has become popular: roll-back recovery. In this method, the recovery program scans the log file to locate the incomplete transactions (those interrupted by the system crash or program abort) and removes the changes that make the database corrupt. Since there are typically only a few changes in incomplete transactions, roll-back recovery is very quick.

Log files provide other advantages beyond recovery. Not only can they serve as security log files (who did what to which record when?), but they can even provide statistics for performance analysis and optimization. For example, which modifications are the most frequent? How long did each transaction take? Are they forcing extensive changes to little-used index fields? If so, you might want to remove the unnecessary indexing. If your logging allows read accesses to be recorded, you can learn even more about what's going on in your database. Why was Ralph reading the salary database last night after hours? How often do people do serial reads on this dataset? Is this index being used effectively?

[A] Less intrusive backups

TYMLABS is a firm specializing in HP3000 utilities, including BACKPACK, which performs system backups. TYMLABS surveyed its client base in May 1992 to determine what portion of down time (system unavailability) was due to backups. The 200 respondents indicated that, on average, their systems were available 81% of the time, with 16% down time for backups and 3% due to other factors such as scheduled maintenance and unscheduled system halts and crashes.

If 16% of system time is due to backups, that means that backups are the single most important reason for system unavailability. Any reduction in backup time will have a major effect on system availability. Backups have become increasingly important because average storage capacities have exploded--per device, per system, and per shop. For example, when I started working for Hewlett-Packard in 1980, HP still sold 7906 disk drives: washing-machine sized units that held (gasp!) 20 Mb of formatted space. Today, you can put 20 Mb and more on a 1.5" diameter battery-powered unit that fits into hand-held computers. Oh--and the cost of the HP7906 was $25,000 (and that's in 1980 dollars).

Today's goals for backup technology, according to Chuck Stern of TYMLABS, include

- faster backups
- reduced operator intervention
- physically smaller backup media
- remote-system backups.

[B] Data compression

To shorten backups, software engineers have turned to techniques of data communications: data compression. The idea is to represent data in a more compact form than usual.

In ASCII, each character is represented by a byte: 8 bits. However, 8 bits can represent 255 different characters: the "extended" character set that is defined differently by different manufacturers of computer equipment and peripherals. The basic set of 127 ASCII characters can fit into 7 bits. Therefore the 8th bit is "wasted" in ordinary ASCII text. By turning a stream of bytes into a bit stream, it is thus possible to compress this type of data by 1/8 or 12.5%.

Another easy data compression technique much used in backup technology is zero/blank compression. Much commercial data uses flat files in which each record has the same length whether all the space is used or not. Empty parts of the record can be padded with blanks or with zeroes, depending on the data type of each field. By substituting a zero-count and a blank-count for each set of padding characters, software can significantly compress the data stream. For example, in commercial databases and word-processing documents, compression ratios of 3:1 or higher are often achieved. That means that the final space used by a compressed file can be as low as 20 or 30% of the original space.

Image data typically contains a great deal of blank space or other repeated sequences. Huffman encoding is an extension of the idea of zero/blank suppression. It counts the occurrences of repeated sequences and creates a table of shorter equivalences. Decompression entails substituting the original values for each occurrence of the codes. Such approaches can result in very high compression ratios as a function of how sparse the file is. For line drawings, for example, 100:1 compression is not unusual. This approach--substituting counts for any kind of repeated sequence--helps keep spreadsheets to manageable sizes by implementing sparse-matrix technology.

More complex, heuristic data compressions such as the Limpel-Zev-Welch (LZW) algorithm adapt to the changing characteristics of the data stream. For example, LZW compression keeps a table with string sequences and substitutes a shorter symbol or pointer to a symbol. As the data stream continues, a tuned table develops which allows the specific text to be encoded more efficiently. If a table is used to keep track of the compression symbols appropriate for specific files, the compression process can become faster with repeated applications.
Drivers are available for automatic disk compression on PCs; such disk compressors double the available file space and work completely transparently. For other systems, there are software packages which compress entire databases and still leave them readable by normal applications. Some compressors also allow writing to compressed databases.

Microcomputer shareware compressors such as ARC and PKZIP have enough features to serve as good backup utilities. For example, I use ARC to write 88 Mb of hard disk data to 44 Mb Syquest cartridges without problems. On another microcomputer which I carry with me on trips, PKZIP in a batch file lets me bundle up all modified files into a single compact file which I can upload to CompuServe as a backup.

[B] Streaming tape drives

Sometimes, if a disk drive is badly fragmented (i.e., when pieces of the file such as clusters or extents are scattered over one or many disks), I/O slows down. Each head repositioning requires a seek time to locate the correct cylinder of disk and then a rotational latency while the disk spins around and positions the desired sector under the read/write head of the disk assembly. Seek and rotational latency are much slower than the disk's transfer rate; for example, it can easily take 20 ms (milliseconds) to position the head for a transfer, compared with only about 1 ms for the actual transfer.

When a processor cannot supply its backup device with enough data to keep the backup going, the backup cannot just go on indefinitely with null output: the cost in tape or other medium becomes

too large. The backup must be interrupted while the medium is repositioned to resume writing in the appropriate place when the data stream resumes. Streaming devices use data buffers to smooth out the data flow. These buffers can be part of the hardware or they can be borrowed from system memory.

Another approach to smoothing out the data stream is to send copies of disk instead of copies of files. In the UNIX and DOS worlds, for example, IMAGE or TAR backups send entire disk copies to tape. These backups are fast to write but slower to read. They require special software to piece together the appropriate sections of data to form entire files; some older packages actually have to reconstitute an entire disk drive rather than allowing individual file access.

[B] Unattended backups

If an operator has to change units on the backup storage device, the cost of backup increases. In addition, human intervention increases the error rate, either because of inattention or because of inadequate training. Mounting tapes, cartridges, or optical disks is boring. To solve this problem, large centres have used tape silos and robots: large arrays of tapes equipped with robotic arms to mount and dismount the proper volumes under computer control. With the advent of cartridges, several manufacturers developed auto-changers similar to audio-cassette automatic players. Optical disks are typically mounted and controlled by juke-boxes, so named because they resemble old-fashioned record juke-boxes.

All of these methods cost money, but the payback can be quite short. For example, if the cost of ownership (purchase, maintenance, insurance, financing) of a juke-box is $50,000 over three years and an operator costs $25,000 a year including salary and benefits, it won't be long before the organization is saving money--even excluding the cost of error avoidance.

My own preference is to move night operators to an overlapping shift at the busiest part of the day. For example, the 08:00-16:00 shift and the 16:00-24:00 shift can often use a helping hand between 14:00 and 20:00. Firing night operators instead of benefitting from their experience and knowledge can be a mistake.

[B] Online backups

All of these backup methods still require the users to get out of their files before the data are copied to a backup medium. Users with experience in microcomputers and small networks sometimes have no conception of the size and speed of larger systems. In the microcomputer world, sustained data transfer rates of 5-10 Mb/sec are considered high. At that rate, transferring 1 Gb (10^9 bytes) would take only 100 seconds. However, transferring 1 Tb (10^12 bytes) would take more than 27 hours. Intel's PCI chipset is reported to provide up to 133 Mb/sec, so that 1 Tb backup could shrink to 2 hours.

One solution to the delay caused by locking users out of files during the backup is to allow them to keep accessing their files despite the copy operation. This approach means that the changes made after the backup program has copied a section of the active files must be recorded later. Such online backup tools keep a log file of changes and store that file on the tapes too. When restoring the files

to disk, the online backup software integrates all the changes with the stored versions of files to generate the actual form of the file at the end of the backup. With such software, it is possible to reduce system down time to about 5 minutes for initial synchronization of the tape and the log files.

An intermediate sort of technology that depends on large amounts of free disk space is to send the data to a gigantic disk file instead of to tape. Then during the day, when operators are available, the data are copied to the backup medium. This method consumes CPU, memory and bus bandwidth and can impede normal daytime processing.

[A] Disk mirroring

In disk mirroring, a special disk driver copies all the changes intended for one disk drive onto another "mirror` disk. Large fault-tolerant systems such as TANDEM and STRATUS computers have used such systems for years. In recent years, there has been much excitement about RAID devices (redundant arrays of inexpensive disks), which provide large capacity with fault tolerance and a high data transfer speed.

There are five levels of RAID, and the cost rises with the degree of fault tolerance. The Chapter Notes provide references to extensive reviews of current technology.

One application of disk mirroring for speeding up backups is that you can backup one of the copies of the data without interfering with online access. During the backup, no changes are permitted in the disk being backed up; all changes are logged in a file. When the backup is complete, the changes are installed into the mirror disk. As in the disk-based online backup method, such backup strategies must be examined to be sure that they do not adversely affect online performance.

[A] Retention of backups

How long you keep backup tapes depends on the data. Data that are legally required for audit purposes must be kept as long as the appropriate laws and regulations stipulate. However, as discussed below, magnetic media are not eternal. If magnetically-stored data are to be perfectly recoverable in the long term, you'll have to copy them to fresh media about every three years.

Archival information from databases should be stored with the relevant application programs and possibly even the operating system (OS). A few years from now, it may not be possible to read the files under the new versions of the application system, database management subsystem, or OS. You may even have trouble finding hardware that will run any of this old software.

Data stored on tapes and cassettes may be difficult to locate unless you keep careful records of exactly what's on which tape. One good practise is to send all backup listings into disk files as well as onto paper. These electronic lists can themselves be stored for rapid access using any editor or word processing package. For more sophisticated lookups, you can enter the file/data/reel data into a database and find answers even more quickly.

One alternative to storing the raw data and the programs is to format the output in readable text files (ASCII, EBCDIC) that can be printed out on demand. Or you can store the reports

micrographically using computer-output microfilm (COM). COM equipment may save you a good deal of money and space compared with magnetic tape (although multi-Gb cassettes are certainly compact) and with far longer shelf-life and greater retrievability.

Here is a sample backup retention strategy:

- o the daily full backup is immediately sent off-site
- o daily backups are kept for one week
- o end-of-week backups are kept for two months
- o end-of-month backups are kept for a year
- o end-of-year backups are kept for 5 years.

[A] Hierarchical storage

System managers always encounter a well-known law of computing: storage expands to fill the space available. No matter how much disk storage one adds to a system, users seem to be able to store enough files to use up all the free space. Hierarchical storage systems solve both the backup problem and the storage problem by automatically moving files through a list, or hierarchy, of storage types. Recently-accessed files reside on high-speed, expensive magnetic disks; older, less-used files migrate to slower and less-expensive media such as optical disks and eventually magnetic tapes. Some software systems maintain pointers to the slower media so that users are little inconvenienced by the migration. For example, back in the 1970s on the Dartmouth Time-Sharing System running on twin-processor Honeywell 6600 mainframes, I remember some files being listed in our directories with parentheses; e.g., (filename). These parenthetical names represented files we hadn=t used for a long time and which had been Amigrated@ to magnetic tape.

Today=s software usually goes further by providing disk space management such as defragmentation as well as migration to different levels and costs of storage.

[A] Verify backups

There are countless stories in the literature about sites where backups turned out to be unreadable. Always verify your tapes, especially if you intend to erase the originals. The most complete way to verify tapes is to restore all the data to disk, but this method takes a long time and poses a risk: what if the tape data are wrong? A more usual method is simply to read all the data without writing them to disk.

[A] Short- and medium-term storage of backups

Treat your backups with care. Store tapes vertically, preferably hanging. Lateral pressure on tapes can crush parts of the tapes that may protrude slightly from the main body of the reel because of eccentric winding. These folded areas of tape cause parity errors and data loss. Tapes should never

be stored in piles, because the pressure from the upper tapes can crush the ones below, which are not meant to support such weight.

Do not put backup tapes in the same room as the systems they are supposed to be protecting. This recommendation may seem too obvious to write down, but you'd be surprised at how many people think nothing of putting their latest--and therefore most important--backups right next to the computer systems.

Small shops often allow operators to take backups home with them. This is a dangerous practise for all concerned. Employees may be liable for enormous damages if they lose or damage backups that are required for disaster recovery, even if they are volunteering to render a service to their employer. Storage conditions in a home may be inadequate; I have heard of backups being kept under a bed. Backups may be left in cars in cold weather (problems of condensation when they're taken inside a building) or in hot weather (problems of melting).

Others store tapes in bank vaults. This may be reasonable for small shops, but it is virtually impossible to retrieve your tapes in off-hours even in an emergency.

Most organizations come to realize the advantage of using a good offsite data storage facility. Be sure you deal with data storage facilities, not simply archiving services that specialize in paper files. Environmental requirements are different for paper and for magnetic media. And certainly don't allow anyone to store your tapes in commercial self-store facilities designed for furniture and domestic belongings.

Verify that off-site storage facilities meet your requirements for safe storage of your backups. Check for limits on humidity, dust, and electromagnetic fields. Test the security arrangements to make sure imposters can't get your tapes. Be sure that the storage facilities are far enough away from your office that they won't be involved in a local disaster. Ensure that your tapes won't be lost: ask about how your materials will be located and how fast you can retrieve them in an emergency. Be sure you have 24 hour a day, seven day a week access.

Evaluate the delivery service that can usually be arranged along with storage. The personnel who handle your tapes should be bonded. The carriers in which they place your backups should be clean, sturdy, insulated, labelled and locked.

[A] Long-term storage of backups

Storing records is only half the task of records management; supporting availability and utility is the essential function. No one wants a WOM (write-only memory) for their records. For short-term storage, there is no problem ensuring that stored information will be usable. Even if a software upgrade changes file formats, the previous versions are usually readable. In a year, technological changes such as new storage formats will not make older formats unreadable.

Over the medium term, up to five years, difficulties of compatibility do increase, although not catastrophically. There are certainly plenty of five-year old systems still in use, and it is unlikely that this level of technological inertia will be seriously reduced in the future.

Over the longer term, however, there are serious problems to overcome in maintaining the availability of electronic records. Over the last ten to twenty years, certain forms of storage have become essentially unusable. As an example, AES was a powerful force in the dedicated word-processor market in the 1970s; eight-inch disks held dozens or hundreds of pages of text and could be read in almost any office in North America. By the late 1980s, AES had succumbed to word-processing packages running on general-purpose computers; by 1990, the last Canadian company supporting AES equipment closed its doors in Montreal. Today, it would be extremely difficult to recover data from AES diskettes.

The problems of obsolescence include data degradation, software incompatibilities and hardware incompatibilities.

[B] Data degradation

Magnetic media degrade over time. Over a period of a few years, thermal disruption of magnetic domains gradually blurs the boundaries of the magnetized areas, making it harder for I/O devices to distinguish between the domains representing ones and those representing zeroes. These problems affect tapes, diskettes and magnetic disks and cause increasing parity errors. Specialized equipment and software can compensate for these errors and recover most of the data on such old media.

Tape media suffer from an additional source of degradation: the metal oxide becomes friable and begins to flake off the mylar backing. Such losses are unrecoverable. They occur within a few years in media stored under inadequate environmental controls and within five to ten years for properly-maintained media.

Optical disks, which use laser beams to etch bubbles in the substrate, are much more stable than magnetic media. Because CD-ROMs and laser disks are still so new, no one knows how long optical disks will last; nonetheless, technologists predict that the information will remain readable for decades and more.

[B] Software Incompatibilities

Hardware is necessary for successful retrieval, and so is software.

[C] Application Software

The data may be readable, but will they be usable? Manufacturers provide backward compatibility, but there are limits. WordPerfect 6.0a can convert files from earlier versions of WordPerfect--but only back to version 4.2. Over time, application programs evolve and drop support of the earliest data formats. Database programs, E-mail, spreadsheets--all of today=s and tomorrow=s versions may have trouble interpreting data files correctly.

In any case, all conversion raises the possibility of data loss since new formats are not necessarily supersets of old formats. For example, in 1972, RUNOFF text files on mainframe systems included instructions to pause a daisy-wheel impact printer so the operator could change daisy wheels--but

there was no requirement to document the desired daisy wheel. The operator made the choice. What would document conversion do with that instruction?

[C] Operating System Software

Even operating systems evolve. Programs intended for the DOS of a decade ago do not necessarily function on today=s DOS version 6.20. And the operating systems of yesteryear do not necessarily run on today=s hardware. Even emulators can cause problems because, again, there is no guarantee of absolute isomorphism between the emulated system and the emulator.

[B] Hardware incompatibilities

Finally, over time, even hardware becomes impossible to maintain. As mentioned above in the introductory comments, it would be extremely difficult to retrieve and interpret data from word-processing equipment from even twenty years ago. In the mainframe world, no one outside museums or hobbyists can read an 800 bpi 9-track :-inch magnetic tape from a 1980 HP3000 Series III minicomputer. Over time, even such parameters as electrical power attributes may change, making obsolete equipment difficult to run even if they can be located.

The most robust method developed to date for long-term storage of data is COM (Computer Output to Microfilm). Documents are printed to microfilm, appearing exactly as if they had been printed to paper and then microphotographed. Storage densities are high, storage costs are low, and in the worst case, the images can be read with a source of light and a simple lens.

[A] Disposal of magnetic media

As discussed in the section on Dumpster diving or scavenging, you must take care to dispose of all magnetic media in an appropriate way. Overwriting with random patterns of 0s and 1s and degaussing are helpful, but the most secure method of preventing access to your discarded media is physical destruction. Incineration will certainly work for tapes, but you should check with local environmental protection authorities to be sure your incinerator is capable of destroying Mylar without generating toxic byproducts.

If you are trying to destroy a non-functional disk drive, physical destruction is the only method that is guaranteed to dispose of the data. A contact at the Canadian Defence Intelligence Establishment told me that discarded disk drives have the oxide removed with oxy-acetylene torches.

Now that's thorough.

CHAPTER NOTES

1. General reading about backup strategies and tools:

Anonymous (1994). Storage: 1994-1995 Buyers= Directory Issue. LAN Times 11(18):425

Isaac, I. (1985). Guide on Selecting ADP Basckup Process Alternatives. GPO: SN 003-003-02701-4. Available from NTIS (National Technical Information Service / U.S. Department of Commerce / 5285 Port Royal Road / Springfield, VA 22161 (tel. 703-487-4650 08:30-17:00 Eastern Time Zone). Also available from Superintendent of Documents / U. S. Government Printing Office (GPO) / Washington, DC 20402 (tel. 202-783-3238 08:00-16:00 Eastern Time Zone).

Negrino, T. (1995). Successful workgroup backup. Macworld 12(5):p114

Platon, J. (1994). Tape talk: automating data storage with tape is a cost-effective, long-term solution. HP Professional 8(11):S6

Sawicki, E. (1992). LAN Desktop Guide to Security: Your Network Advisor for Sound LAN Performance (NETWARE Edition). SAMS Division of Prentice Hall Publishing (Carmel, IN). ISBN 0-672-30085-0. Appendix A, "Backups and archives," p. 287 ff.

Sullivan, K. B. (1995). Backing up data move to front of the line; many differences abound in LAN-to-mainframe packages. PC Week 12(16):N3

2. On data compression:

Anonymous (1993). Coping with compression. Corporate Computing 2(5):160

Gookin, Dan (1993). Stacker and your memory manager. PC-Computing 6(4):243

Kruger, Anton (1992). Block Truncation Compression: an efficient algorithm for image compression. Dr. Dobbs Journal 17(4):48

Phillips, Dwayne (1992). Data compression using Huffman coding. C Users Journal 10(2):55

Prosise, Jeff (1993). Understanding data compression. PC Magazine 12(10):305

Ratcliff, John W. (1992). Audio compression: digitized sound requires its own compression algorithms. Dr. Dobbs Journal 17(7):32

Ross, Ed (1992). A simple data-compression technique. C Users Journal 10(10):113

Smith, Gina (1992). Free up disk space with Stacker. PC-Computing 5(3):164

3. Data transfer rates:

Anonymous (1993). Networking is a natural role for EISA. PC Sources 4(2):264

Devoney, C. (1993). A solution to the hard disk dilemma: how to shake off shackles of a stagnant drive technology. Computer Shopper 13(3):88

4. Online backups:

Anonymous (1992). Online-BACKUP+/XL requires zero dowtime. HP Professional 6(10):84

Anonymous (1992). Online backup for Vines. LAN Computing 3(10):55

Horton, J. (1992). Virtual devices deliver online backup: limitations to tape backup sway managers toward this gap-free solution. LAN Times 9(24):S25

5. Disk mirroring and RAID:

Anonymous (1993). Open storage: keen competition in the Unix environment is pushing the development of storage technology and keeping prices down. IBM System User 14(2):31

Backus, K., P. Houston, & E. Longsworth (1993). Right as RAID. Corporate Computing 2(5):60

Bauer, C. J. (1994). RAID subsystems: Buyers= Guide. Government Computer News 13(6):83

Chepetsky, S. M. (1994). RAID devices offer various levels of redundancy, tolerance (Part 2). Digital News & Review 11(22):36

Chepetsky, S. M. (1994). RAID brings fault-tolerant mass storage to host systems (Part 1). Digital News & Review 11(21):38

Kliewer, B. (1994). RAID to the rescue. OS2 Professional 2(2):33

Miles, J. B. (1993). RAID storage. Government Computer News 12(8):77

Milne, J. (1995). RAID storage solutions: Which is right for you? Network Computing 6(5):154

O'Connor, K. (1994). The benefits of RAID. PC User (246):112

O'Harra, S. L. (1994). Build an affordable RAID array for NetWare apps. Data Based Advisor 12(6):76

McCusker, T. (1994). Pick the RAID that's right for you. Datamation 40(4):79

Rigney, S. (1993). Immunity: mirroring utility eliminates downtime. PC Magazine 12(2):54

Sharp, B. (1994). RAID: now you can take your pick. Datamation 40(22):81

6. Recent reviews and tutorials dealing with PC backup products:

Anonymous (1994). Backup solutions: 1994-1995 Buyers= Directory Issue. LAN Times 11(18):7

Anonymous (1993). Windows backup programs. PC User (206):124

Bigley, T. (1992). Backup software; InfoWorld evaluates a half-dozen packages, in both DOS and Windows versions, from the three leading vendors. InfoWorld 14(22):59

Fowler, D. (1992). Backups, the shareware way. Computer Shopper 12(5):713

Guterman, J. (1992). Safety Disk backs up your configuration. Computer Shopper 12(3):629

Hill, J. (1995). Backing it up. Windows Sources 3(4):115

Kent, L. & C. Goldberg (1993). Tape backup solutions. InfoWorld 15(10):64

Kramer, M. (1992). Cheyenne's Changer option simplifies, automates ARCserve backup. PC Week 9(17):57

LaPolla, S. (1992). Backup software saves the day (and money) for Amoco. PC Week 9(12):101

Myers, B. (1995). "There must be 50 ways to lose your data, but we've got a QIC and easy backup solution." Windows Magazine 6(3):230

Reff, B. J. & D. Seachrist (1993). Windows backup programs. Computing Canada 19(5):16

Rigney, S. (1995). Don't get burned: A look at storage management solutions. Computer Shopper 15(3):595

Smith, J. (1992). Backing up isn't hard to do with Windows: eight hard disk backup programs. PC-Computing 5(10):354

7. Recent reviews and announcements of MAC backup products:

Adams, E. J. (1994). Build your own RAID. MacWEEK 8(45):66

Anonymous (1993). Utilities. MacUser 8(13):284

Bobker, S. (1992). Down to basics. MacUser 8(2):253

Cummings, S. (1994). Automated backup software offers centralized control. MacWEEK 8(33):36

8. Recent reviews and announcements of LAN backup products:

Adhikari, R. (1994). LAN storage tools take cue from mainframe world. Software Magazine 14(4):55

Anonymous (1994). Network management: Annual Buyers' Guide. LAN Magazine 9(11):185

Cavanagh, J. (1992). Smart backup within reach. LAN Technology 8(8):67

Duffy, C. A. (1993). Backup that lightens LAN managers' load: new packages offer more access to users, better file grooming. PC Week 10(10):105
Kent, L. & E. Eva (1992). Backup to the rescue: NLM backup software speedily resuscitates crashed servers. InfoWorld 14(45):84

McCusker, T. (1993). Hierarchical storage reaches the LAN. Datamation 39(24):73

Moslehi, F. (1992). Reflections on fault tolerance: when your LAN breaks, seven years bad luck is getting off easy. LAN Technology 8(1):35

Saunders, S. (1994). HSM tries to tame the LAN storage tiger. Data Communications 23(11):73

Sullivan, K. B. (1995). Backing up data move to front of the line; many differences abound in LAN-to-mainframe packages. PC Week 12(16):N3

9. Recent reviews and announcements of AS/400 backup products:

Anonymous (1995). Report archiver. MIDRANGE Systems 8(3):47

Anonymous (1994). Come and get it. MIDRANGE Systems 7(22):40

Anonymous (1993). Mirror, mirror. MIDRANGE Systems 6(24):42

Anonymous (1993). Automatic recovery. MIDRANGE Systems 6(18):64
Anonymous (1993). Teamwork: Mersch-Bacher Associates joins with IBM to offer Backup Recovery and Media services/400 for AS/400. MIDRANGE Systems 6(3):44

Anonymous (1992). AS/400 mirroring: Midrange Information Systems introduces release 3.0 of its Object Mirror System OMS/4000. MIDRANGE Systems 5(6):62

Anonymous (1992). Down with back-up. IBM System User 13(2):55

Anonymous (1991). Media Management System. Software Magazine 11(8):89

Anonymous (1991). US vendors show off storage tools; the highlights of the Systems 3x/400 Midrange Expo held in New York. IBM System User 12(11):15

Didio, L. (1992). IBM AS/400, OS/400 get performance boosts: operational assistant aids in scheduling backups. LAN Times 9(6):72

Henderson, L. (1993). Where the buck stops: keeping information available puts IBM's reputation on the line. MIDRANGE Systems 6(14):21

Simpson, C. (1992). Lean on me: Midrange Information System's Object Mirroring System back-up system for IBM AS/400 minicomputers. MIDRANGE Systems 5(11):28

10. Recent reviews and announcements of DEC systems backup products:

Anonymous (1994). Backup software goes DEC. Digital News & Review 11(3):12

Anonymous (1993). DEC Network Save and Restore, DECnsr: DEC's backup and recovery software for TCP/IP networks. Software Magazine 13(1):96

Anonymous (1992). VAX Storage Library System (SLS): datacenter features at the desktop. Digital Review 9(8):44

Nesdore, P. (1995). Legato adds to Polycenter. Digital News & Review 12(3):21

Schroeder, E. (1993). DEC division unleashes barrage of high-end storage options. PC Week 10(51):N11

Varney, S. E. (1992). Pathworks PCs gain unattended backup, restore over DECnet. Digital Review 9(8):6

11. Recent reviews and announcements of UNIX systems backup products:

Bailey, D. (1994). Backup and minor peripherals. UNIX Review 12(6):95

Bowen, T. S. (1992). Polycenter gains boost capabilities of DECmcc for Ultrix. Digital Review 9(8):4
Bowen, T. S. (1992). SI to market Unix-based net backup software. Digital Review 9(5):6

Brennan, L. (1992). NetWorker 2.0 backs up Unix, NetWare clients. PC Week 9(30):45

Burgard, M. (1992). Look before you back up. UNIX World 9(9):71

Busse, T. (1993). HP pumps up enterprise management on Unix. InfoWorld 15(19):48

Clark, C. T. (1994). StorageWorks suits Sun workstations. Digital News & Review 11(19):6

Cohen, A. (1992). Safe passage. DG Review 13(1):18

Gillooly, C. (1992). Legato rolls out NetWare, Unix versions of software: firm beefs up its NetWorker backup offerings. Network World 9(31):11

Horner, S. (1994). Judge for yourself. Computer Weekly (August 18, 1994):24

Jander, M. (1992). NetWare backup software with room to grow: Legato unveils Netware software, plans for integration with Unix package. Data Communications 21(4):103

Jarvie, B. (1992). Epoch's UNIX backup products to ship in May. Computer Reseller News (469):90

Sharp, B. (1994). Tales of the tape: backup and archiving means good business for UNIX software vendors and users. HP Professional 8(2):36

12. Offsite storage sites for backups:

Anonymous (1991). Contracting for hot sites, cold sites, and off-site data storage. Datapro Reports on Information Security report #IS38-220-101.

Balter, B. (1983). Insurance against a data disaster. Security Management, July 1983, p. 69. Reprinted in: Gallery, S. M. (1987), ed. Computer Security: Readings from ASecurity Management@ Magazine. Butterworth Publishing (Stoneham, MA). ISBN 0-409-90084-2. P. 155 ff.

13. Computer output to microfilm

Anonymous (1992). More advances to COM. Information Week White Paper (378):S1.

Edelstein, H. A. (1993). The future of microfilm. INFORM, Nov. 1993; reprinted as report 1030DIS in the Datapro Computer Systems Analyst CD-ROM for February 1995.

Taylor, B. (1994). COM giant quietly charts hybrid future: Corporate profile of Anacomp and interview with top product planner and marketer. ImagingWorld: Image and Document Management News 3(4&5).

14. Disposal of magnetic media:

Anonymous (1991). A Guide to Understanding Data Remanence in Automated Information Systems. (The ADark Green Book@ in the Rainbow Series) NCSC-TG-025, Version 1. Available from Director, National Security Agency (NSA) / INFOSEC Awareness / Attention: X71 / 9800 Savage Road / Fort George G. Meade, MD 20755-6000 (tel. 301-766-8729 in Eastern Time Zone).

<<end of chapter>>

LAST MODIFIED: April 18, 2020

NCSA Guide to Enterprise Systems Security

File: 08 Networks.wpd
Chapter 8: Voice and data networks

Objectives:
After studying this chapter, readers should be able to:
1. identify and reduce vulnerabilities in their networks.
2. analyze and prevent toll fraud.
3. end abuse of voice-mail systems.
4. warn users about the vulnerabilities of electronic mail.
5. establish policies to reduce risks in sending FAX messages.
6. protect networks against physical penetration.
7. reduce unwanted radio-frequency emanations and associated data leakage.
8. evaluate the needs for a firewall when connecting to the Internet.
9. recognize specific security issues for managing PCs and other workstations.

[A] Networks in the office and beyond

Storing information is only useful if someone can actually get to the data in a timely and secure manner. Bringing up your company's market position on screen is less useful if your competitor is getting the same information simultaneously. Communications are therefore just as important for enterprise systems security as number crunching processors and high-capacity mass storage.

Communications security includes not only data; you have to consider the security aspects of voice transmission (private branch exchanges or PBXs) and storage (voice mail systems). Electronic mail (e-mail) poses additional demands for security, as does electronic data interchange (EDI).

Communications channels vary in *bandwidth:* the capacity to carry information. Some systems now provide gigabyte/second (Gb/sec) bandwidth; the risks from uncontrolled interception of such channels grows with the volume of data being transmitted.

The following sections describe vulnerabilities of communications channels and countermeasures for protecting security.

[A] Asynchronous links

Asynchronous links (EIA 232-D and similar standards) are easy to tap. Twisted pair cabling installed for telephone use has served for data communications in many buildings. It is now common to see dual RJ-11 jacks at every desk in an office: one for voice and another (often brightly coloured) for data.

Telephone wiring was never designed with security in mind. Most systems use unshielded cables and connectors. The wires are either run externally along baseboards or are easy to find even when embedded in walls. *Fox and Hounds* by Jensen Tools consists of a tone generator and receiver kit. You clip the generator on the wires wherever they're exposed and then use the receiver to pick up an audible tone. This technique allows anyone to trace wires through walls, floors and ceilings.

Too many security managers walk right on by the wiring closets located on every floor of their building without realizing that an eavesdropper has everything required to patch tap into every phone circuit (and data line) on the floor right there in a little unprotected cubicle. In some buildings, the wiring closets aren't even locked. A tapper can impersonate phone company personnel, saunter into the wiring closet, and clip a handset into voice lines or a portable computer system into data lines without hindrance.

Once an intruder is patched into a data circuit, they can read any unencrypted data as they are sent between terminals and hosts. Even if the twisted pair is being used for 10BaseT IEEE 802.3 (Ethernet) LANs, a suitably-equipped eavesdropper can decode the data packets as they go by. In any case, without message authentication codes (MACs), it is possible for an intruder to remove transactions from the data stream or insert them for fraudulent purposes.

Front-end processors for data communications offer a perfect point of attack for information thieves. A few deft changes to the configuration via unprotected maintenance ports and the network is theirs.

Some key protective mechanisms for your asynchronous links:

- o use shielded cable: physically shielded against cutting, spiking and other physical attacks and electromagnetically shielded against signal leakage and interference.
- o protect patch panels against tampering.
- o guard your data switches against unauthorized access with the same severity that you apply to the rest of your enterprise systems.
- o encrypt critical and sensitive data transmissions (see chapter 10).

[A] Microwave relays

About two-thirds of all the switched phone calls traveling through the U.S. are sent through the 740 million miles (1.2 billion km) of microwave relays in the U.S. alone. These familiar towers, spaced about 25 miles (40 km) apart, receive, amplify and resend high-capacity signals carrying 24 to 19,200 phone calls per carrier band simultaneously.

Information on how to intercept and interpret this mass of voice and data is freely available from the Federal Communications Commission (FCC) of the U.S. You have to demultiplex the signals and then select the ones you want to interpret. The radiation is not collimated, so it spreads as it travels from one relay tower to another; by the time it reaches the target, the beam is so diffuse that it's detectable within miles of the antenna. Interception equipment may be as inexpensive as $600 or as costly as $50,000, but it is possible to acquire legally. Digital transmissions through the microwave relay system are harder for a novice to tap but are easier for professional eavesdroppers to interpret. Basically, you need equipment equivalent to that of a common carrier (phone company).

The only protection for information traveling through microwave relays is encryption.

[A] Leased lines

When you dial a phone number to call anywhere outside your own PBX, your call is *switched* through the interexchange carriers (IXC). The path each call takes is determined essentially by chance: the instantaneous load of each possible connection influences which circuit is assigned to make up the *virtual circuit* you need to reach your party. For example, in calling from New York to San Francisco, a call might go through a switching center in Chicago on your first call; if you repeated the same call a moment later, the routing might go through Denver instead. This variability explains why, in voice calls, sometimes we exclaim, "Why, it sounds as if you're next door" whereas other times we growl, "We have a bad line. Let me call you back right away.'

To avoid this kind of variable quality when sending data, many customers *lease* a line from point to point. Thus you can install a *tie line* from your New York office to your San Francisco office. The line is always open; you just pick up the phone and it rings at the other end--something like the courtesy phones at airports which automatically connect you to limousine or hotel reservation services. The IXC *conditions* the leased line by selecting routes which provide a guaranteed minimum signal-to-noise ratio. In other words, leased lines can be guaranteed to be as quiet as your data transmission requires. In addition, leased lines can be purchased with redundant routing that provides greater stability during emergencies. Finally, leased lines cost a fixed amount regardless of volume; they can be substantially less expensive than switched lines for high-volume applications.

With all this to go for them, it is too bad that leased lines are even less secure than ordinary switched lines. The fixed routing means that it's easier for dishonest employees of your IXC to tap into your voice or data transmissions at will.

Ken Shoopman, an expert in electronic surveillance countermeasures (Albuquerque, NM), explained to the April 1993 session of the *Information Systems Security* course in Denver that a phone company can agree to a

remote extension of a leased line *without bothering to check the authenticity of the request.* So a competitor can order a tap on your leased line--and have you pay for it. Shoopman recommends that you always check your phone bills to ensure that there are no unauthorized or forgotten extensions on your tie lines.

Protect leased lines the same way you protect switched lines.

[A] Fibre optics

Fibre optics are a rapidly-growing part of high-speed networks. With their enormous 1 Gb/sec bandwidth, optical fibers can carry 15,000 phone conversations over 25 miles (40 km) without repeaters; in contrast, conventional copper wires can carry only 1,250 conversations using repeaters every mile.

Fibre optic cables are difficult and expensive to tap physically without causing a tell-tale loss of signal strength. However, in the late 1980s, it became clear that stripping away the insulation and then bending the light-conducting core of a fibre optic cable through a hairpin bend with a 1/8 inch (3 me) radius allows enough light to escape that an eavesdropper can capture some of the data. True, there are usually many channels being used concurrently in one cable, so the task of sifting through the signals is not trivial. Nonetheless, fibre optic cables are unfortunately not as secure as they were once hoped to be.

Be sure you use protect fibre optic cable against physical damage.

[A] Satellite links

There are hundreds of geosynchronous satellites in orbit. At 22,300 miles (35,900 km) above the earth, these devices orbit at the same speed as the rotation of the planet; they thus act as very tall stationary microwave relay towers. Data (and cable TV and telephone) transmissions are beamed up from uplink stations and then bounced back to receiver dishes. Even when the satellite downlink is aimed at a specific target, the beam is about 50 miles in diameter when it reaches ground. That means that the satellite transmission is easily captured over an area of thousands of square miles. Interception is easy, as owners of pirate cable-TV dishes will tell you.

Since the signal strength of the normal uplinks is quite low, the satellite equipment avoids interference by locking in on whichever signal is strongest. In April 1986, 8 million TV views were startled to find the visage of a bearded lunatic suddenly interrupting their evening situation comedies. Captain Midnight, a Florida operator of a satellite uplink, managed to commandeer network TV to spout his message of abuse at the FCC for its regulatory decisions in the cable TV industry.

Users of satellite linkages (most of us, at one time or another) should consider encrypting data transmissions and even voice messages.

[A] Mobile radio, cellular phones and cordless phones

As data communications become more mobile, technologies such as wireless networks and cellular phones are increasingly finding a place in the corporate network. Wireless communications include mobile CB (citizens' band) radio, cellular phone networks, and cordless phones principally used in homes. Another form of wireless communications, wireless LANs, is discussed separately below.

Although these wireless technologies make remote communications (both voice and data) easier, they also increase the risk of security breaches.

The growing use of remote access--including especially mobile, wireless remote access--will increase security risks for networks. Several trends suggest that remote access is growing fast. For example, notebook and laptop computer sales are growing faster than sales of desktop models. Sales force automation is based on portable computers. Remote access to e-mail systems is a logical development of sales force automation. Wireless data communications services link even palm-top computers to messaging networks.

Remote access facilities allow users full network services from their hotel rooms via modems. With cellular phones dropping in size and cost, people will use modems through cellular phones. Incidentally, I'm already

frightened by people using cellular phones while they weave through traffic. The prospect of seeing them drive while trying to type responses to their e-mail systems is terrifying.

International trade competition is making confidential information ever more valuable to foreign companies and governments. Using unencrypted wireless communications will be like shouting messages from the rooftops.

For the last decade, anyone with a wireless phone at home has been an easy mark for dial-tone thieves and eavesdroppers (we can't call them wire-tappers any more). Most wireless phones have no on-off hook on the wall-mounted base station. The dial-tone is initiated on the hand-held unit. But that means that anyone nearby with a compatible handset can use the victim's dial tone to make calls--including long-distance calls. It also means that compatible handsets permit unrestricted eavesdropping. If you want to send a less unsecured transmission through your phone lines, unplug the base units of all wireless phones before calling your network.

Another problem in homes is baby monitors. These devices transmit in the same frequencies as cordless phones. Anyone with a wideband scanner can pick up everything you and your baby say to each other. In this case, the walls may *really* have ears.

Similarly, anyone thinking of using a modem via cellular phones must remember that cellular calls can be monitored using inexpensive scanners which used to be available at the corner electronics store. In most jurisdictions in the United States, these are now illegal; the Electronic Communications Privacy Act of 1986 explicitly made cellular phone calls private in all jurisdictions. However, in practice, there is a culture of eavesdroppers who still listen in on police chatter over the CB bands; they also listen to cellular phone calls. Even an old TV set with UHF bands can tune in cellular phone calls.

Although wireless transmission has always had some risk, the sheer scale of wireless communications as we enter the 21st century will bring major increases in the risk of unauthorized disclosure of sensitive data and modification of critical data.

As wireless communications become more widespread, people send and receive both critical and sensitive data via mobile units. For example, emergency medical teams can download full medical files on accident victims. Field engineers send data captured from client systems to support computers for analysis. Police routinely
download full details about any suspect to their squad car computer. Sales people in their cars upload their prospect analyses to home base for immediate discussion and receive instructions on special pricing for competitive bidding.

Given the current lamentable state of information security awareness among most network users, we can look forward to trouble as they unknowingly use non-secure transmissions around the country and, eventually, the world.

I wouldn't suggest that you use a cellular phone to do your banking, for example. It's just too easy to decode card numbers and PINs (personal identification numbers) from such transmissions.

When using non-secure transmission media for sensitive and critical data, users should automatically encrypt their transmissions. Identification and authentication should be carried out only after a secure link is in place. Secure links can be established with encrypting modems and appropriate key management technology such as hand-held password generators.

[A] Packet-switching networks

X.25 packet switching networks (PSN) such as Tymnet and Telenet in the U.S. and Datapac in Canada allow large numbers of users to share high-bandwidth channels at low cost. Data are bundled up in *packets* (usually of 256 bytes or more) and labeled with *headers* which indicate where the packet comes from, where it's supposed to go, and what sequence number it has. The interface between your computer systems and the PSN is a *packet assembler-disassembler* (PAD), much liked by communications engineers because it gives them the opportunity to ask an attractive fellow-engineer, "Well, your PAD or mine?'

PADs cost several thousand dollars and up, so they're not trivial investments for casual snoops. Nonetheless, PSN transmissions *are* sent via ordinary IXC, so it is in theory possible to intercept X.25 traffic and decode it. In practice, this is not a reasonable worry.

However, to reach a PAD, communications have to go through other channels such as asynchronous links, leased lines and LANs. The PAD itself may be connected to the PSN via a leased line. Therefore all the security measures which are mentioned elsewhere in this chapter apply to networks which include PSNs.

[A] LANs

Remember Superman, the comic-book hero with X-ray vision? One of the remarkable and admirable attributes of Superman was that although he could look all the way through concrete, he never misused his power to look through people's clothing--or at least, so the comic books claimed.

Unfortunately, local area networks (LANs) are falling victim to the electronic equivalent of X-ray vision--and these "Superusers" are looking all the way past electronic clothing and even underwear. Unencrypted LAN communications are completely open to anyone with about a thousand dollars to spend on off the shelf software.

[B] Network monitors

This story began for me when a security-conscious user spoke worriedly to me at the San Diego Annual Conference of INTEREX in August 1991. He was extremely concerned about the widespread lack of security on unprotected local area networks. He pointed out that almost all LANs operating today are completely unprotected to penetration--even with the most sophisticated access control software and hardware. Once he pointed it out, the problem was shockingly obvious. The inexplicable part is why so few seem to be worried.

The problem is the availability of LAN-monitoring software. Judge for yourself; here are extracts from a flier advertising INTEL's NetSight Analyst product:

> "NetSight Analyst fully decodes IPX/SPX (Netware), TCP/IP, and AppleTalk packets on any Ethernet network.... fully decodes packets to seven levels in tabular, English translations.... makes light work out of giving cryptic node addresses more understandable node/user names.... Build sophisticated packet filter specifications.... Helps you determine the source of a fault on the network by 'listening" to network conversations...."

These are wonderful features and should surely be available to network supervisors on every LAN in the land. However, the scary part is this brief note: "...NetSight Analyst resides on a single floppy disk, so it's always ready to travel and easy to run from any workstation."

There's the problem: an off-the-shelf program whose existence is impossible to detect can be loaded onto any work station that has a floppy disk drive and can then decode any packet going by.

That includes packets being sent from a work station using the LAN for connection to a minicomputer or mainframe. That includes packets with secure information such as the passwords used for logon/login, file lockwords, and worst of all, the encryption keys used to encrypt or decrypt secure files on the servers.

[B] Fundamentals of LAN sniffing

Let's begin at the beginning.

Most LANs in use today conform to various standards set by the Institute of Electrical and Electronic Engineers (IEEE). E.g., IEEE 802.3 defines broadband and baseband bus systems using carrier-sense multiple access with collision detection (CSMA/CD) such as Ethernet protocols. IEEE 802.4 defines token-passing bus protocols and IEEE 802.5 defines token-passing rings. All of these systems encapsulate data into packets, which contain headers (and sometimes trailers) defining origin, destination, and various attributes of the message.

Depending on LAN topology, some or all packets pass every work station (node) on the network. In connected LANs, known as internets (and further described as WANs or wide-area networks if the internets are geographically dispersed), packets from one LAN may be routed through other LANs on their way to their destinations. Destinations may include other work stations, servers, and hosts such as the HP3000 and HP9000 series of mainframes and minicomputers.

To send data along a LAN, software running on each work station encapsulates data originating at that node with appropriate headers and trailers. Similarly, to receive data from the LAN, the work station software must ignore packets being sent to other nodes and read those addressed to it. The packets then have to be decoded by stripping the headers and trailers and the contents fed to the application software.

For example, when an HP3000 is linked to a network using a LAN Interface Card (LANIC), a user logging on to the HP3000 must send a packet for each line of data (string terminated with a carriage return character, shown below as <return>). The HP3000 responds with its reply. E.g.,

user sends A<return>@ = packet 1

HP3000 sends ":" = packet 2

user sends AHELLO USER.PROD <return>@ = packet 3

HP3000 sends "ENTER ACCOUNT PASSWORD (PROD)?" = packet 4

user sends "M3H4A7L1<return>@ = packet 5.

The HP3000 does not echo this password, so it very properly fails to show up on the user's screen.

How many of these packets could be racing by each node in the LAN at any one time? It depends on LAN bandwidth and the number of users actually transmitting and receiving data concurrently.

Packets vary in size depending on type of network software and the network manager's choice of configuration value. Typically, packets run from about 256 to around 4096 bytes. So with LAN bandwidths (throughput) running from about 10 million bits per second (Mbps) on up into the 100 Mbps range and higher, one can calculate that the number of packets passing a node can be from several hundred to several thousand per second when the LAN is heavily used.

Ordinary LAN software used by ordinary users does not allow a work station to detect packets being sent to other destinations. So there's no security problem.

But what about the user who installs, say, NetSight Analyst on her work station? She can suddenly decode every single packet that goes by her work station. By selecting a particular node--say, the HP3000 system manager's (SM) work station--she can follow *every single interaction* on that work station. She could, for example, happen to be watching for the initial dialogue used in logon, including the invisible password scooting along in its little packet from the SM's work station to the HP3000.

In fact, LAN monitor software is so clever that a user can automatically trap packets according to specific nodes and specific strings; e.g., "HELLO". Such macro functions record the chosen data stream without human intervention. The log files can then be examined offline at leisure.

Without belaboring the point, the same principle applies to ANY information being sent along the LAN: database passwords, personal profile questions and answers, private e-mail, obscene responses to system error messages....

Network monitor software is read-only. It does not interfere in any way with the data stream, so there is simply no way possible for a network supervisor to tell that someone is decoding packets. X-ray vision indeed.

[B] Countermeasures against sniffing

I had a very fruitful discussion of these issues in November 1991 with Bob Bosen, Senior Scientist at Enigma Logic, Inc. (2151 Salvio Street, Suite 301 / Concord, CA 94520 / Phone 510-827-5707 / FAX 510-827-2593). He sent me a booklet entitled, *There are only 5 ways to configure LAN security... and 4 of them don't work!* which he will send you if you ask him nicely. Without repeating his work, it's easy to summarize the main message: only work station-mediated encryption can prevent a user of network monitor software from reading your transactions.

- Access control on work stations? Once logged on to the work station, all its traffic on the LAN is wide open to the network monitor user.
- Access controls on servers? A network monitor lets the user see your passwords and authentication codes.
- Encryption on the server? The cleartext data move over the unprotected LAN.
- Encrypting LAN cable? Data are encrypted before being encapsulated and decrypted after the packet is transmitted, so the network monitor won't see anything readable. However, once the data leave the cable, they're unprotected.
- Encrypting file system? Data are encrypted at each work station. Only encrypted data are transmitted across the LAN to servers. If the data need to be decrypted (as for example by an HP3000 or a shared printer), the decryption can be carried out on a secure node immediately before transmitting the cleartext data to the destination.

Enigma Logic manufacture SafeWord PC LAN-safe, which includes transparent encryption and also virus detection functions for MS-DOS systems using LANs. According to the specification sheet, this product requires 25Kb RAM on the work station and takes 1 Mb disk space. It can be configured to protect specific subdirectories. Managers can define different access rights for different user classes. Files and directories can be protected against unauthorized modification (write-protection). Encryption can use a variety of algorithms, including DES, DES TURBO, TURBO, and ELI. DES and DES TURBO are not exportable due to US government restrictions.

Encryption speed depends on processor speed; the spec sheet states, "Processors running at 10 MHZ and higher are generally able to use DES encryption...without inconvenience. All of the other encryption algorithms are at least 10 times as fast as DES and provide reasonable performance even on XT-type PCs."

SafeWord PC LAN-Safe is said to function correctly with Novell, 3Com, Banyan, DECNET-DOS, IBM Token-Ring, and other network operating systems.

In summary, unless network managers take special precautions, any LAN is entirely open to eavesdropping using widely-available network monitoring software. Preventing access to confidential information traveling through LANs requires work station-mediated encryption.

[A] Wireless LANs

Combining the advantages and disadvantages of wireless communications and LAN protocols, wireless LANs have become more popular as the century draws to its close. Using infrared light or radio frequencies, these techniques offer special benefits for applications where mobility is important. For example, I have seen wireless communications at work in a modern paper mill where mobile robotic forklifts trundle through the factory carrying equipment and products without human intervention.

Another good place for wireless communications is temporary accommodations or historical buildings where it is either uneconomical or illegal to break up the walls, ceilings and floors to lay cable.

Even in normal offices, it may be cost effective to use wireless LAN connections (either standalone or as adjuncts to an existing wired LAN) if there are work stations to be situated in areas that have no cabling in place.

From one pont of view, wireless LANs are the worst possible medium for carrying sensitive information: the data are *broadcast* through the work area. Infrared systems are limited to line-of-sight transmission but radio-frequency systems can penetrate normal walls and some floors. Radio LAN linkages are interrupted by structural steel and metal sheaths; they are attenuated by concrete.

Spread-spectrum technology, on the other hand, is actually *more* secure than normal LANs. Spread-spectrum radio transmission was refined during the 1950s and classified for military use only. The technology was declassified in the 1980s and has been used since then for commercial applications. In spread-spectrum transmission, frequency-agile modems send bits to each other in a constantly-changing sequence of frequencies. Without having precisely the right equipment, the radio transmission sounds like low-power noise. The chances of a casual hacker having the right equipment to reassemble spread spectrum transmissions are negligible; however, there's nothing to stop a determined eavesdropper from joining your wireless network--possibly even from outside your office or building.

[A] Powerline spread-spectrum LANs

One more type of LAN medium has entered the field: electrical power lines. There are products which plug into your electrical system and send data at modest speeds (2 to 19.2 Kbaud) through existing wiring. Transmission is spread-spectrum to avoid interference from other equipment plugged into the electrical system (motors, fluorescent lights and computers). Indeed, one of the reasons the bandwidth is still low is that the spread-spectrum implementations break bits into fragments called *chips.* There can be 31 chips per bit--each chip being sent at a different frequency and then reassembled into bits at the destination.

As in wireless spread-spectrum LANs, this method of communications is hard to crack. For all practical purposes, the data are encrypted. On the other hand, there's nothing to stop a proficient criminal hacker with physical access to your building from adding an unauthorized node to your powerline LAN.

[A] Toll fraud

What's the single most widely-distributed interface for computer systems on our planet? Keyboards and monitors, right? Wrong. The most widely-distributed mechanism for interacting with computers is the touch-tone phone (TTP).

In a narrow sense, TTPs can actually connect us to computers as we normally think of them. For example, you can call up Federal Express and request one of their couriers to drop by the office to pick up packages. You dial their phone number and a voice tells you to punch "1" or "2" and so on in response to specific questions. Do you want a package picked up? Punch 1. Do you want to talk to an attendant? Punch 2 or wait a few moments without doing anything. Is your package ready for shipment now? Punch 1. Enter your account code. Enter the number of packages. Enter the approximate weights of the packages. And so on. If there were a modem port available, you could do exactly the same using a terminal, only the questions would appear on your screen and you'd answer with your own keyboard (or mouse, or touch-screen....). In this sense, the TTP is just another data entry device.

However, there is one kind of computer the TTP is *really* good at reaching: telephone switches.

Telephone switches route calls through public carriers (e.g., AT&T, MCI, Sprint) and through private branch exchanges (PBXs) in large and not-so-large companies. These switches are all specialized computers. And they can be abused.
John Haugh and his colleagues have invested over 9000 hours in research on the problems of toll fraud and telabuse. Their two-volume report serves as a landmark text to help enterprise systems managers protect their organizations against potentially enormous costs. The summary that follows is based on that report and on presentations arranged by Mr Haugh for the telecommunications security track at the June 1993 conference of the NCSA in Washington, DC.

[B] Extent of toll fraud

Haugh *et al.* define toll fraud as the theft of long-distance services by an unrelated third party. That is, someone you don't know makes expensive calls that you end up paying for. The total losses are impossible to

estimate precisely because of under-reporting, but they amount to somewhere in the $2B-$9B range per year--and the total is rising rapidly.

With the widespread distribution of Direct Inward System Access (DISA), employees of companies with special telephone switches, voice mail systems, and voice-response systems (generically referred to as *customer premises equipment* or CPE) can get access to outside lines. This *outbound access* can include wide-area telephone services (WATS), tie-lines to other switches in a company network, and plain local calls. With uncontrolled access to the local exchange, employees and intruders can call long-distance carriers and make toll calls that are charged to the employer. If such uses are rationed correctly, the CPE owner can actually save money compared with allowing employees to use phone credit cards. The credit cards usually incur a surcharge (e.g., the highest possible operator-assisted rate) whereas the calls routed through the CPE get billed at the lowest possible rates.

Of course, the whole cost/benefit calculations goes down the tubes when thieves begin using the CPE.

Toll fraud falls into three categories:

- *First party* toll fraud involves insider collusion; e.g., employees sell authorization codes to crooks.
- *Second party* toll fraud involves employees of long-distance carriers or other telephone service providers.
- *Third party* toll fraud involves criminals who gain codes.

Here are some of the more spectacular cases of toll fraud cited in Chapter 5 of Haugh *et al.* and elsewhere:

- Mitsubishi International's New York office experienced $400,000 of stolen international calls in two weeks in July 1990.
- Over the period from August 1990 to March 1991, Avnet, Inc. was saddled with $750,000 in phone charges, of which $500,000 were generated in a single weekend in September 1990.
- Chartways Technology of Rockville, MD, was informed on March 31, 1988 that someone using its CPE had placed $42,935 of calls to Pakistan via AT&T--and an additional charge of $49,768.34 from another phone carrier.
- A call-sell operation charged more than $1.4M in stolen phone calls through a single PBX in a single four-day weekend.
- Prisoners have tricked hospital switchboard operators into patching them into long-distance lines to South America by claiming to be doctors with an emergency.
- Criminals have called switchboard operators and claimed to be top executives calling from cellular phones. In 90% of the cases studied, they succeed in getting an outside line through the CPE.

In his NCSA conference presentation, Haugh cited a case in which a single toll-fraud criminal was found to earn $900,000 a year (tax-free) from organizing second-party theft of authorization codes. He paid a clerk at the phone carrier head office $2,000 a week for just two new stolen phone-switch passwords at a time.

Thomas Crowe, an attorney specializing in communications affairs, reported at the NCSA conference that 70% of all U.S. companies have been victims of telephone fraud; average bills were $75,000. He quoted an unnamed phone-company official who stated, "There are only two kinds of telephone company customers: those who have been victims of phone fraud and those who will be victims.'

[B] Who pays?

First of all, inter-exchange calls have to be routed through the web of interconnecting phone carriers all over the planet. Each one charges different rates for calls routed through its equipment. These bills have to be paid by the upstream carrier. The originating carriers have to pay real money to the downstream phone companies. So the originating carrier definitely sees a cost for every long-distance call outside its local calling area.

In the U.S., jurisprudence dating back into the early days of telephony has long dictated that phone calls initiated on a subscriber's phone are the entire responsibility of the subscriber. For example, if a sneak-thief who has broken into your house pauses during his depredations to make a phone call to France, it's just too bad: you're liable for the cost of the phone call.

When the carriers *rented* CPE to subscribers, jurisprudence could reasonably hold that the carrier was responsible for toll fraud charges. However, in the late 1970s, when the Supreme Court ordered divestiture of the regional Bell operating companies (RBOCs), the liability shifted from the carriers to the subscribers. From that point on, it was possible for businesses to *buy* and *own* their own CPE--and so the responsibility for the use of that equipment fell onto the subscribers. Of the seven federal court cases decided to date (June 1993) in the U.S., all have ruled against the subscriber and in favour of the carrier.

But it gets worse.

Criminals know that the phone companies can trace calls quickly and accurately. Therefore there's a surcharge for *looping* calls through several switches. A criminal will call switch A, get an outbound line, route the call through switch B, get an outbound line, call switch C, and only then call some distant country. The owner of switch C gets nailed with enormous bills (sometimes there are so many illegal calls that the detailed invoices have to be delivered in cartons).

During the course of investigation, it becomes clear that the owners of switches B and A also shared some responsibility for the fraud: they didn't protect their switches, either. Therefore the owner of switch C can name the other CPE owners in a civil lawsuit to demand restitution of part of the expenses.

[B] Who steals?

Who's doing all this toll fraud? Calling patterns are suggestive. Over 80% of all stolen phone calls are placed in New York City. Most of the illegal calls are placed to Panama, Bolivia, Colombia, Pakistan, and several other South American countries where illegal drugs originate. The rest are mostly to the 809 area code (Puerto Rico and other locations), to the Caribbean area, and Mexico.

Analysts think that the purchasers of stolen phone services fall into three categories:

- criminals involved in the drug trade: these people don't like using their own phones because they know that the FBI and other law enforcement agencies currently have some 15,000 legal wiretaps in place.
- illegal immigrants who can't risk signing up for phone services because the paperwork could flush them out of hiding.
- poor folks who can't afford long-distance rates but still want to phone home.

As a result of these demographic patterns, phone companies are beginning to ban long-distance calls from pay phones in certain heavily immigrant neighbourhoods in New York, Chicago, Los Angeles and Toronto. A recent news story reported that the Nippon Telephone and Telegraph Company has closed down long distance credit-card calls from phone booths in certain neighbourhoods. The toll thieves are thus not only harming their victims, they're also causing inconvenience for honest people in their neighbourhoods.

The organizer of a call-sell operation was interviewed by Haugh and his colleagues. With an MBA from an Ivy-League college, he looks like a yuppie businessman: lives in Connecticut in an expensive house and has a nice family who have no idea what he does for a living. In his college days, he used to run a cocaine ring--but decided that it was too dangerous. Now he has happy, relatively peaceful employees (the people with stop

watches who time the calls they steal) and feels that he's doing something nice for people. It's not addictive, it doesn't get anyone killed, and he helps folks reach out and touch someone.

He also knows that the chances of being punished for his theft is negligible. As Thomas Crowe pointed out in his presentation, the toll fraud artists are not caught; they're not prosecuted when they are caught; they are not convicted when they are prosecuted; and they are not punished when they're convicted. Judges in New York City won't even look at cases with under $1M of damages; since the law makes it possible to convict someone only if there's overwhelming evidence beyond a reasonable doubt that the suspect is indeed guilty, law enforcement is often limited to capturing peons. Hours of waiting and watching may bring in a paltry dozen users who each stole about $25 of phone time; the person with the stopwatch and the phone access codes is more difficult to catch. The organizer of the ring is almost never caught.

[B] Who's responsible?

There's plenty of blame to hand around. At the toll-fraud user end, there are people who see nothing wrong with stealing phone time. They see their actions as victimless crime; they think that the carriers own the equipment anyway, so it doesn't actually cost anybody anything to borrow some spare capacity. As we saw above, this naive view of some impersonal machine without human victims is just plain wrong.

Some users and toll-fraud organizers are simply criminal minds who don't care about laws or about the companies they may be putting out of business. Either they're sociopaths or they come from cultures with a profound contempt for social values.

Vendors of CPE must take responsibility for part of the problem. Of 90 manuals studied by Haugh and his team, *not a single one* included information warning about phone fraud. Sales staff from these suppliers explained candidly that they didn't want to scare customers away from buying their equipment, so they never talked about toll fraud and countermeasures. However, Haugh sees a change in attitude, and new CPE manuals do include information about such fraud.

Phone companies are accused of being too slow to warn customers that they are under attack. Hours can go by while thousands of illegal phone calls are made. This problem is also being addressed by the carriers. Robert Carman, Operating Manager of the Network Monitoring Center of AT&T, spoke at the NCSA conference. He reported a series of measures to protect customers.

NetPROTECT basic services are available to all domestic 800 number subscribers. Measures aimed at reducing toll fraud include

- network monitoring that tracks 41 high-fraud locations throughout the U.S.
- near-real-time information: notification of the victim within a couple of hours.
- 800 lockout, which can block a hacker's phone from dialling AT&T 800 numbers.
- a security hotline available 24 hours per day, 7 days a week.
- improved support for law enforcement officials to increase arrests, indictment, and conviction of phone fraud criminals.

Over 10,000 customers had been trained by the end of 1992; the program has reduced average losses by 75%; over 2,500 phone *phreakers* (from phone + freak) have been thrown off the AT&T network for 6 days or more; and over 1000 customers a month are being informed of the theft of their long-distance services.

Additional services are available for a fee. For example, Advanced Monitoring Service

- limits customer liability to $25,000 per incident.
- cuts customer liability by 50% if the customer notifies AT&T of the fraud first and the customer shuts down its long-distance accesses within two hours.

Premium service provides the same as Advanced Monitoring and in addition covers 100% of all abuse of AT&T 800-number inbound lines. It requires an 11-digit minimum DISA password length.

CPE owners and user are shockingly lax in applying common-sense security to their valuable services. Users don't read manuals and they still don't know about the vulnerability of unprotected phone services or the enormous risks they're running.

[B] Preventing toll fraud

Haugh provides advice for preventing 95% of all toll fraud:

- Start by deactivating or blocking remote access (DISA).
- Block all international calls outright, or at the very least block calls to the most popular destinations for toll fraud: The Dominican Republic and the 809 area code, Egypt, Pakistan, India, Russia, El Salvador, China, Colombia, Mexico and Ghana. You can do so by programming your own CPE and by using registered mail to demand that your phone carrier block such calls.
- Block casual calls to long-distance IXC (special numbers). For those employees who really need to call foreign countries, supply phone-company credit cards. Although each call will cost more than if it had been placed through the CPE, the risks of abuse are lower. Be sure to train your credit-card users to block the line of sight to their phone keypad if they're entering their card numbers and personal identification number (PIN) in public. Remember that shoulder-surfing gangs throng public areas and are on the lookout for card numbers.

  Unfortunately, the Federal Communications Commission forces organizations who serve transient populations (e.g., colleges and hospitals) to allow access to the outside IXC. One college racked up over $400,000 in fraudulent charges within a few weeks of opening up their system to allow casual calls to outside carriers.
- Block access to all system ports (through which your CPE can be programmed by phreaks who know your PBX instruction manual better than you do).
- Implement automatic restrictions on when long-distance calls can be placed through your PBX; 80% of all toll fraud occurs between 18:00 Friday and 08:00 Monday.
- Configure voice mail systems to access outside phone lines.

In addition to these simple measures, you can also install special protective software and hardware on your CPE. The most immediate anti-abuse method is the *aggressive system,* which listens to the voice of a supposedly-authorized caller. Using voice-recognition technology, this system bars imposters (or authorized users with bad colds...) from the PBX. Another type of device is known as a *reactive barrier.* For example, Xiox Corporation's Fort Knox line of microcomputer software includes *Hacker Preventer,* which watches how people are using your PBX; any deviation from the normal activities registered for a specific employee sparks an alert to the network manager. An example of *passive response* is *Hacker Tracker,* which generates useful reports on system activity that can help pinpoint abuse without having to wait for the IXC notifies you. *Hacker Deadbolt* is a special card you can install in the PBX to control access to the remote maintenance and testing ports.

[B] How to respond to toll fraud

The first thing to do when you receive crates of phone bills is to shut down the mechanisms which are being abused. Cut off outbound long-distance calls, warn your operators about imposters, and change your control codes and passwords.

Although you are legally bound to pay bills for fraudulent use of your phones, you do have some bargaining power. The phone companies will generally cooperate in reducing the damage by up to 30% if you ask them to. You can negotiate with the IXC and demonstrate that you do have adequate security. Involve the CPE

vendor in your discussions, with the implication that they might be involved in further proceedings if they don't help pay for the damage. You can file informal or formal complaints with the FCC about how badly you have been served by the carriers and your CPE provider. What you probably should *not* do is sue the IXC and the CPE vendor. Your chances of winning are low and the costs can be astronomical.

[A] Voice mail

Protecting information stored in a voice mail system should be part of the enterprise systems security mandate. Clients can leave orders by phone; suppliers can warn of delivery delays; prospects can request information. These data can be just as valuable as any other kind of data.

On 1-2 September and then on the weekend of 5-7 September 1991, phone phreaks attacked the voice mail system of Logitech, Inc., makers of the famous computer mouse. They deleted about 20 messages left on the sales line. A few days later, the phreaks erased messages in 100 mailboxes (out of a total of about 600). Not content with this damage, the phreaks had the gall to leave messages on how they cracked the system. It hadn't been hard: most users had mailbox passwords identical to their own extension number (a system default--and well known to phreaks). On computer systems, such password/mailbox combinations would be known as Joe accounts and are strictly forbidden.

In a case I alluded to in Chapter 2, two teenagers caused $2.4M of damage to a NJ publisher by trashing their voice mail and wiping out advertisers' instructions.

Other cases have been reported where hackers and phreaks have invaded voice mail systems like parasites, installing their own mailboxes without the consent of the equipment owners. The phreaks then use the parasitized system to leave messages for each other.

All of these cases could have been prevented by simple-minded security provisions analogous to the access-control methods used in other computer systems. No default passwords, no Joe accounts.

Voice mail systems also usually allow special codes to switch a call to an outside line, with predictable results when toll-fraud criminals get control of the voice mail system. The same principles as described for PBX security apply to voice mail computers.

There's another aspect to voice mail beyond the issue of outsider abuse. Walter Houser pointed out that inappropriate use of voice mail can lead authorized users into trouble. Some of his advice:

- o phone calls are temporary, but voice mail is forever.
- o voice mail can even be forwarded to other or multiple recipients.
- o the lack of feedback when you deliver a voice mail message may lead you into inappropriate speech style or content that would quickly have changed had a live person been on the other end of a real conversation.
- o voice mail can fall into the ears of unfriendly listeners more easily than ordinary untapped conversations.
- o therefore, don't leave voice mail when you're angry.

[A] Electronic mail

The same problems you face with voice mail exist with e-mail. Users can mistakenly *flame* their colleagues in the heat of a conflict. Flaming is common among novice or immature users on the Internet and other networks and is generally frowned on. Nuances are even harder to communicate in writing than in phone messages; that clever, sarcastic remark can look like a raging insult to a reader with a different mood and context. A sly joke that has you chuckling at lunchtime with your friends may look like crass vulgarity to a colleague who has just come out of a serious conference with the boss. Although these issues may not count as security problems in the narrow definition of the term, misuse of e-mail does damage human communications.

[B] E-mail is forever

E-mail makes it incredibly easy to make spectacular bloopers. In a case reported in a session of the *Information systems Security* courses, a user at a major corporation sent a love letter to another employee in the company through the e-mail system. Unfortunately, the sender pressed the wrong key and sent his message to the entire company through an automatic mailing list. Even more unfortunately, the sender was a married man. Even more unfortunately than that, the intended recipient was also a man.

In general, when an e-mail message is sent, it is impossible to recall it--just like paper mail (derisively called *snail mail* by e-mail aficionados). Unlike paper mail, it's virtually impossible to destroy the original; even when people delete the copies in the e-mail network, there are usually backups in which the deleted messages can be recovered.

[B] My mail or the company's?

Another issue that applies to both e-mail and voice mail is intra-organizational privacy. Are the communications which cross your e-mail network *personally private* or only *company private?* It's not an easy question. Consider the following anecdote, told on the Interet ethics list (ETHICS-L@vm.gmd.de) in December 1992: someone at one of the major TV networks asked a manager his opinions of why a certain show was suffering in the eternal ratings battle. The manager responded candidly by e-mail and specifically requested that his critical message not be shown to the crew of the show in question. However, the e-mail system suffered a glitch which removed security from all the messages in storage. Other users riffled through the manager's files and discovered his analysis. The breach of security resulted in hard feelings among the cast and crew.

The *Electronic Communications Privacy Act* of 1986 (ECPA) specifically does *not* protect the privacy of e-mail in private e-mail networks. If a private organization sets up a network, it can legally establish a policy that allows supervisors to access employee messages. The absence of legal strictures does not, however, imply that managers *ought* to invade their employees' privacy. If the organization protects the privacy of phone conversations, voice mail and correspondence marked PRIVATE AND CONFIDENTIAL, then the same rules should be applied to e-mail.

If employee privacy is not guaranteed, it is important to establish this principle openly to avoid misunderstandings and lawsuits. If the company explicitly warns its employees that their e-mail system is to be used for business only, employees can assume that their communications may be monitored. Reasonable people will then act accordingly.

In a discussion on the USENET ETHICS-L discussion in Dec 1992, one correspondent pointed out that e-mail has many similarities with snail mail. Employees do not, for example, expect confidentiality when they send mail through reusable envelopes that cannot be sealed. The commentator recommended that managers always reserve the right to examine any message *in the process of managing its system.* He pointed out that this reservation will protect management against suits if they happen to see messages unintentionally.

Another correspondent responded with the cogent comment that restrictions on personal use of e-mail (and phones) can become onerous impositions that sour the employee-management relationship. Such effects on personnel morale can become as costly as the personal use that has been avoided. This person emphasized that just because managers *can* read other people's e-mail, it doesn't follow that they should.

These are not academic discussions without practical import. In 1990, a group representing 2,500 employees of Epson America sued in Los Angeles Superior Court for damages of up to $3,000 *each* because they allege that Epson invaded their privacy. It seems that Epson managers regularly printed and read the internal e-mail and external MCI Mail of the employees at their Torrance, CA facility.

In 1991, two ex-employees of Nissan Motor Corporation launched a lawsuit against their former employer for invasion of privacy and wrongful dismissal. They claimed that Nissan managers had monitored their electronic correspondence with dealers throughout the U.S. and had criticized them for some of the sexual innuendos that the *dealers* sent the two women. When the women protested the criticism and objected to the unannounced monitoring, they were fired.

[B] Privacy and the Internet

What happens to privacy when your e-mail leaves the confines of your home network and wanders through the Internet? The ECPA *does* address privacy in public networks (e.g., the Internet, CompuServe, Prodigy, GEnie). All e-mail messages are strictly protected except under named circumstances such as legal authorizations from law enforcement authorities and system maintenance. Even when messages are accessed, however, they are not legally divulged to others. However, that doesn't mean your messages are safe. With messages often going through two, three or more intermediate nodes in the store-and-forward transmission characteristic of the Internet, there are possibly dozens of people who potentially have access to your messages. Although there is a general impression among system managers that such invasions of privacy are rare among system administrators, there is at yet no solid evidence one way or the other.

Since the Internet opened up in the summer of 1991 and allowed businesses (the .com domain) to join the net, several million commercial users have come online. However, there are still holdouts: companies who refuse to establish gateways with the Internet for their e-mail. In some cases, this decision is based on knee-jerk fear of hackers, even though it is possible to establish Internet connections which allow only the exchange of e-mail and nothing else. In others, the decision is an informed one; security managers are worried about having to install *firewall* systems and additional access controls if they allow file transfers to outside users. You=ll find a section on Internet access and firewalls at the end of this chapter.

A little-mentioned risk of connecting to the Internet is disk space saturation. According to the Electronic Mail Association of the U.S., the number of messages being sent via e-mail is growing 50% per year and was expected to hit six billion messages in 1992. It is not uncommon for subscribers to several news groups to receive over 500 messages a day. Unless you take special precautions, each user on your e-mail system who subscribes to a news group will receive a copy of each message sent to that list server. So if you have each of 100 users daily receiving 500 messages averaging 1 Kb, that's 49 Mb of new mail a day. At that rate, if your users are pack rats who save everything they get, you'll fill 1 Gb of storage in 20 working days--about a month.

[B] Legal issues

On the legal side, there are regional complications. For example, it is illegal in Canada for any organization to compete with the government-funded Canada Post Corporation at less than the exorbitant rates charged by that holdover from the days of state monopolies. What happens if someone sends a message to a company office in Montreal and has it delivered to an employee in the Vancouver office? Lawyers at one large Canadian computer manufacturer worried that this be interpreted as competing with Canada Post and forbade allowing customers to use their global network.

Another question is ownership of e-mail messages and responsibility for illegal activities carried on through e-mail. What happens if someone transmits pornographic graphics, offensive and (in some countries) illegal neo-Nazi propaganda, or messages concerning illegal drug deals *to* or *through* your Internet node? How about civil liability if someone posts stolen copies of software on your system? What about virus-infected software that can be shown to have originated in or been transferred through your e-mail system?

In the litigious atmosphere of late-twentieth century America, where the doctrine of deep pockets makes it reasonable to assign damages regardless of culpability, these questions should make for interesting discussions with your corporate counsel.

Another legal issue that troubles some managers contemplating the installation of e-mail and Internet connections is authenticity. Since the e-mail message is just a bunch of bits in memory or on disk, there is nothing to stop someone from altering some crucial bits. Imagine how much damage a disgruntled system administrator could do by altering the content, distribution, or security of certain e-mail messages in your own site.

There are ways of authenticating messages; e.g., a message-authentication code (MAC) can be calculated using encryption techniques and then appended to each message. The MAC can be time-stamped by a trusted authority and returned to the message, making it difficult for malefactors to tamper with the mail. Even more thorough is encryption of the entire message using a public key encryption algorithm (see Chapter 10). These

methods can reliably indicate who sent a message and prevent anyone but the intended recipient from deciphering the content.

Of course, with so many executives assigning their secretaries to reading their e-mail, there is a potential problem: some of these executives no doubt give their secretaries their (the executive's) own password and logon. This practice seriously compromises security on the network because is makes it impossible to ascertain who actually sent or read an e-mail message. Most e-mail packages have arrangements which allow a secretary or other authorized person to log on *as themselves* but to have limited access to someone else's e-mail. There is no excuse for allowing two people to share an ID and password.

Finally, you will have to determine your e-mail retention policies in accordance with legal requirements for records retention. As e-mail becomes more widespread, the courts will eventually catch up--or at least, be less far behind. For example, in January 1989, a journalist and several organizations wishing to preserve e-mail records generated by the Reagan administration filed suit to prevent the government from destroying electronic archives. Judge Charles R. Richey of the U.S. District Court granted a temporary restraining order in 1989 barring the destruction of e-mail records (although some files were in fact destroyed illegally after that ruling). In his decision of January 1993, the judge wrote that any records touching on federal government matters have to be preserved because of the terms of the *Freedom of Information Act.* This interpretation covers the entire federal government. However, records of communications purely affecting presidential affairs are not protected and may be destroyed at will. Unfortunately, it is not clear how anyone can determine that records were *not* touching on federal affairs *after* they're destroyed. In any case, Judge Richey explicitly ruled that arbitrary distinctions between paper files and electronic records were not a basis for selective destruction of e-mail.

[B] Management implications of external e-mail access

Any external access by an organization=s users raises important issues about authorized functions and the image of the employer in the outer world.

[C] E-mail access to FTP

Although e-mail-only gateways are feasible to allow users to exchange messages with other users in the wider world, it must be mentioned that there are ways for users to perform unauthorized functions such as file transfers simply using e-mail. E-mail FTP servers receive search or file-transfer requests (scripts or batch files) by e-mail and carry out those instructions anywhere on the Internet. The server then packages the results of the file transfer (or search, etc.) and sends it back to the originator as an e-mail message. Binary files are converted using MIME or UUENCODE transformation to 7-bit ASCII. This mechanism thus provides a covert channel for receiving binary files without going through normal security restrictions imposed on the import of executables.

Another form of binary file that may cause considerable embarrassment to the organization is graphics. There have already been several cases in the United States in which government workers have been discovered using official computer resources to retrieve, store and exchange pornographic and other undesirable materials.

In addition, USENET discussion or news groups can be joined using e-mail. Subscribers receive information about specific subjects of interest as ordinary messages and can reply if the e-mail system provides outbound Internet messaging. Given the wide range of topics available in the USENET, it is important to establish which news groups may be joined by users. Many of the news groups cover highly technical areas (although the signal-to-noise ratio tends to be low) and are legitimate sources of information for special purposes. However, many news groups (especially those in the *alt.* category) are of questionable value to the work of employees. Some news groups would be extremely undesirable: those dealing in extremist propaganda, organized hatred, and pornography would be embarrassing for the organization if there were to be subscribers.

Such activities must be carefully controlled and will require explicit policies to prevent abuse. If intelligence gathering requires monitoring of such groups, analysts should subscribe using IDs not traceable to their employer.

[C] E-mail addresses in the wider world

The previous section deals with inbound e-mail from Internet/USENET news groups.

However, it is important to realize that any contribution to any news group by a user on the organization=s systems will be identifiable as coming from the employer simply by the user=s e-mail address. This implies that every message sent out of the organization into the Internet must be considered as potentially damaging to the interests of the employer.

The employer must frame and implement clear policies on participation in such news groups. For users authorized to participate in selected groups, the organization must provide training on appropriate Anetiquette@ to ensure that employees consistently project their professionalism. It would be embarrassing for the employer, for example, to have an employee Aflame@ another user (send offensive E-mail) using their official ID.

[B] The Internet denial-of-service problem

Bob Bales, Executive Director of the National Computer Security Association, has argued for years that one of the most serious security problems caused by the Internet is that employees can waste such enormous amounts of time surfing the Net. With the low signal-to-noise ratio in so many reaches of Cyberspace, people can discover that the Internet is even worse than television as a time-sink. To paraphrase a well-known politician, employers with Internet-happy employees may hear a giant suckin= sound as their productivity goes down the tubes. In this sense, the Internet itself can lead to a denial of service--to the employer!

[B] Recommendations about e-mail and the Internet

In summary, you can avoid such problems by supplying an e-mail users' guide which includes at least the following practical points about e-mail:

[C] Using the e-mail system:

- o Anyone who finds out your e-mail password can send messages that will appear to be from you.
- o Guard your passwords against disclosure to anyone, including e-mail and system administrators.
- o Report any attempt to obtain your e-mail passwords.
- o If you want your secretary to read and answer your e-mail, he or she can do so by logging on as themselves, not by using your ID and password.

[C] Writing messages:

- o E-mail messages are limited in their capacity for carrying non-verbal information. To avoid embarrassing and harmful misunderstandings, don't send jokes, sarcastic remarks, or innuendos through e-mail.
- o Add indications of emotion to your message; e.g., <grin>, <smile>, <frown><rolling on the floor, laughing>. With time, you=ll get used to the acronyms (e.g., <rof,l>) or symbols called *emoticons.* Examples of emoticons:

  :) someone smiling (look at the emoticon sideways)
  8^) someone with glasses and a large nose, smiling
  ;^) a wink
  (>8^{(> a bald, frowning, large-nosed person with a handlebar mustache and a goatee (any resemblance to the author is coincidental).
- o You don't have to answer e-mail the moment you receive it. Take time to think about your reply--it's going on the record.

- o Don't *flame* people on the network by sending abusive, excessive, intemperate, threatening or just plain rude remarks. In fact, don't write e-mail messages when you're angry about the topic or mad at your correspondent.

- o Be careful to distinguish what you imply to be facts from what you want to express as opinions. Your reader cannot tell what your verbal inflections would have been in expressing these ideas.

- o Spell-check and style-check your e-mail. Your message could end up in your boss's in-basket or in a prospective client=s.

- o Respect the rules of copyright. Check for permission from the copyright owner before posting any published material.

[C] Personal use of e-mail:

- o The administration of this organization agrees that e-mail is subject to the same rules and expectations as phone calls during working hours.

- o You may use e-mail for private messages in ways that would be reasonable for phone use. For example,

[C] Confidentiality:

- o E-mail can be kept indefinitely, whether you delete your copy or not. There are system backups and e-mail database backups which are archived for several years. Furthermore, recipients can keep a copy of your message in their files without restriction.

- o You should act under the assumption that everything you write could someday become public knowledge.

- o Recipients of your e-mail can, if they choose, broadcast your message throughout your organization or even (conceivably) through the planetary network.

- o Encrypting your e-mail protects it only while it is still encrypted. The moment a single recipient decrypts your message, the plaintext message exists and is subject to unwanted disclosure and dissemination.

- o Be very careful about mailing lists. Don't assume you know who's included in a list just by looking at its name. Check to see that you actually want *everyone* on that mailing list to receive your comments.

[C] Receiving e-mail:

- o When you receive e-mail, assume that it is private and meant only for you unless the message specifically indicates otherwise.

- o If you receive a message clearly sent to you in error, try to be more than human: don't read it. Return it to the sender at once with a polite note explaining their error.

- o Don't assume that your first impression about an e-mail message is what the sender meant. Sometimes people express themselves poorly in writing.

- o Before assaulting, insulting, flaming, firing, or suing a correspondent, find out if the apparent author really sent it or whether you=re both the victims of an imposter. And if you do find the authentic author, find out whether those awful things they said were merely the result of a moment of insanity, a passing rage or if they really do want a fight

[C] Administration:

- o E-mail and system administrators and technical staff will make every effort to protect the confidentiality of all e-mail messages.

- o However, e-mail and system administrators may occasionally have to review e-mail messages when solving technical problems. For example, they may need to examine message headers to see why mail is being delayed or misrouted.

- o If technical staff inadvertently see confidential messages in the e-mail stream as part of their work, they will not divulge the contents to anyone except under special circumstances including but not limited to:

    * indications of criminal activity; e.g., drug sales, insider trading, blackmail, extortion, murder, theft, transferring stolen software.

    * evidence of unethical actions endangering the organization, employees, clients, or members of the public; e.g., slander, defamation of character, transmitting pornographic materials, sending instructions on hacking into computer systems, exchanging computer viruses.

- o This organization will comply with law enforcement officials who present legal authorization for surveillance of e-mail.

- o E-mail and other electronic surveillance will not be used in monitoring employee work levels.

[B] Mail storms

One final point about e-mail. Networks, because of their complexity, often have peculiarities that lead to unexpected trouble. One case that can put a network down originates from a simple request to autoforward messages. That is, an e-mail user arranges to send incoming messages automatically to some other address.

Normally, autoforwarding causes no harm. If A autoforwards messages to address B, there is no problem.

However, autoforwarding leads to a *mail storm* if users define recursive loops. In the simplest, two-member loop, if A autoforwards messages to B and B autoforwards messages to A, every message will spawn infinite copies between A and B. The situation becomes far worse when multiple people include each other in autoforwarding loops. On the Internet, mail storms have occurred when the mail systems of subscribers to news groups fail to disable automatic non-delivery notifications. The original non-delivery notification bounces back to the news group mailing-list server, which copies it out to (sometimes thousands of) members of the news group--including the one which rejected the original message. The new message may cause another non-delivery notification to be spawned. Each such message gets multiplied by the number of recipients on the news-group mailing list. If several users on the list generate non-delivery messages, the total number of useless messages grows exponentially as each non-delivery messages spawns yet more futile responses.

It is extremely difficult to prevent such loops in any automated way. Ideally, no system should return non-delivery notifications to a news-group server, and news-group servers should not forward such notifications if received. Another approach to nipping the problem in the bud is for heuristic software to alert human system managers when traffic through the news-group server exceeds a reasonable threshold--or better, when the rate of growth in traffic signals a mailstorm brewing.

[A] FAX

Sending confidential information by FAX is problematic. If you print your message and then send it through a facsimile machine that scans documents, the document will be public while it's at the FAX. You can avoid this problem by having your own FAX machine at hand or by using a FAX board in your work station.

Unfortunately, you have no control over the treatment of your FAX at the receiving end. For all you know, your valuable and confidential message is being read by every mail room clerk, secretary, sales person, and general layabout in the intended recipient's office. Sending a FAX this way is equivalent to mailing a postcard: it's public by definition.

However, the real problem lies in being sure that the *intended* recipient receives your message. Normal Wingrove told the story of an information systems consultant in Hong Kong who received a confidential FAX from a firm of lawyers. The FAX was not intended for him, and he very kindly called the law firm and lectured the senior partner in a friendly way about the need for better security. Turned out the FAX number neatly typed on the cover sheet was indeed his own--but the author had mistyped that number and failed to check for accuracy. The FAX clerk had dutifully sent an important letter to a total stranger.

A month later, the consultant received a misdirected FAX from the same person--in two copies.

[B] Confirmation

How do you, in fact, know that your FAX has reached the correct FAX machine? Most FAX machines include Called Subscriber Identification (CSI), which is sent back to the originating FAX where it appears on a display and is logged for later printout with date and time. Unfortunately, there is no legal requirement for CSI to be initialized or correct; nothing stops someone from programming their FAX machine to read BANK OF IOWA instead of JOE'S PIZZA PLACE if they so choose. Furthermore, BANK OF IOWA will be printed across the top of every FAX Joe sends from his trick machine.

Unmodified FAX machines provide no mechanism for registering the content of received FAXes. So FAX transmissions are of dubious value in establishing legal obligations and liability.

There are ways around these problems. For example, the FaxBox from DCE Corporation (Stamford, CT) is being used in the banking industry to register all outgoing FAXes. FaxBox works only with FAX boards, which act as printer drivers for all common word processing and graphics packages. You print to the FAX board and the document comes out as a FAX signal. FaxBox takes the signal, prints a copy of the FAX, calls the destination FaxBox, checks its CSI, and prints that along with time, date and phone numbers involved in the transmission. After every page is transmitted, FaxBox checks that the receiving unit can confirm receipt and records the response.

It is possible to encrypt faxes. For example, there are (expensive) encrypting faxes on the market which can exchange encrypted messages with each other. There are special add-ons such as the TX-161 unit from Encryptco (Dallas, TX) that works with the secure telephone unit (STU-III) mandated for U.S. government agencies. Other companies make portable units that can encrypt voice, data and FAX transmissions.

[B] Remanence

Most people are aware that faxes have remanence problems: they are both evanescent and peristent.

Thermal FAX paper is not suitable for long-term storage: it fades over time. So you have to photocopy such documents if you want to keep them. On the other hand, some FAX machines keep faxes in memory buffers until the buffers overflow or someone deletes them. If someone knows the access codes for their particular FAX machine, it is possible to print out several faxes that are intended for other people.

There is also a little-known feature of FAX machines: polling and pulling. It is possible to have your FAX machine with an empty input hopper call another FAX machine with documents in its hopper. If the timing is right, the calling FAX can *pull* a FAX from the FAX machine that answers. The problem is that there's no way of guaranteeing that the message being pulled is the right one; it could be there waiting to be sent to some other destination.

[B] Binary file transfers

In April 1992, I was asked by a U.S. government agency to investigate FAX server security. The agency was implementing cc:Fax software in cc:Mail from the Lotus Corporation and were using an Intel SatisFAXtion board installed on the workstation serving as cc:Mail gateway for their LAN.. The SatisFAXtion board includes

modem functions, too. Could someone dial the FAX number and somehow trick the board into assuming modem functions so they could hack into the LAN? Could someone embed a worm or a virus program inside a FAX transmission?

Several companies who make FAX boards and associated software, including Intel, confirmed that it is *not* possible to switch a FAX board from FAX function to modem function in mid-transmission or from an external phone call. Even if a modem signal were received, the software running on the platform would have to be programmed to address the modem signal. No one could imagine how a perturbation of the inbound FAX signal could possibly switch the board into modem mode.

The Intel SatisFAXtion board does, however, allow files to be uploaded onto the recipient platform *without priori authorization or control.* That is, another SatisFAXtion board can call up your system's SatisFAXtion board and initiate a binary file transfer of .EXE or .COM files (or any other file type) without so much as a by-your-leave. These binary files are stored in the inbound FAX queue with the .RCV suffix and are therefore not executable as is. On the other hand, if someone in the receiving site renames the files to end in .EXE or .COM, or if the .RCV files are copied into other directories with these executable-file suffixes, then the uploaded files *could* in theory be executed.

Another problem with unauthorized, unannounced binary file uploads is that someone could inadvertently or maliciously upload enormous quantities of data and saturate your FAX server disk drive.

After these discussions with Intel staff, I requested that Intel modify the SatisFAXtion board software to include a configurable switch allowing file send and receive, file send only, file receive only, or no file send and receive.

Until such a revision is available in the software, anyone with a SatisFAXtion board or any other board allowing file uploads should carefully monitor and control the inbound file queue to ensure that no executable files are entering your system through covert channels.

[A] Electronic data interchange

According to a report on the future of EDI, 70% of computer input is rekeyed output from someone else's computer. EDI is growing rapidly worldwide, and security is a key issue in the ultimate success of this technology. When paper purchase orders, bills of lading, invoices, and receipts are replaced by their electronic equivalents, we have to find electronic equivalents of the human signature.
Signatures are supposed to *authenticate* documents and *authorize* transactions. Theoretically, signatures make it harder to forge such documents and transactions. Signatures and other seals or symbols are legally recognized in courts of law. Electronic signatures are still not fully integrated into normal business practice. As with any electronic entity, it seems just too easy to diddle a few bits and alter the evidence without a trace. This area of research and development is known as *electronic document authorization* or EDA.

The fundamental approach to EDA is to encrypt a transaction using *public key encryption* (described in Chapter 10) which allows decryption only if the official *public key* of the sender is used to extract the original message. Then the originator has to arrange to ask a *trusted authority* to send the appropriate public key to the recipient. The trusted authority certifies that the public key is valid by a cryptographically-sound *certificate*. The encryption key used by the trusted authority has to be absolutely protected against disclosure for the entire system to work.

Governments are notoriously slow in adapting to technological change. Vendors trying to supply efficient services and cost-effective products to government departments have been stymied by insistance on paper forms and manual signatures. Several initiatives are under way in the U.S. to remove these archaic restrictions; the Food and Drug Administration (FDA), for example, launched a program to examine alternatives such as biometric patterns. The FDA is also studying implementation of technology for pattern recognition of human signatures using equipment like that of Federal Express and United Parcel Service.

Another thorn in the side of specialists trying to move towards EDI is U.S. export restrictions on encryption technology (see Chapter 10). The National Computer Security and Privacy Advisory Board of the National Institute of Standards and Technology (NIST) has been working on the Digital Signature Standard (DSS) for several years in conjunction with the National Security Agency (NSA, also jokingly known as *No such Agency*).

The Board moved in mid-1992 to initiate a review of industry's and government's concerns over the difficulty of using encryption for international communications.

[A] Emanations control

In 1982, Dutch engineer Wim van Eck, working for the Netherlands' government post, telephone and telegraph (PTT) system, established that it is easy to pick up radio-frequency (RF) emissions from ordinary video display terminals (VDTs) using inexpensive electronic equipment such as ordinary portable black-and-white TV sets. With minor adjustments, it is possible to dechipher the typed messages and read them. Reading other people's VDT displays at a distance using RF emissions became known as *van Eck phreaking* by hackers and *passive electromagnetic eavesdropping* by more formal (stuffier) people. Eric Corley, editor of the hacker magazine *2600*, is reported by Vin McLellan (writing in *PC Week*) to have said in 1987, "You'll begin to see hackers and hams experimenting with this soon.... It's just on the verge of becoming widely known, and it's just the sort of thing that draws hackers.'

Van Eck presented his work in March 1985 at Securiom in France, then published what appeared to be a deliberately incomplete report in scholarly journals. Winn Schwartau, in his typical and most enjoyable in-your-face stye, commented in April 1992, "The NCSA went ballistic and classified every copy of van Eck's paper they could get their hands on.'

In 1986, an electrical engineer working on a summer project at the Chase Manhatten was asked to replicate van Eck's work. Over the course of a fortnight, she managed to construct a van Eck device out of an old TV set and $12 of parts from a local Radio Shack outlet. Admittedly, she could only reproduce the VDT text at about a yard (1 m) from the computer, but it was still impressive.

More recently, Professor Erhard Moller of the University of Aachen in Germany has studied the van Eck phenomenon and published a report (in German) about how it works and how to fight it. Winn Schwartau has arranged to translate the report into English and it is now available.

Commercial organizations have not been terrorized by van Eck phreaking. The technique is completely non-selective; which VDT you happen to be able to spy on depends not only on its own emissions but also on chance arrangements of other nearby electronic equipment and its emission characteristics, building-wall thickness and composition. Another difficulty for spies is that in a large organization, really sensitive information is likely to show up on only a very small proportion of all the VDTs in use, thus masking the most interesting data. In a site with many VDTs, the signals may be so garbled together that no meaningful information can be extracted--at least, not by an amateur. One of the simple methods you can make the spy's job harder is to include conductive wall panelling in any new site where computers will be used.

The U.S. government began working on emanations control in the late 1950s. The project became known as TEMPEST, which some interpret as an acronym for *Transient ElectroMagnetic Pulse Emanations STandard.* The Industrial Tempest Program began in 1974 as a method of getting more manufacturers to define and meet the evolving government standards and to certify the levels of emanations for equipment to qualify for government purchase.

TEMPEST-qualified equipment is heavily shielded with conductive materials. As a result of the extra materials, labor and certification requirements, TEMPEST versions of standard equipment can cost 5-20 times more than off-the-shelf equivalents. For example, at one time, a $2,000 OKI FAX machine cost $20,000 in its TEMPEST incarnation.

TEMPEST technology can apply to entire buildings. For example, in the U.S. government, some installations are known as *SCIFs*--Sensitive Compartmented Information Facilities. These are essentially buildings or rooms inside a Faraday cage--a grid constructed to interfere with all emissions and make the facility radio-silent.

Another approach to stopping van Eck phreaks is to mask the emissions with random electromagnetic noise. Hughes STX, a division of Hughes Aircraft, has developed a device they call *Stealth.* It garbles RF emissions into TEMPEST-quality unusability and it costs only about $1,000 per unit. Best of all, it can be installed on any existing equipment.

One side-issue about TEMPEST equipment is that it can also serve to protect computers against high-energy radio-frequency (HERF) guns. These devices project bursts of energy that disrupt unprotected processors. Theoretically, with a strong enough projector, it should be possible to cause random system crashes and memory errors in operating computers at distances of hundreds of meters or more.

According to Schwartau, the U.S. Navy is reported to have used microwave bombs to destroy Iraqui electronic circuits. The projectors were allegedly mounted on Tomahawk cruise missiles. The *EMPT-T* (electromagnetic pulse) bombs generate a huge magnetic field which can blow transformers, wipe magnetic memories and disks, and fuse semiconductor chips. Sounds like quite a mess. Wonder what would happen if one of *those* went off in New York City?

[A] Internet access and firewalls

Firewalls are mechanisms for controlling *who* can access *which* functions of a system linked into the Internet.

One of the most highly-praised security textbooks to appear in recent years is Cheswick and Bellovin's *Firewalls and Internet Security.* With the enormous increase in interest shown in the professional and popular press about connecting to the Internet, this book is required reading *before* anyone opens a system to Internet access.

Part I of the book, AGetting Started,@ provides a brief chapter of introduction to the issues of Internet security. Chapter 2 , AAn Overview of TCP/IP@ includes 29 known weaknesses in the world of UNIX-based Internet connections. Examples: tampering with routing protocols, executable instructions in MIME-encoded messages, transparency of *telnet* sessions to eavesdropping, promiscuous distribution of password files by the *Network Information Service (NIS),* danger of letting files be owened by the *ftp* login, and failures of *World Wide Web (WWW)* servers to control file transfers. The book as a whole presents 41 such Abombs@ and lists them neatly in a couple of pages after the bibliography.

Part II, ABuilding Your Own Firewall,@ includes chapters on AFirewall Gateways,@ AHow to Build an Application-Level Gateway,@ AAuthentication,@ and AGateway Tools.@ Chapter 7, ATraps, Lures and Honey Pots,@ provides a look at setting up attractive targets (Ahoney pots@) for criminal hackers to attack--but which in fact are surrogates of no importance to the defenders. These dummies can be fitted with scripts simulating slow response time to delay intruders and waste their time. Chapter 8, AThe Hacker=s Workbench,@ reviews how criminal hackers carry out penetration of insecure systems.

Part III of the text discusses the authors= experience with an attack on Cheswick=s system in January 1991. The attack began with an intruder using a stolen account at a Stanford University computer and manually simulating a mail program. The criminal hacker requested a copy of the AT&T computer=s password file and was duly sent a fake file including the imaginary user Fred Berferd. The attacker resumed his penetration attempts a few days later using Berferd=s ID. Cheswick responded by simulating a slow, poorly-administered system. Every attack was scrupulously logged and reported to the Computer Emergency Response Team Coordination Center (CERT-CC) at Carnegie-Mellon University. When Cheswick tired of responding to the attacks, he simulated a problem with his system=s disk drives and shut down access; he comments, AI suspect that hackers may have fored the general opinion that disk drives ar less reliable than they really are.@

Cheswick and his colleagues set up a circumsribed area on their computer system that they called a Achroot Jail@ or Aroach motel.@ The attacker=s sessions were routed to this closed environment and every interaction closely monitored. Stanford=s systems appeared to be under attack by the same criminal, and after a short time both groups were informed by Wietse Venema, a computer scientists from the Netherlands, that he was on the trail of this ABerferd@ character. Unfortunately, there was no basis for prosecution in Netherlands at that time. Eventually Cheswick closed down his Ajail@ at the request of company management and Berferd Amoved his operation to a hacked computer in Sweden.@

The authors conclude that sites should be prepared to deal with penetration attacks *before* they happen.

The text concludes with an analysis of a few years of log files; the data reveal what kinds of attacks are the most popular, when they occur during the day, week and year, and where they come from (mostly from educational institutions). The authors present chapters on ALegal Considerations,@ ASecure

Communications over Insecure Networks,@ and AWhere Do We Go from Here?@ Their appendices include AUseful Free Stuff,@ ATCP and UDP Ports,@ and ARecommendations to Vendors.@

[A] S.A.T.A.N.

Any security probe is a two-edged tool; in the hands of honest people, it pinpoints weaknesses and gives system administrators a chance to improve their security. War-dialers, password crackers--these tools have been written by criminal hackers and by honest programmers as well. But none has caused the controversy that erupted over SATAN in early 1995.

The Security Administrator Tool for Analyzing Networks (SATAN) was written by Dan Farmer, at that time with Silicon Graphics, and Wietse Venema. This tool was designed to help system managers probe their own security; however, its uncontrolled distribution on the Internet provoked a storm of controversey in April 1995 because many observers felt that its easy availability would put many systems at risk from criminal hackers. Farmer was fired by SG and went to work for SUN. Partisans of the different sides of the debate excoriated Farmer and Venema or praised them as generous heroes of cyberspace. Discussion sometimes veered into flamewar in security forums throughout the Internet. Farmer and Venema=s reputations were not enhanced among their critics when it turned out that the first version released with such fanfare actually had a bug which damaged security in the systems being probed. A fix was issued immediately.

In response to the controversy, NIST, the National Institute of Standards and Technology, issued a Fact Sheet about the tool, which I quote in its entirety below. The FAQ is so clear that I have nothing to add.

Another tool was written shortly after release of SATAN: *Courtney* informs system managers that their system is under attack by SATAN by monitoring Internet probes and looking for the pattern used by SATAN.

> RELEASE OF SATAN SOFTWARE TOOL
> FACT SHEET
>
> INTRODUCTION
>
> Due to extensive media attention regarding the release of another version of SATAN (Security Administrator Tool for Analyzing Networks), the National Institute of Standards and Technology (NIST) is issuing this fact sheet to answer questions about SATAN.
>
> WHAT IS SATAN?
>
> SATAN is a software tool for assessing Internet host and network security. SATAN tests host systems to determine which Internet services are present and whether those services are misconfigured or contain vulnerabilities that an intruder could exploit. SATAN provides limited information on how to correct the vulnerabilities it identifies as well as a modest tutorial on
> host system security. SATAN can test individual hosts or entire networks of host systems. SATAN is an analysis and reporting tool only and does not break into systems or exploit new and/or rare vulnerabilities. All the vulnerabilities it finds are well known and have either bulletins and/or patches from an incident response team or a vendor. However, as with most tools of this type not just system administrators but intruders will undoubtedly use SATAN to find vulnerabilities in certain systems and then they will exploit those systems. Thus, while the tool aids a conscientious security-aware administrator it does increase the risk to the unwary administrator.
>
> SATAN'S AVAILABILITY
>
> SATAN's authors, Mr. Dan Farmer and Mr. Wietse Venema, made SATAN widely available over the Internet without cost starting April 5, 1995. Many Internet sites now have SATAN and thousands of copies have been distributed worldwide.
>
> WHAT IS REQUIRED TO RUN SATAN?
>
> SATAN runs on specially-configured UNIX systems and can be configured so that only users with system-level privileges or root privileges may execute the software. The first release of SATAN runs

only on UNIX systems made by Sun Microsystems and Silicon Graphics. Ports to other UNIX systems such as Linux have followed quickly. SATAN requires installation of additional software and World Wide Web (WWW) client programs such as Mosaic. It is important, however, to distinguish between systems that execute SATAN and those that SATAN can scan. SATAN can be used to scan many different vendor systems and, furthermore, could be modified to probe routers and other networked devices.

WHY IS SATAN CONTROVERSIAL?

As stated earlier, SATAN is controversial because conscientious system and network administrators and would-be hackers or intruders are both helped. Administrators who have both time and the capability to use and understand SATAN and its findings will clearly close up the holes or vulnerabilities in their systems. However, many system administrators are often ill-equipped or equipped but over-burdened, and thus are quite vulnerable to intruders who run SATAN against them. A typical hacker will scan a site for vulnerabilities with a tool like SATAN, find some systems vulnerable, and then install trojanized login programs (permit access by legitimate users but steals their passwords and system Ids) or sniffer programs that silently sniff legitimate user passwords and Ids for later illegitimate use. Several computer security incident response teams report that internal testing for vulnerabilities indicates that very high percentages of Internet host systems are vulnerable to tools like SATAN. As a consequence, some incident response teams and others in the Internet community have and are writing detectors to note when SATAN is being used to scan their systems.

IS SATAN OVERBLOWN?

As we saw in the Michelangelo Virus furor that erupted a few years ago, our fear and the attendant hype outstripped the actual damage caused. Part of the issue here is our attention span. Clearly, viruses are very real and can and do cause much mayhem even if the damage occurs after the press and management focus moves on to other issues. Similarly, the vulnerabilities that SATAN identifies are real and exploitable but won't evidence themselves in a sudden series of attacks days or hours after the SATAN release. However, with thousands of copies freely available and in use SATAN will make an impact. It won t aid the knowledgeable intruder who is already aware of how to break in but it will assist the less than gifted would-be intruder. As these thousands of copies coarse throughout the Internet, we and the computer security community will be in a better position to assess the real impact of SATAN and whether the initial hysteria was founded after about 6 months of perspective is gained.

DOES SATAN IDENTIFY NEW VULNERABILITIES?

No, all the vulnerabilities it finds are well known and have either bulletins and/or patches from an incident response team or a vendor.

HOW IS SATAN DIFFERENT FROM OTHER SECURITY TOOLS?

Tools similar to SATAN have been available to Internet users for several years, both commercially and in the public-domain. These tools are also used by the intruder community to identify systems vulnerable to attack. SATAN is different in that it can be configured to test virtually any system or network of systems accessible to the Internet. SATAN is also more powerful than previous tools and able to identify more vulnerabilities. SATAN can discover whether a system trusts connections from other systems, and then scan those systems. SATAN's WWW interface is easy to use and its results are easy to view. Additionally, SATAN can be modified easily to exploit new vulnerabilities.

ADVICE FOR SYSTEM AND NETWORK MANAGERS

Sites should be concerned that internal users as well as intruders could run SATAN and expose site vulnerabilities. Thus, NIST recommends the following:

- sites should develop policies for using SATAN responsibly and efficiently,
- sites should promptly correct all vulnerabilities before vulnerable systems could be attacked,

- sites should look-out for illicit scans of their networks by SATAN or other tools, and
- system managers should install access control software to ensure scans of their systems by SATAN will be noticeable and consider installing SATAN detector software developed by incident response teams.

Sites should also improve their network and host security policies and measures. Sites should consider installing firewall systems so that internal systems are easier to manage and less vulnerable to attacks. Sites should install all vendor patches and subscribe to vendor and incident response team mailing lists so that they will be notified of future patches or vulnerabilities. Sites should develop policy for network usage, Internet access, and incident reporting. It is very important that sites improve system management by allotting sufficient time for system administration duties and training as necessary. Lastly, when purchasing systems, sites should demand security features and properly install and configure new systems and periodically recheck old systems.

FOR FURTHER INFORMATION

NIST operates a clearinghouse of computer security information and tools accessible via the Internet and dial-in at all times. The clearinghouse contains links to information about computer security and incident response team clearinghouses. Together, these sites provide basic and detailed computer security information, vulnerability and threat assessments, incident response team alerts, vendor patches, and computer security tools including firewalls and pointers to vendors. The clearinghouse is accessible via the following methods:

WWW: http://csrc.ncsl.nist.gov
ftp: csrc.ncsl.nist.gov, login as "anonymous"
email: send message "send INDEX" to docserver@csrc.ncsl.nist.gov
dial-in: 301-948-5717

[A] Special Considerations for PC and Workstation Security

Network managers end up having to be concerned about the security of the workstations hooked to their network. In this section, I review some key issues related to PCs and other workstations. However, the subject is treated fully in my colleague Stephen Cobb=s book in this series, *The NCSA Guide to PC and LAN Security,* also available from McGraw-Hill.

PCs are in a sense more vulnerable than larger computers. Along with the convenience and cost-effectiveness of microcomputers has come a greater vulnerability of the data residing on these systems. Problems include theft of equipment; the ease of unauthorized data interchange; and
the difficulty of managing software licenses.

[B] Physical accessibility

Microcomputers handle as much critical and sensitive data as mainframes and networks, but they are generally much easier to access. Micros are distributed throughout the organization whereas larger systems are usually sequestered behind at least a modicum of physical protection. Current trends suggest that PC thefts are increasingly common. For example, here are some news items of interest dating back over several years; almost all of these were summarized in a bibliography posted in the news group Acomp.security.misc@ by Ed Wilson in June 1995 and reposted in the NCSA InfoSecurity Forum on CompuServe by David Kennedy:

1987 *Federal Computer Week* reports an $80,000 theft of computers and disk drives at Apple Computer=s Reston, VA office--just before the deadline for proposals on a major government procurement contract. The theft looked like a professional job; may have been industrial espionage.

Federal Computer Week reports a second major theft of Macintosh computers in a couple of weeks, this time about $50,000 of equipment from a retail store--including office disk drives containing information about the store=s federal contracts.

1989 In an interview with Donn G. Parker, *PC Week* quotes him as saying that an insurance company was robbed of over $1 M of PCs despite security measures that included bolting the machines to their desk tops. The thieves simply removed the desk tops along with the PCs. Lost data caused loss of business during the recovery period.

1990 *ISPNews* reports that 10,000 to 25,000 laptop computers are stolen yearly in the U.S. Recovery of 20 Mb of stolen or lost data can take between three to six weeks.

The Stanford University Campus Report estimates that about $150,000 of PCs and peripherals or components have been stolen on campus within the current year.

In *The Peninsula Times Tribune,* a writer comments, AAlready, the dollar loss this year in stolen Macintosh, IBM and Next Inc. computers is equal to last year's total--more than $140,000. Police said that in 22 thefts this year, 30 computers were stolen. In some cases multiple thefts occurred, such as one in which six Macintosh computers valued at $29,000 disappeared and another in the music annex where three Next computers valued at $32,000 were taken.@

1991 In Tallahassee, FL, Barrington Salmon writes that a single thief was caught with $200,000 of stolen electronic equipment. APolice described the suspected computer thief, a high-school dropout, as a hacker who cannibalizes computers for parts to install in his own computer. We have taken out two truckloads of stuff,@ said an investigator. AThey include everything from software to floppy disc drives to TVs and entire computer systems. In a recent breakin about $40,000 worth of computers and other equipment was taken from Pietrodangelo Production Group. Danny Pietrodangelo, whose company was hit four times by burglars, said he had just bought some of the computers to replace those stolen last August.@

Detroit Free Press claims that University of Michigan students, faculty and staff are expected to steal $400,000 of computer equipment. One student, a chemical engineering major, hid in a closet until

the campus engineering network closed; he then stole the network file servers. Most of the thefts occur with no sign of forced entry, even when doors are locked.

University of California at Davis *Davis Enterprise* notes that 12 Macintosh computers worth a total of $30,000 were stolen during a weekend in November.

1992 In June, Rensselaer Polytechnic Institute library loses $26,000 in computers, printers, typewriters and software. Burglars disengaged the alarm system and used bolt cutters to cut the security cables holding down the equipment.

Stolen Computer Registry reports $10 billion of stolen computer hardware in 1992 in U.S.

Five North Carolina universities lose $250,000 in computer equipment.

1993 University of New Mexico *Campus Crimeline* states that in November, thieves cut a hole in the wall of the Director=s Office and stole $1600 of hardware and $1500 of software; data replacement was estimated to cost $75,000.

Corporate Computing publishes an article by Patrick Houston in which he recounts the 1991 theft of a laptop with valuable corporate data from an NCR executive. The thieves are alleged to have been working for the French intelligence agency.

Jim Seymour, writing in *PC Week*, states that at one of his own consulting clients, 8% of their laptop computers were lost or stolen within a year; even more worrying, the thieves tried to log onto the corporate networks using those stolen machines. The same company lost several more laptop computers during breakins at two regional offices.

1994 *Pittsburgh Postgazette* article reports that a graduate student=s computer--including his entire anthropology thesis--was stolen from his home. Student begs thieves to return the data.

1995 Gary Anthes of *Computerworld* reports that theft of computer systems and components a growing problem; the black market in memory chips, power supplies and other bits and pieces is flourishing. Computer chips currently worth more than their weight in platinum.

[B] Data at greater risk

Data are at even greater risk on PCs and Macintosh computers than they are on mainframes and servers. Larger systems often use proprietary operating systems, expensive database management subsystems, and locally-written or modified applications software. Anyone stealing backup tapes, for example, will have difficulty matching the specific combination of hardware and software required to make use of the stolen data. In contrast, microcomputer users tend to have one or two widely-distributed operating systems (e.g., DOS, OS/2, Windows95, Macintosh System software), standard database software (e.g., dBase, Foxpro, Access) and off-the-shelf application programs.

In an unintended side effect of cooperation, manufacturers have made PC software so interoperable that PC data thieves can count on making sense of practically anything they steal. Word processing packages can read each other=s files; so can most spreadsheets and graphics packages. Data have become the common currency of cyberspace.

[B] Software management

Network managers must be concerned with software management on PCs and other workstations. For proprietary packages written using the client/server model, it is critically important that production software be installed uniformly throughout the network. There are tools available for such software management. For example, some sites have batch files which scan client disks when the PCs are booted up; the server can then automatically update any proprietary software that is not up to date. Similar approaches can work with off-the-shelf software.

Software manufacturers demand compliance with their contracts; network managers must ensure that their software licenses cover actual use. For example, if a firm signs an agreement for a site license specifying that no more than 64 users at once may run the program, the managers must install software metering. Software metering software not only prevents excessive use of licensed software, but also provides reports on the number of attempts to exceed the limit. As the license becomes saturated, managers can buy the next larger site license.

Another issue facing network managers is the prevalence of computer games. Some games merely waste employee time; others, such as Doom, can actually interfere with network operations by saturating the bandwidth. Most organizations should have firm policies in place banning the installation and use of computer games on office computers and networks.

CHAPTER NOTES:

1. For an introduction to data communications and network security:

Anonymous (1995). Communications. *Windows Magazine* 2(2):112

Anonymous (1990). Data communications: basic concepts. *Datapro Management of Data Communications* report #CS10-100-101.

Anonymous (1989). PC-to-host communications products. *Datapro Management of Communications* report # CS20-425-101. See p. 116 ff for security aspects of terminal emulation and of increased network access.

Baker, S. (1995). Solving the PC connectivity puzzle. *UNIX Review* 13(1):29

Goodall, G. (1994). A guide to going remote. *Computing Canada* 20 (10):52

Hansen, A. (1990). Coming through loud and clear, part II. *UNIX World* 7(8):141

Hansen, A. (1990). Coming through loud and clear. *UNIX World* 7(7):153

Miller, M. A. (1991). *Internetworking: A Guide to Network Communications--LAN to LAN; LAN to WAN.* M&T Books, Division of MIS Press / Henry Holt & Co. Inc. (New York, NY). ISBN 1-55851-143-1. xxiii + 425. Index.

Miller, M. J. & S. V. Ahamed (1988). Computer networks. From *Digital Transmission Systems and Networks, Vol. II.* Computer Science Press. Reprinted (1988) in *Datapro Management of Data Communications* report #CS-10-640-101.

Musgrove, J. (1994). Managing integrated voice, data, and video network access using today's carrier services. *Telecommunications* 28(12):22

Schweber, W. L. (1988). Communications channel characteristics. Chapter 2 of *Data Communications.* McGraw-Hill. Reprinted (1988) in *Datapro Management of Data Communications* report #CS-10-220-101.

Sloman, J. (1994). A crash course in networking basics. *Windows Magazine* 5(7):313

Stallings, W. (1995). *Network and Internetwork Security: Principles and Practice.* Prentice Hall (Englewood Cliffs, NJ). ISBN 0-02-415483-0. xiii + 462. Index.

Stallings, W. (1988). Digital data communications techniques. From *Data and Computer Communications, 2nd ed.* Macmillan. Reprinted (1989) in *Datapro Management of Data Communications* report #CS-10-500-101.

Stang, D. J. & S. Moon (1993). *Network Security Secrets.* IDG Books Worldwide Inc. (San Mateo, CA). ISBN 1-56884-021-7. xxxiii + 1166. Index.

Williams, D. (1994). A route to a bridge through a gate: determining the best setup for your data communications interconnectivity. *LAN Times* 11(17):58

Tugal, D. A. & O. Tugal (1989). Communications and communications links. Chapter 1 of *Data Transmission, 2nd ed.* McGraw-Hill. Reprinted (1990) in *Datapro Management of Data Communications* report #CS-10-225-101.

2. I wish to thank Ken Shoopman for contributing so much information to the April 1993 *Information Systems Security* course in Denver, CO. His demonstrations of surveillance technology and countermeasures were illuminating, not to say breathtaking. You can reach Ken at SAIC / P. O. Box 5307 / Aluquerque, NM 87185 / Tel. 505-845-6423).

3. A good review of the basics of leased lines:

Anonymous (1991). An overview of interstate private line facilities. *Datapro Management of Data Communications* report #CS15-710-201.

4. Fibre optic links and security:

Anonymous (1990). Fiber optic communications markets and leaders. *Datapro Management of Data Communications* CS10-690-401.

Bushaus, D. (1990). More network protection. *Communications Week* (312):27

Chao, J. C., J. C. Hershauer, & D. C. Kneer (1991). A primer on fiber optic concepts and an analysis of related security issues. *Computer Security Journal* 6(2):67

Dolev, D., C. Dwork, O. Waarts & M. Yung (1993). Perfectly secure message transmission. *Journal of the Association for Computing Machinery* 40(1):17

Levine, J. (1991). Securing LANs. *Communications Week* (351):37

Olsen, F. (1990). Smithsonian revamps security with new fiber-optic network. *Government Computer News* 9(15):46

5. Satellite links and the Captain Midnight incident:

Anonymous (1989). Satellite communications: Technology briefing. *Datapro Management of Data Communications* report #CS15-745-101.

Anonymous (1987). The vulnerabilities of communications systems. Chapter 3 of *Defending Secrets, Sharing Data,* document OTA-CIT-310 from the U.S. Congress Office of Technology Assessment. Reprinted in *Datapro Management of Data Communications* as report #CS40-750-101.

Blackburn, R. J. (1988). Digital broadcast network: a down-to-earth view. *Telecommunications* 22(1):43

Shimabukuro, T. M. (1988). Securing satellite signals. *Telecommunication Products & Technology Magazine* 6(6):20

6. Concerning packet-switching networks:

Gavurin, S., C. H. Liu & M. D. Piesner (1993). On a higher plane: vendors have elevated packet switches to a new level by adding frame relay support and promising to embrace ATM. *Network World* 10(51):33

Hassig, L. & S. V. Kelly (1986). *Communications.* Part of the series, *Understanding Computers*. Time-Life Books (New York). ISBN 0-8094-5700-8. See pp. 65-77 for an extended pictorial essay on packet switching. See also p. 44 ff.

Michel, A. (1989). Packet-switched networks. In: *ISDN, DECnet and SNA Communications,* edited by T. C. Bartree. Reprinted in *Datapro Management of Data Communications* as report #CS-10-670-101.

Strizich, M. (1994). Connect your LANs: public online services offer low-cost ways to link far-flung offices. *Macworld* 11(8):152

7. Wireless technology:

Anonymous (1992). Narrow band or spread spectrum: which one is right for you? *Digital News & Review* 9(18):49

Deixler, L. (1994). Wireless wonders! (Wireless Buyers= Guide). *Teleconnect* 12(11):40

Birkhead, E. (1992). LANs on the airwaves: three technologies, each with their selling points, have emerged into the wireless networking mainstream. *LAN Computing* 3(8):12

Dryden, P. (1991). Wireless options abound for desktops, portable PCs. *LAN Times* 8(23):25

Eisenberg, A. (1993). Beaming data across town: wireless data technologies come to PCs. *Computer Shopper* 13(2):200

Else, K. (1992). Making waves. *DEC User* :45

Leonard, M. (1992). Wireless data links broaden LAN options; vendors and regulatory bodies confront limited-bandwidth and interference problems. *Electronic Design* 40(6):51

Loudermilk, S. (1992). Spread-spectrum technology catches on. *PC Week* 9(30):45

McLachlan, G. (1992). Spread spectrum breaks barriers. *LAN Computing* 3(6):1

McLachlan, G. (1992). Wireless network hops frequencies. *LAN Computing* 3(11):1

Miles, J.B. (1994). Wireless LAN products. *Government Computer News* 13(26):55

Simons, D. (1992). Wireless data services help solve real business problems. *Computing Canada* 18(19):S6

Tuite, D. (1992). Powerline spread-spectrum modulation saves copper in LANs and control systems. *Computer Design* 31(11):50

Ubois, J. (1993). Wireless LANs are due for an encore (*MacWEEK Special Report:* Wireless Communications). *MacWEEK* 7(10):24

Wilson, R. (1992). Offices without wires. *Electronics Weekly* (1602):19

8. LAN monitors

Anonymous (1994). Test & analysis equipment: 1994-1995 Buyers= Directory Issue. *LAN Times* 11(18):460

Jander, M. (1991). Keeping watch on Ethernet problems as they occur. *Data Communications* 20(17):100

Kabay, M. E. (1992). Protect LANs from the X-ray of LAN monitors. *Network World* 9(48):39

Kabay, M. E. (1992). Gaping hole in local area network security. *NCSA News* 3(3):4

Merenbloom, P. (1995). A good protocol analyzer is crucial to cleaning up your network traffic. *InfoWorld* 17(13):80

Waltz, M. (1994). Packages help managers put networks in analysis. *MacWEEK* 8(31):63

Wexler, J. M. (1992). LAN security marching to smart hubs: 3Com, Ungermann-Bass unveil tools at Networld; Cabletron on deck. *Computerworld* 26(7):1

9. Toll fraud

Anonymous (1994). Toll fraud: AT&T expands and re-prices its toll fraud service. *EDGE, on & about AT&T* 9(304):19

Booker, E. & G. H. Anthes (1994). Toll fraud rings in high cost. *Computerworld* 28(41):1

Burch, B. (1994). Sprint nixes toll fraud liability, but for a price; carrier's Elite option gives users full protection. *Network World* 11(41):27

Haugh, J. J., R. E. Burney, G. L. Dean, & L. H. Tisch (1992). *Toll Fraud and Telabuse: A Multibillion Dollar National Problem.* Telecommunications Advisors Inc. (Portland, OR). ISBN 0-9632634-2-0. 2 volumes. Also available from the NCSA (Carlisle, PA).

Haugh, J. J. (1993). Toll fraud: the scourge of telecommunications. Presentation to the annual meeting of the National Computer Security Association, Washington, DC, 10-11 June 1993.

Herman, B. & T. K. Crowe (1993). A call to arms: only you can prevent toll fraud. *Teleconnect* 11(1):69

Lyons, K. (1994). Toll fraud: the billion-dollar heist. *Telecommunications* 28(5):49

Michalecki, R. (1994). Toll fraud: multimillion-dollar telecomm problem. *Communications News* 31(2):34

Quinn, Brian (1993). Dialing for dollars. *Corporate Computing* 2(5):124

Staino, P. A. (1995). Practice safe sets! Protect handsets, PBXs and ACDs against unwanted intruders. *Teleconnect* 13(1):112

Staino, P. A. (1994). Small business hacker's delight. *Teleconnect* 12(8):33

Staino, P. A. (1994). The 100% sure way to get fired: don't protect yourself from toll fraud. *Teleconnect* 12(1):57

10. Abuse of voice mail

Hertzoff, I. (1991). Tips for beating voice net hackers. *Network World* 8(19):50

Houser, W. R. (1992). Voice mail "sound bites" can be embarrassing indeed. *Government Computer News* 11(18):21

Langsberg, M. (1992). Telephone crackers hit Logitech, Inc. *San Jose Mercury News* (Sept 12, 1992):8D.

Leibowitz, E. (1991). Voice mail toll fraud: and other tales of telecom woe. *Teleconnect* 9(8):26

Salamone, S. (1992). Voice mail systems make easy targets for hackers: net managers often overlook voice mail security. *Network World* 9(10):25

11. E-mail

Anonymous (1990). Wire tap? Class action suit filed against Epson America, Inc. for invasion of privacy; employee E mail allegedly tapped. *EDGE, on and about AT&T* 5(107):8

Achenbach, J. (1993). Plugging in to E-mail: From your house to the White House, it's leaving a stamp on the way we communicate. Washington Post wire service (Mar 22, 1993); retrieved automatically through *CompuServe Executive News Service.*

Caldwell, B. (1991). More e-mail controversy: former Nissan employees file invasion of privacy suit. *Information Week* (303):50

Carroll, J. (1992). Is it right to read other people's e-mail? *Computing Canada* 18(25):50

Carroll, J. (1992). How secure are the messages on your network? *Computing Canada* 18(23):53

Gerber, C. (1993). Booming commercial user changes face of Internet: security, legal issues coming up. *InfoWorld* 15(15):1

Glen, R. (1991). E-mail voyeurism. *Canadian Datasystems* 23(10):57

Hogan, M. (1992). Is that your E-mail ticking? *PC World* 10(9):37

Houser, W. R. (1992). The ghost of e-mail past could come back to haunt you. *Government Computer News* 11(17):25

Kallman, E. A. & S. Sherizen (1992). Private matters. *Computerworld* 26(47):85

Kolstad, R. (1992). Daemons and dragons: mail privacy. *UNIX Review* 10(8):79

Miller, S. C. (1992). Privacy in e-mail? Better to assume it doesn't exist. *New York Times* 141(June 7, 1992):8F.

Quindlen, T. H. & S. P. McCarthy (1993). Ruling says most federal e-mail records must be preserved. *Government Computer News* 12(3):77

Robinson, P. (1992). *Delivering Electronic Mail: Everything You Need to Know About E-Mail.* M&T Books (San Mateo, CA). ISBN 1-55851-170-9. xi + 336. Index.

12. FAX security

Anonymous (1992). Electronic fax security. *LAN Computing* 3(5):50

Brewin, B. (1992). AFCEA showcases comm wares for feds; secure fax and color videophones top the list of new items. *Federal Computer Week* 6(17):30

White, R. (1992). Castelle FAXPress designed for NetWare network users; bases covered with security, routing, administration. *LAN Times* 9(2):109

Wingrove, N. (1990). Hiding the fax. *Newsbytes* (Mar 6, 1990):NEW03060085.

Wingrove, N. (1990). Lax fax security lesson goes unlearned in slack lex firm. *Newsbytes* (Apr 3, 1990):NEW04030064.

13. Electronic data interchange and document authentication

EDI Council of Canada (1992). *EDI or DIE. Issues for Canada's Future:* Supplement in the *Globe and Mail*, June 1992.

Fischer, A. (1992). Put your "John Doe" here--digitally, that is. *Computing Canada* 18(23):46

Kevin, P. & V. J. Grimm (1992). Board hopes review will douse DSS flames. *Government Computer News* 11(15):10 .

Wright, B. (1992). Feds to erase paper signature rules. *Corporate Computing* 1(4):40

14. Van Eck phreaking

Abramson, J. (1989). Mind what you say; they're listening. *Wall Street Journal* (Oct 25, 1989):B1.

John, M. (1990). UK security awareness campaign highlights the hidden threats to everybody's data. *Computergram International* (1441):CGI06070007

McLellan, V. (1987). CRT spying: a threat to corporate security? *PC Week* 4(10):35

McLellan, V. (1987). An end to easy CRT eavesdropping. *Digital Review* 4(3):76

Moller, E. (1992). *Protective Measures Against Compromising Electromagnetic Radiation Emitteed by Video Display Terminals.* Translated from the German. Inter.Pact Press (Seminole, FL).

Schwartau, W. (1992). Van Eck II. *Security Insider Report* (Apr 1992):1.

Schwartau, W. (1991). Information terrorism threatens way of life. *InfoWorld* 13(36):S72

Wiegner, K. K. (1990). Is someone listening to your computer? *Forbes* 145(11):342

15. Emanations control, TEMPEST and HERF Guns

Duncan, R. J. (1993). TEMPEST standards and products: overview. *Datapro Reports on Information Security* report #IS80-001-101.

Masud, S. A. (1992). Vitalink adds Tempest security to its bridge-routers. *Government Computer News* 11(13):56

Schwartau, W. (1993). Magnetic weapons. *Security Insider Report* (Jan 1993):5.

Schwartau, W. (1992). Home brew HERF guns. *Security Insider Report* (June 1992):1.

Schwartau, W. (1992). EMP-T bombs used. *Security Insider Report* (May 1992):7.

Schwartau, W. (1992). $1000 TEMPEST. *Security Insider Report* (Apr 1992):5.

Taft, D. K. (1992). Tempest laptop from RDI offers security to go. *Government Computer News* 11(8):45

Taft, D. K. & R. Vizachero (1992). Stealth technology brings down the cost of security. *Government Computer News* 11(7):58

16. Introduction to the Internet

Dern, D. P. (1994). *The Internet Guide for New Users.* McGraw-Hill (New York). ISBN 0-07-016511-4. xxvii + 570. Index.

Hahn, H. & R. Stout (1995). *The Internet Yellow Pages, Second Edition.* Osborne McGraw-Hill (Bereley, CA). ISBN 0-07-882098-7. xxxvi + 812. Index.

Krol, E. (1992). *The Whole Internet User's Guide & Catalog.* O'Reilly & Associates (Sebastopol, CA). ISBN 1-56592-025-2. xxiv + 376. Index.

Lynch, D. C. & M. T. Rose (1993). *Internet System Handbook.* Addison-Wesley Publishing Co. (Reading, MA). ISBN 0-201-56741-5. xxxii + 790. Index.

Wiggins, R. W. (1995). *The Internet for everyone: A guide for users and providers.* J. Ranade Workstation Series (McGraw-Hill, New York). ISBN 0-07-067019-6. xvi + 655. Index.

17. Internet firewalls

Bryan, J. (1995). Build a firewall. *Byte* 20(4):91

Bryan, J. (1995). Firewalls for sale. *Byte* 20(4):99

Cheswick, W. & S. Bellovin (1994). *Firewalls and Internet Security: Repelling the Wily Hacker.* Addison Wesley (Reading, MA). ISBN 0-201-63357-4. xiv + 306. Index.

Farrow, R. (1994). Protecting your network. *Open Computing* 11(10):83

Firewalls FAQ (ongoing). Widely available list of frequently-asked questions about firewalls from NIST (U.S. National Institute of Standards and Technology) stored among many other places in Library 8 (Unix/Internet) of the NCSA FORUM (GO NCSAFO) on CompuServe.

Hancock, B. (1994). Before you hook up to the Internet, build yourself a sturdy fire wall. *Digital News & Review* 11 (11):14

Harwood, R. (1994). Install the wall. *DEC Professional* 13(12):44

Kalakota, R. & A. B.Whinston (1994). Firewalls aren't foolproof. *InformationWeek* (507):62

Kobielus, J. (1994). Firewalls aren't foolproof cure for Internet security woes. *Network World* 11(50):50

Merenbloom, P. (1994). Network 'fire walls' safeguard LAN data from outside intrusion. *InfoWorld* 16(30):69

Merenbloom, P. (1994). Setting and testing the groundwork for your network fire wall. *InfoWorld* 16(31):56

Merenbloom, P. (1994). Final steps for creating a fire wall and guarding Internet access. *InfoWorld* 16(32):59

Moskowitz, R. G. (1994). Firewalls: building in that peaceful, easy feeling. *Network Computing* 5(6):159

Ranum, M. (1994). Internet firewall protection. *Open Computing* 11(9):95

Snyder, J. (1995). Choosing the right firewall to defend your network: a host of products can protect confidential network information from Internet snoopers. *Network World* 12(10):1

Tristram, C. (1995). Ten things you need to know about firewalls. *Open Computing* 12(5):61

Note: The NCSA founded the Firewall Product Developers= Consortium in June 1995. Its objectives, as defined by Bob Bales, the Executive Director of the NCSA, are to:

- Increase public awareness
- Provide forum for product developers to discuss issues of mutual concern
- Encourage sharing of technical information to improve products
- Provide focal point for industry representation in dealing with the press
- Undertake special projects such as white papers and market research
- Establish product testing and certification guidelines.

18. S.A.T.A.N.

McCarthy, S. P. (1995). Free program will detect SATAN probes. *Government Computer News* 14(8):6

Rupley, S. (1995) Satan: good or evil? *PC Magazine* 14(11):31
Streeter, A. (1995). The good and bad of SATAN. *MacWEEK* 9(19):18

19. A more detailed look at PC security:

Cobb, S. T. (1995). _NCSA Guide to PC and LAN Security_. McGraw-Hill (New York). ISBN 0-07-912168-3.

<<end of chapter>>

The NCSA Guide to Enterprise Security

File: 09 Criminal Hackers.doc

Chapter 9: Criminal Hackers

Objectives:

After studying this chapter, readers should be able to

1. Describe criminal hacker methodology, psychology and motivations.

2. Explain the need for a Computer Emergency Response Team in each organization.

3. Establish countermeasures to reduce the likelihood of system penetration by criminal hackers.

1 The Hacker Problem

I used to laugh at the following quotation; now I'm not so sure it's funny:

`Today, there is virtually no system or network, either telecommunications or mainframe computer, that has not been compromised. Tens of thousands of juveniles, equipped with home computers and modems, regularly make attacks on systems. Hundreds of adults, motivated by the potential for financial gain, openly aid and abet the hackers. A new breed of criminal is emerging and unfortunately appears to be here to stay. You can be sure that they are out there right now trying to crack your system!' (Maxfield, 1985)

Are there really armies of sinister figures covertly breaking and entering into our computers? Isn't that paranoia?

For Cliff Stoll, an astrophysicist at the Lawrence Berkeley Laboratory in California, the sinister figures existed. He tells a fine tale in his engaging, informative and intelligent best-seller, ***The Cuckoo's Egg.*** Seconded from the astronomy section to the computing section because of budget cuts, he began a mundane assignment tracking down a 75-cent discrepancy in the system accounting routines and ended up fighting an international ring of determined spies who were

Copyright 1996, 2004 M. E. Kabay. All rights reserved.

cracking computer systems all over the United States. Incidentally, he plays himself in a televised version of his story shown on the U.S. Public Broadcasting System in the acclaimed NOVA series of science programs; it's called "*The KGB, the Computer and Me.*"

Articles are appearing regularly in the trade press about users of on-line services experiencing harassment on the Net; for example, Menke (1995) complains about having her credit-card information stolen and misused and also about volleys of offensive e-mail arriving in her in-box. The crudity and incivility of many men on the Net has driven away some women and pushed others into using male pseudonyms to avoid unwanted attention in cyberspace.

Having said that, before we launch into an extended discussion of criminal hackers, I want to point out again that most computer crime is carried out by insiders. Burger (1995) quotes estimates by Sgt. Craig Hannaford of the Royal Canadian Mounted Police's technological crime section suggesting that 90% of all computer crime is committed by employees of the victim. The same figure pops up in reports from the UK's National Computer Centre (Kelly, 1995).

It remains a fact, however, that the increase in computer-literate young people is increasing the number of attacks on systems, especially those linked to the Internet. It appears to be true that as some of these young criminal hackers enter the legal age of majority, they turn to organized crime and earn money by stealing information (e.g., credit-card and phone-card numbers) for use by international drug cartels and others.

2 History and current status

According to Bloombecker (1986), computer hacking has some of its many roots in the evolution of the interstate phone system. When direct distance dialling (DDD) was implemented in the late 1950s, AT&T began using audible tones which conveyed switching and billing information for the phone network. These tones can occasionally still be heard in the background of a switched phone line when we dial a long-distance number; listen for a rapid series of faint sounds shortly after you finish dialling or punching the touch-tone buttons. The `blue box' became popular around 1961 as a method for avoiding long-distance costs. This device generates the tones used for internal communications by the phone system and sent false information to the billing office. Thus thieves were able to defraud the phone company of their long-distance phone charges. These people became known as `phone phreaks'.

Even today, experts say, phone fraud is still a problem. Eckerson (1990) asked Meglathery, `We hear a lot about threats to data networks, but what are the big problems with voice nets?' Meglathery answered, `Credit cards are the biggest problem. Evidently, some kids in New York are using binoculars to read the calling card numbers of people who are making calls at pay

Copyright 1996, 2004 M. E. Kabay. All rights reserved.

phones. Phone companies have had to write off hundreds of thousands of dollars of bad credit card calls as a result.'

A recent variation is the voice-mail criminal hacker. Many organizations use sophisticated computer-controlled internal phone systems that give every user a private mailbox for storing verbal messages. In a recent case, two teenage brothers from Staten Island, NY caused an estimated $2.4 million in lost business and extra work by hacking into International Data Group's voice-mail system in New Hampshire (McMullen & McMullen, 1990). The youngsters, angry at not having received a poster promised with their magazine subscription, penetrated system security, changed mailbox passwords and deleted advertising copy left by phone. At first, technicians assumed there must be a problem with the system. However, the vandals began leaving offensive and even obscene outgoing messages ostensibly from company employees. When customers complained about the tasteless greetings, management finally realized the system was under attack. The pests were finally trapped by putting a trace on the toll-free 800 phone number.

Another root of modern hacking is time-sharing. This operating system development arose in the early 1960s and allows a multitude of users the illusion that they have the undivided attention of a computer. Thousands of university students became involved in using, modifying and creating sophisticated operating systems, thereby gaining life-long interest in computing machinery and telecommunications. With modems to allow easy communications through ordinary, voice-grade switched telephone lines, the stage was set for the birth of the modern criminal hacker.

The forced breakup of AT&T around 1980 spawned hundreds of local phone companies (sometimes called BOCs, or Bell Operating Companies) who had to pass billing codes from company to company as each long-distance call flashed across the continent. Unfortunately, notes Bloombecker, AT&T failed to make its ANI (automatic number identification) feature available to the BOCs, so it became much more difficult to track fraudulent use of the interstate phone system.

Finally, the advent of packet switching networks (e.g., TELENET, TYMNET, and DATAPAC) increased the ease with which criminal hackers could reach across great distances to attack host computers. Criminal hackers in major cities could simply dial a local call to a handy access node and then try hacking their way into any computer on the network--even on the other side of a continent. No more long-distance calls. Furthermore, on most networks, there are no logon IDs for network use proper; instead, the host is billed for connect time and then bills its users. If a criminal hacker fails to connect properly to a host, there are no penalties at all.

Copyright 1996, 2004 M. E. Kabay. All rights reserved.

3 Hacker Techniques

Hackers can attack any system which allows outside access. In addition, with the advent of customer-premises equipment that includes telephone switches linked to internal computer networks, companies are vulnerable to criminal hackers even if they think they have no outside ports. Beyond the technical attacks for forced entry, criminal hackers can also use deception (false representation, impersonation, outright lies) to gain information about access codes.

3.1 Forced entry

Criminal hackers depend on public or private access ports. If your computer cannot be accessed outside your offices, you're probably safe against criminal hackers. It is the combination of switched (dialup) telephone lines and inexpensive modems that makes hacking a hobby. To locate telephone numbers, criminal hackers either find them or learn them. I once saw a telephone number printed out as a banner posted on a computer room wall (through the glass windows, another no-no) in letters a foot high. It was the dialup modem. To learn phone numbers, criminal hackers ask each other. It seems that criminal hacker bulletin board systems (BBS; see below) routinely traffic in stolen modem numbers. Even without relying on other criminal hackers, if a criminal hacker knows that a particular target organization uses a particular exchange (e.g., 342-xxxx), s/he can use a brute-force method to find the modem: just have a computer program dial every number in the exchange and record all the numbers that have carrier signals. The modem identifies VOICE or NO CARRIER (no answer) and CONNECT 1200 or CONNECT 2400, so it isn't hard to figure out what's on each number.

Once the modem has located a carrier signal, the criminal hacker can try logging on. Criminal hackers become expert at identifying the type and operating system of computer they've reached. Some systems, especially simple BBS, announce precisely what kind of hardware and software they are running on right from the start, even without appropriate IDs. These systems are practically begging for criminal hackers to use their specialized knowledge of hardware and software to bypass security. Others have characteristic prompts; e.g., the : that follows a carriage return is a giveaway for either an HP3000 or a TANDEM. Some systems have overly helpful error messages; the default set for MPE leads a criminal hacker step by step through the logon process (see box). Luckily, it is not difficult to change the HP3000 message file, CATALOG.PUB.SYS, to substitute something like *INVALID* for all these helpful messages (use the GENCAT.PUB.SYS utility).

```
A CRIMINAL HACKER/HP3000 DIALOGUE
(lowercase is what the criminal hacker types, UPPERCASE is HP3000 response):
:
:fjfjd
EXPECTED HELLO, :JOB, :DATA, OR (CMD) AS LOGON. (CIERR 1402)
:hello
```

Copyright 1996, 2004 M. E. Kabay. All rights reserved.

```
 HELLO
EXPECTED [SESSION NAME,] USER.ACCT [,GROUP] (CIERR 1424)
:hello manager
 HELLO MANAGER
EXPECTED ACCOUNT NAME. (CIERR 1426)
:hello manager.system
 HELLO MANAGER.SYSTEM
NON-EXISTENT ACCOUNT. (CIERR 1437)
:hello mgr.sys
 HELLO MGR.SYS
ACCT EXISTS, USER NAME DOESN'T. (CIERR 1438)
:hello manager.sys
ENTER USER (MANAGER) PASSWORD: manager        [passwords are not visible]
ENTER USER (MANAGER) PASSWORD: reganam
ENTER USER (MANAGER) PASSWORD: super
INCORRECT PASSWORD. (CIERR 1441)
NO CARRIER                                    [message from modem]
```

Techniques for guessing passwords range from brute-force battery to sneaky psychology. One brute-force approach would try words drawn from an online dictionary; passwords like ROVER and DOLLY would pop up eventually during the search. An even more exhaustive search would generate all possible random sequences of the ASCII symbols, starting with short combinations and letters only and then moving on to longer ones including special symbols. A more subtle approach works by learning about the user of a particular password. `Dumpster diving' involves searching through rubbish looking for discarded information that can give clues to probable passwords; researching the user's background can lead to possible words too. These techniques don't work unless the user has foolishly chosen words that have personal meaning; e.g., names of spouse and children or of favourite sports.

Brute force methods will work efficiently only if the operating system allows unlimited, rapid retries after password failures. The HP3000, for example, puts a message on the system console after every bad logon attempt. After three password failures, the system prevents further attempts until a configurable delay has expired (e.g., 2 minutes by default).

Recent developments in password technology may improve our chances against hackers (Alexander, 1990). A mechanical engineer, Earl R. Collins Jr, has devised a system using a symbol matrix for enforcing access codes. Both computer and user need a copy of a square grid containing many codes. The computer randomly selects any two locations on the grid, defining a rectangle; the user would have to name the codes on the other two corners of the rectangle. The number of possible rectangles and codes is so large as to be virtually uncrackable by brute-force methods.

In the example of logon dialogue with an HP3000 shown above, the computer hung up its modem. A hacker would have to redial to get through for another try, slowing down the process

Copyright 1996, 2004 M. E. Kabay. All rights reserved.

and either frustrating the human or giving an operator on the targeted computer a chance to set up some counter-measures.

3.2 Social Engineering

Criminal hackers rely on lies to trick employees of a firm whose computers they want to crack. They can befriend people and casually move the conversation towards details of logon procedures and access codes. They can phone staff members and pretend to be befuddled or angry authorized users in an attempt to wheedle or bully passwords out of the victim.

4 The hacker subculture

Criminal hackers inhabit a world cut off from the normal give-and-take of social contracts. They boast and strut for each other electronically, often adopting fantastic names and aggressive personae that are frequently belied by their unimpressive selves.

One of the classic accounts of first contact with the hacker underground was written by John Barlow, who founded the Electronic Freedom Foundation with Mitch Kapor and others in 1990. He noticed that two odd names had joined the Whole Earth 'Lectronic Link (the WELL): Phiber Optik and Acid Freak. As these young hackers engaged in electronic discussion and debate, it became clear to all that they had highly idiosyncratic--not to say sociopathic--views of normal human relations in a civilized community. For example, they explicitly felt that weak security deserved to be broken--and this principle extended to unlocked homes.

Another interesting report on the hacker ethos comes from Piglia & Rayl (1992), writing in ***Omni*** magazine. They review some of the roots of the cyberpunk phenomenon, including science fiction writers like William Gibson, author of the novels ***Neuromancer***, ***Count Zero*** and ***Mona Lisa Overdrive.*** The cyberpunks espouse a philosophy, if that's the word, of untramelled electronic liberty. Knowledge and computing power are supposed to be available to all in an anarchic free-for-all. Worried by the growth of trans-national corporations, some of the more politically-minded cyberpunks foresee a world divided into information haves and have-nots. The article continues with a review of the musical cyberpunk scene.

4.1 A Rogue's Gallery

Several popular books have provided insights into the psychology of criminal hackers. The following brief notes present highlights (or lowlights?) of some hacker careers and personalities.

4.1.1 "Susan Thunder."

Copyright 1996, 2004 M. E. Kabay. All rights reserved.

Family breakdown. Gawky, buck-toothed little girl. Rejected and abused. Random phone caller by age 8. Dropped out of grade 8. Ran away from home. Lived on streets of Hollywood. Took name Susy Thunder. Prostitute by age 14. Rock groupie. Quaalude-, alcohol-, heroin-addict. Thrown out of rehab program. Joined telephone conference calls as antidote to loneliness. Used lies ("psychological subversion" or "social engineering") to get backstage passes to concerts. Seduced military officers in order to search their possessions for passwords and access codes. Learned PDP-11 operating system by herself. After discovering Roscoe's unfaithfulness to her, she threatened him with disclosure to FBI and then asked him to marry her.

On warpath, Susan left spiteful messages on Roscoe's answering machine. Arranged to have him fired from his job. Testified against Roscoe and Kevin at their trial in return for immunity from prosecution.

In 1982, she was arrested for prostitution. In 1984, she and a friend tried to release Steven Rhoades from jail by impersonating a deputy district attorney. She became a professional poker player.

4.1.2 "Roscoe."

Called reporter looking for info about HOBO-UFO conference call system and announced himself by listing "billing name on this unlisted phone number, his home address, the year and make of his car, and his driver's license number." "Roscoe claimed that he had acquired as much knowledge about the telephone system and the computers that controlled it as anyone else in the country.... He boasted that he could order prepaid airline tickets, search car registrations and even get access to the Department of Motor Vehicles' computer system to enter or delete police warrants." Well-organized lists of personal info and personality of contacts for use in social engineering. "Presenting a stranger with a litany of personal facts and watching him or her come unhinged gave Roscoe his greatest pleasure." Betrayed Susan by concealing his relationship with a prim and proper law school student. In interviews, "There was something oddly mechanized about Roscoe's language.... formal, almost bureaucratic way of speaking.... curious affection for the passive construction." Lived with his mother in a slum. Spontaneously insulted religious people for fun. Stole long-distance phone services from corporate systems. "Roscoe regarded ... [users of his conference line] ... with ... delight at their obvious respect for him, and disdain for the emptiness in their lives."

Gave himself system privileges at U.S. Leasing in San Francisco; offered guided tours to hacking neophytes. When he was refused access one night after a preliminary lie to the system operator, he caused the system printer to print thousands of pages reading, "THE PHANTOM, THE SYSTEM CRACKER, STRIKES AGAIN. SOON I WILL CRASH YOUR DISKS AND BACKUPS ON SYSTEM A. I HAVE ALREADY CRASHED YOUR SYSTEM B. HAVE

Copyright 1996, 2004 M. E. Kabay. All rights reserved.

FUN TRYING TO RESTORE IT, YOU ASSHOLE." Other pages consisted of the words "FUCK YOU!" repeated hundreds of times. Deleted all inventory, customer, and billing information and substituted obscenities.

First message to Bernard Klatt, sysop of 8BBS, a phreak bulletin board:

"... I AM ROSCOE, FAMOUS IN L.A., CA AND IN THE PAPERS OF L.A. FOR MY PHONE-COMPTR PHREAKING, FREE ACCESS TO ALL, AIRLINE TICKETS, ETC.... I WILL BE LEAVING YOU MORE DETAIL MSG WITHIN 7 DAYS BECAUSE I CAN BE OF GREAT ASSIST TO YOU AND ALL USRS. BASICALLY: TELL ME WHAT INFO TO WHAT YOU NEED, I CAN GET . . . ANYTHING. FREE AIRLINE, FREE HOTEL, FREE CALLS . . . BEST PHONE PHREAK IN L.A.! (I HAVE REPUTATION) AND ANM KNOWN BY MANY, WAS ON THAT'S INCREDIBLE, T.V. SHOW IN L.A., AND AM MOST POWERFUL IN LA.A.... CAN CRASH SYSTEMS WITHIN 20 DAYS OF REQUEST TO DO SO, CAN GET ANY PHONE NO TO ANYTHING!!!...."

Inordinate amount of time phreaking: "MY INFORMATION GATHERING IS TAKING UP ABOUT 4 TO 5 HOURS OF MY TIME EVERY DAY, AND THAT'S TOO MUCH CONSIDERING THE FACT THAT I WORK FULL TIME AND ATTEND SCHOOL FULL TIME."

Broke into Pacific Bell and stole reference books for COSMOS software. Charged and convicted with computer fraud and burglary.

4.1.3 Steven Rhoades.

Prankster. Dirverted directory assistance for Providence, R.I. to themselves and gave outrageous answers ("the number you have requested is 8750 and a half.")

4.1.4 Leonard Mitchell DiCicco ("Lenny").

Began cracking security in his high school days. Poor attendance at school made worse by friendship with Mitnick. Would use Radio Shack demo computers for hours until managers would throw them out. Used USC computers despite not being students there. When arrested and handcuffed with Mitnick, stole handcuff key and unlocked his own and Mitnick's handcuffs. Proposed that Mitnick escape from custody. Expelled from Pierce College along with Mitnick for security violations. Worked as a flower delivery man. Betrayed his long-time friend Mitnick to the FBI during the VAX source-code theft. Became a security consultant after being freed from jail.

4.1.5 Hans Heinrich Huebner ("Pengo").

Copyright 1996, 2004 M. E. Kabay. All rights reserved.

Born 1968 in West Berlin. Raised in a permissive home and went to special Kinderladen nursery school where children were encouraged to determine their own diet, when they ate with utensils and when their diapers needed changing. Parents divorced when Hans was in elementary school. Teachers complained Hans was lazy and disruptive; mother would ignore his grades. When moved up a year in school, he became even more withdrawn. At 12, began squatting in abandoned buildings with punk rock band. Grew six-inch spikes of jet-black hair; wore black military boots, heavy chains. Began stealing from stores; overdosed on alcohol and marijuana and passed out at a rock concert.

Early forays into computer illegality included systematically breaking copy-protection on Sinclair games. Found ways of sabotaging video games at local arcade for free games. Would spend all day and all night at video arcade, skipping school entirely. Also worked part time there distributing pornographic videos.

By late 1985, Huebner was spending almost all of his time working through his modem, cracking networks and systems. Joined CHAOS Computer Club from Hamburg.

By early 1985, had penetrated SLAC (Stanford Linear Accelerator Center) computers through Tymnet and stolen NUIs. Crashed the SLAC system by launching a small, rapidly-replicating worm. Broke into CERN and participated in ruining an open, friendly environment by abusing its resources.

Began trying to sell stolen information to Soviet intelligence in 1986. Stole a copy of a security program from a DEC VAX in Singapore and offered it to the East German contact. Became deeply involved in theft/espionage ring.

Lied to his partners about how he was paying for network connection (he was actually using stolen NUIs) and took the money they offered to defray expenses for legitimate NUI he was supposed to be using. Then he asked his "friend" Petter Carl for a legitimate NUI--and proceeded to run up bills of 4000 DM in a single month.

A lawyer asked him, "Did you have any scruples about what you were doing and did you consider whether it was unethical?" He answered, "I don't care about ethics.... I don't care about that stuff." He began working undercover with the criminal investigation services of the West German police, informing on his colleagues. His hashish addiction worsened, and he increased his compulsive use of coffee and nicotine.

4.1.6 Karl Koch ("Hagbard Celine").

Father abandoned his mother with him and small sister when they were infants. Mother died of cancer with Karl watching. Father, alcoholic high-profile journalist, died of cancer when Karl

Copyright 1996, 2004 M. E. Kabay. All rights reserved.

was 16. Inherited about 100,000 marks as bought a Porsche and rented an apartment. Drug addict: daily, constant ingestion of hashish, LSD, cocaine, amphetamines. Conspiracy freak; perceived himself as a character (HC) from a fantasy novel dealing with worldwide conspiracy. Apartment a chaotic mess. Worked for the W. German authorities after betraying his "friends" to save himself. Burned himself to death in May 1989.

4.1.7 Dirk-Otto Brzezinski ("Dob").

Brilliant systems programmer. Addicted to hashish; alcoholic. Periodically deeply depressed. Claimed at his espionage trial that he and his friends had sold information to the KGB as a step towards world peace--the first time any such reference had been made in all his 193 pages of prior testimony.

4.1.8 Peter Carl.

Orphan. Dropped out of technical school. Worked at casino; drove cars from Germany to Spain. Convicted drug trafficker; on probation for smuggling hashish. Unemployed from 1986 to 1989.

4.1.9 Markus Hess.

Middle-class, unremarkable childhood. Model son; did well in school. Worked as UNIX programmer. Enjoyed illicit thrill of criminal hacking. Impressed by Koch, he became addicted to hacking UNIX systems. Stole copy of UNIX source code licensed to his employer and gave it to Carl. Koch and Brzezinski sold it to the East Germans for 25,000 DM. When arrested in March 1989, he instantly incriminated his "friends" but denied knowledge of espionage. He lied until confronted with undeniable facts.

4.1.10 Paul Bedford.

At 14, received a computer and became obsessed with hacking. Was accused of unauthorized modification and access of computers and material and conspiring to obtain telecommunication services dishonestly. He also appears to have broken into British Telecom's systems and traipsed through a Lloyds Bank computer system. According to prosecutor James Richardson, "He was tapping into offices at the EC in Luxembourg and even the experts were worried. He caused havoc at universities all around the world so that the computer systems were inaccessible to anyone but him." Despite considerable evidence, including the guilty pleas of Bedford's confederates, Karl Strickland, aged 22 in 1993 and Neil Woods, aged 26 in 1993, Bedford was acquitted of all charges on grounds of a form of insanity: addiction to computer hacking.

4.1.11 Mark Abene.

Copyright 1996, 2004 M. E. Kabay. All rights reserved.

Brilliant child from a middle-class district of New York who learned the alphabet before the age of two; apparently has an eidetic memory. As a little boy, he took apart a broken cuckoo clock and put it back together again--and it worked perfectly. Quickly became an expert in using and abusing telco phone switches. Became active in the BBS subculture as "Phiber Optik," well-known teacher and phreak. Notorious for insulting less-competent hacker youths, especially when they posted inaccurate information in their "philes" and messages. Joined the Legion of Doom hacker club led by Chris Goggans ("Eric Bloodaxe") and others. Eventually fell out with his new friends when he apparently applied some social engineering skills (lying) to one of Chris' friends to obtain a new access code for the NYNEX Packet Switched Network. When Chris demanded payment (a list of codes for cracking computers linked to the Telenet service), Mark insulted him, then hung up on him. The ensuing "war" is the subject of Slatella and Quittner's book. Mark Abene was eventually sent to jail in 1994 for a year. When he was released, he was treated like a hero by members of the hacker underground.

4.2 Kevin Mitnick

One figure stands out as the single most notorious and also pathetic criminal hacker in recent years: Kevin Mitnick.

Mother, waitress, divorced when he was three; succession of short affairs. Father remarried, had athletic, handsome son. Kevin became short, fat, shy slob. "Avoided eye contact." Photographic memory. Malicious: "This curiously oafish friend of Roscoe's always seemed to be busy carrying out revenge of one sort or another, cutting off someone's phone service or harassing people over the amateur radio." "Lenny watched one evening as Kevin attached a local hospital's $30,000 phone bill to the home phone of a fellow ham radio buff whom Kevin disliked."

Accomplished liar: as a phone imposter, could wheedle passwords out of victims. Participated in theft at Pacific Bell, then turned state's evidence in return for lighter (suspended) sentence.

Worked at odd jobs such as delivery boy for delicatessen. Expelled from Pierce College in 1982 for tampering with school's computers.

Went to jail for 6 months a few years later for breaking into USC computers and stealing University accounting data. Became a fugitive from justice when he learned there was an arrest warrant for him on telephone fraud charges and breaching the conditions of his parole. Lied by using an assumed name at Butte College in northern California.

In 1987, Mitnick broke into SCO computers--a felony; arrested and plea-bargained a misdemeanour charge by explaining how he had done it. Got small fine, 36 month probation. During meeting with SCO admin, Mitnick sullenly responded to SCO attorney instead of admin;

Copyright 1996, 2004 M. E. Kabay. All rights reserved.

adopted a condescending attitude. Yet one year later, he had the gall to ask the admin for a job at SCO.

When Mitnick heard of a security memo at Pacific Bell, he called the author's secretary and lied: claimed he was a different security manager. Diverted phone call placed by secretary's FAX so FAX went to Roscoe's FAX--programmed to simulate correct receiving FAX.

On Feb 17, 1988--while still on probation--Mitnick and Lenny tried to steal $20,000 of software from Pierce College. On March 17, they impersonated a security guard and called a computer science instructor and 2 other officials at 03:00 and told them to come to the comp sci labs because they (Mitnick and Lenny) had been apprehended during a burglary.

In March 1988, Mitnick got a job at Security Pacific by lying on his application; denied his arrest record. Misrepresented his delivery boy job at Fromin's Delicatessen as that of programmer/analyst. Job offer withdrawn when truth came out thanks to police efforts. Two weeks later, the Bank was notified that a fraudulent press release in its name had been sent to a news wire service claiming first-quarter losses of $400 million. No evidence ever surfaced linking the fraud to Mitnick.

Mitnick threatened to ruin his long-time pal Lenny DiCicco by revealing that he had lied to get a flower-delivery job.

He and Lenny cracked the USC computers again in the summer of 1988. They misappropriated hundreds of Mb of disk space to store VAX VMS source files stolen from DEC. Fired from his job at electronic testing equipment firm for excessive phone calls from work. While he was hacking, he would lie to his wife and claim he was at evening class at UCLA. Mitnick and Lennie eavesdropped on email between DEC scientists working on VMS security and used the holes to enter other VAXen.

Because Mitnick had altered Pacific Bell computers so that phone traces led to random phone numbers; one victim was watching TV when the FBI burst into his room searching for computer equipment.

Mitnick impersonated an IRS official and tried to have his friend Lenny's pay cheque withheld. Then he forwarded all of Lenny's employer's phone lines to a single number and made all the inbound lines busy as a result.

Mitnick's habit at the fast-food restaurants where he ate almost all the time was to empty half a dozen ketchup packets onto his place mat and then jab French fries into the sauce.

Copyright 1996, 2004 M. E. Kabay. All rights reserved.

Mitnick was arrested by the FBI for having stolen VAX VMS source code. During his trial, he was described as suffering from an impulse-control disorder. In July 1989, he was sentenced to a year in jail and six months rehabilitation. He later tried to become a private investigator and security specialist. He was generally treated with hostility by the established information security community.

In November 1992, Mitnick went underground again when the FBI got a warrant for his arrest on charges of--yes, once again--stealing computer time from a phone company. He was located two years later when he made the mistake of leaving insulting messages on the computer and voice-mail systems of a physicist and Internet security expert, Tsutomu Shimomura. Shimomura was so irritated that he helped law enforcement authorities track the fugitive to North Carolina, where Mitnick was arrested.

4.3 Know Your Enemy

It's always instructive to listen carefully to an enemy. The books mentioned in the references at the end of this chapter include quotations of conversations and postings by many criminal hackers.

In an article published in *Computerworld* in 1992, Chris Goggans, a notorious criminal hacker from the "Legion of Doom" gang, published a defence of hacking, claiming in the title, "Hackers aren't the real enemy." His key points were as follows:

- Yes, criminal hackers break the law--but they're not criminals!
- Criminal hackers are motivated primarily by a desire to learn about computer systems.
- Laws protecting private property are simply obstacles to be overcome.
- Hackers are admirable because of their lack of prejudice about each other.
- They seem to be a bit compulsive about their hacking.
- Although criminal hackers are smart, they do badly in school.
- Criminal hackers distrust authority of all kinds--except other hackers.
- Criminal hackers are just a nuisance; they generally do no harm when breaking into systems and "merely" exploring.

Copyright 1996, 2004 M. E. Kabay. All rights reserved.

o The victims of criminal hackers are to blame for their own victimization because their security is so poor.

Enraged, I wrote the following, submitted it within a few days to *Computerworld*, and was informed that I had been beaten to the punch by one of the editors (Patricia Keefe). My rant was published in *Computing Canada*.

Recently, a hacker got a chance to defend himself and his buddies in the pages of a major American computer trade journal. The hacker tried, and failed, to disguise a defence of illegality as a call to arms for better information security.

No one claims that hackers are the main problem. It is a commonplace that about four-fifths or five-sixths of all damage to information systems is due to human error and wrongdoing by authorized users. No one knows for sure, since we base our estimates only on those cases that are discovered and reported.

The hacker admitted to having broken into private systems, but claimed he never disrupted the operation of business.

Rubbish. Every time a penetration is discovered, it causes operational disruption. It is true that not all break-ins are followed by theft of or damage to data. However, since no one can know without examination whether a hacker has modified data, production may have to halt until data integrity is verified.

> In large installations, where data may be measured in terabytes, such verification may take hours or even days.
>
> During this time, personnel who should be concerned with their normal business have to act as detectives and auditors.
>
> The hacker claimed he and others turned to cracking because they were deprived of the opportunity to learn about operating system internals. That is nonsense. No one has to break the law to learn about computers. There are free books at local and academic libraries; there are local, regional and national computer user groups; and, one may even be able, as the hacker himself admitted, to gain access by merely talking to administrators.
>
> He admitted that he and his friends read restricted files. However, there is no link between reading a confidential database and learning about computers. On the contrary, reading private information is not a trivial crime.

Copyright 1996, 2004 M. E. Kabay. All rights reserved.

Hackers are known to traffic in personal information of all kinds, including credit-card and telephone access card numbers.

These people no more contribute to awareness of the need for improved security than ruffians contribute to public safety.

People who break the law and invade our privacy have no business lecturing us on how shockingly bad our security systems are. The National Computer Security Association (NCSA) is preparing a series of studies of beliefs, attitudes, and behaviour of students in elementary schools, high schools, and colleges and universities about the ethical use of computer systems.

Our goal is to identify, create and distribute teacher-training materials and student curriculum to prevent more children from turning into muddle-headed, amoral hackers.

4.4 Hacker Bulletin Boards

Even in the mid-eighties, Maxfield (1985) estimated that half of all private BBS cater to software pirates. He notes that underground systems usually have elaborate security (better than many legitimate organizations' security) and some sections hidden from normal users. Entry into the inner sanctum of pirated passwords, break-and-entry techniques for specific operating systems, and dialup modem numbers for specific victims requires contributing a piece of illegally-obtained information. Maxfield thinks that some BBS are being infiltrated by organized crime syndicates because of the potential for selling stolen computer components, blackmail, and narcotics distribution. Pirate BBS operators have been known to threaten the lives of undercover investigators who have infiltrated their systems.

The National Computer Security Association is engaged in a program of constant investigation of such sources of information, including BBSs, Internet news groups, and electronic and paper publications catering to the criminal underground. The NCSA's IS/RECON service compiles and indexes all sources of information about criminal hackers it can reach throughout cyberspace and makes these files available for searching by subscribers from government, academic and commercial enterprises. The files and indexes are updated weekly and amount to gigabytes of data.

4.5 Hacker Conventions

Criminal hackers seem to enjoy having conventions, just like normal people. Of course, they have their own ideas on what constitutes fun, and they certainly have odd notions of civilized behaviour. I attended the HoHoCon in December 1993 in Austin, Texas, and wrote notes for the

Copyright 1996, 2004 M. E. Kabay. All rights reserved.

NCSA News article, "On the Margins: Reflections on HoHoCon 93." I hope these extracts will give readers a taste of the flavour of the meeting, obscenities and all.

Conversation Pit, Friday evening 17 Dec

> [Arrived hotel around 20:00. Deliberately wore my navy blue suit and a sober tie as a provocation. Joined about 10 people in a "conversation pit" in the lobby of the Hilton. Most wore jeans (many with the obligatory holes slashed above the knee), longish hair, and backwards baseball caps. Certain amount of wariness as I entered the conversation. People asked who I was ("sir") and stepped back with widened eyes when I smilingly answered that I represented the NCSA]
>
> Met a Russian hacker from Moscow who now works part time in Texas. Asked him about the effectiveness of the U.S. ITAR (International Traffic in Arms Regulations), which tries to restrict export of cryptographic algorithms, software and hardware. He laughed and said that encryption is widely and easily available in Moscow.
>
> [A snaggletoothed man with rotting teeth, a wizened face and curly grey hair spoke with me. He turned out to be the infamous John Draper, better known in hacker circles as Cap'n Crunch. He was one of the earliest of the phone phreaks, reported to have discovered that a whistle found in a Cap'n Crunch cereal box could be used to trick the phone company's switches into initiating long distance calls for free. I asked him what he was doing these days.]
>
> He's interested in cultural issues, privacy. Has a first-hand perspective on how Ravers are using PGP to protect their privacy and run their parties without interference. He was invited to participate in the rave scene to see how encryption is being used to pass the word about location of the next rave to many people without police interference. Police would subscribe to an Internet mailing list, but now the organizers use PGP to protect the messages against interception. The volunteers then phone their "cells." Police don't attend all the raves, so ravers are building a trusted hierarchy by using only people who attend all of them.
>
> [How does he earn a living these days?]
>
> He teaches exercise and evaluates people's personality by the way they respond. Learned to dance right using advice Hatha Yoga master; now capable of dancing 80 hours without sleep. Claims to sleep 4 nights week.
>
> Why go to raves: they are his fountain of youth. Get energy, power, companionship, family. Gets tough gang members asking him how he has all that energy (he's 50). Goal

Copyright 1996, 2004 M. E. Kabay. All rights reserved.

is to generate smiles. On the invitation list for all the raves. Plans to stay awake through the entire HoHoCon.

How does he earn a living? Personal training sessions. Used to be software engineer; but with 11,000 out-of-work Mac programmers, he's waiting for an opportunity. Would love to work. He's a hard worker.

[Tell me about how you got involved in phone phreaking and how you feel about it.] Twenty years ago, my sole purpose in phreaking was to learn about the system. I made no money on it. One day I got a call from Steve Wozniak. He built a blue box and asked me how to use it. I didn't know that he intended to sell them--put himself through college. Wozniak sold a blue box to one of my friends who got busted. My name was on his phone list, so I got busted--grand jury indictment. Convicted. Yet I had helped the phone company on many occasions in identifying bad trunks and keeping the line quality high. We were responsible for helping fix many problems in the switch. For example, there was a fuckup in their translation code which allowed a signal to bounce back and tie up more and more lines until all the intercity lines were busy. We identified the problem and told the AT&T long-line engineers and insisted they fix it right away. With this bug, it would have been possible to tie up all the lines between any city during the 1972 Republican Convention in Miami.

After I got busted I couldn't keep a job; took a lot of energy clearing my record. I no longer have the felony on my record. It's all water under the bridge. Right now, I'd like to have a 9-t-5 permanent job so I can pay for going to raves. I can't reach the American Dream right now because of mistrust. I work hard and play hard--far above and beyond anything anyone can imagine.

[What would you tell a 13 year old who's getting into phreaking and hacking today?] There's this old guy named Darwin. This dude went to the Galapagos Islands and discovered that there's security in obscurity. If you expect to hack and be destructive and destroy valuable work on systems, then you deserve to get visited by the Secret Service. If you somehow manage to get in, don't do anything harmful. If you discover a security hole, you'd be much better letting the security manager know. Maybe you'll get a job.

[How do you respond to system managers' concern over unauthorized and unknown actions on a production system?] If I had a computer system hooked up to a public access dialup port or the Internet, and if I didn't want to have unauthorized use, I'd put a stern and clear warning in the login banner. I would do everything in my power to keep hackers out.

Copyright 1996, 2004 M. E. Kabay. All rights reserved.

[Note: Draper constantly picks at his bleeding hands and eats the skin fragments.]

But if there's a system that doesn't say what it is, it's an invitation to hackers. There's safety in numbers. A mysterious login prompt attracts attention. [Others agree: If you don't want anyone logging on, make it look like a VAX.]

Citizen Fish said he'd stay out of a system if it had no obvious identifier. He continued, I just keep it as a game.

It's not really like someone entering your home or your car; but it is a bit like opening up your daytimer.

I don't get any fun from stepping on the little guy.

At this point, Drunkfux, the organizer announced, "The police are arresting people in 293 because they set up a BBS and accused them of hacking. In another room, people really were hacking, so they're being arrested. Is there anyone from the EFF here? Or any adult? Some of these guys are minors and I'd hate to have them get into trouble."

Citizen Fish continued, the little guy is my fellow man. Reading email is just boring. What I like is being able to infiltrate big secure, hard systems.

A hacker known as AK said, The system managers at my college explained the security holes and told me how to hack. At that point, there was no longer any interest or fun.

Citizen Fish said, There's no fun in breaking into some lame company system. It's the challenge of breaking in--I'm smarter than they are. I have been tempted to crash systems, but I don't.

AK: I'm 16; there was no practical way I could get a job programming. You can program for yourself, but I had to break in to get access.

CF: I've never had any money for books.

AK: I'm now in college, primarily for access to the system.

CF: Reading a book is wonderful.

AK: There's a set of telephone system manuals; there's a thrill to reading them.

[Is it the thrill of the illicit?] Nah. We could just go steal a car. Boring.

Copyright 1996, 2004 M. E. Kabay. All rights reserved.

AK: I would say a good book is like a good hack--different, though.

CF: There's a real rush of adrenaline in hacking a system.

AK: Maybe there's a thrill from knowing that you're a little guy who can overcome the barriers big people put up.

Another person announced, "They're harassing policemen in the other building."

Kevin (Engineer): I find that these people are playing with what other people have built.

[What about virus writers?] I haven't run into any virus writers since Viper died.

There are laws in some places against any program that harms data. So I think Microsoft Windows is a virus. Central Point Software know that there are problems in their programs; they deliberately provide updates to fix bugs.

Writing a virus was once a challenge--make it as small as possible. But now the virus has become political. The anti-virus writers are fostering hysteria.

I think that programming viruses is challenging because you're beating the AV writers. [How do you respond to VCL, MTE, TPME?] Dark Avenger viruses are well thought-out. he had to have skills to write this. In writing the MTE, he upped the level of hi expertise. But if one of us just uses the MTE it shows no skill at all.

Others: Yeah, it's stupid. The whole point is to write a virus from scratch. There's no class in just altering someone else's.

But some people get a kick just by hacking somebody else's virus.

CF: I grew up in a poor neighbourhood. When I see rich kids driving around in Jags it makes me mad. When I wave "Hi" and they ignore me, I feel mad.

There's a certain depersonalization of the corporate world by the hackers. It didn't bother me to steal a row of manuals from the phone company, but I wouldn't steal a boombox that belonged to an individual there.

The interesting thing is that the hacker community doesn't organize its attacks. You don't get 50 people attacking TRW all at once.

Copyright 1996, 2004 M. E. Kabay. All rights reserved.

CF: The golden age of hacking is gone. Hacker BBS are just a bunch of stupid kids talking about drugs and being cool.

There's more people with computers today.

CF: There used to be interest in uploading schematics; but now all you see is people talking about taking drugs and watching a movie.

[What about anarchist files?] No hacker would be interested in these files.

The problem is that enforcement is capricious.

Pure hacking: accessing the system for the challenge; there's no intention of harm. Applied hacking is for a specific goal like stealing information. Reverse engineering of OS to write drivers is classic hacking.

Saturday morning, 93.12.18

Discussion before the meeting: would token-cards stop hackers? Yes.

What about encrypting modems? Would discourage attack. And blank or meaningless login prompts? Discourage the amateurs and interest the more expert hackers.

Keith Perry (Security Consultant) doesn't hook his computer up to the phone lines often. Thinking about setting a BBS with security info "to thumb my nose at the powers that be." There used to be war dialer written in BASIC; I rewrote it to call a whole string of digital pagers and leave the number of someone I wanted to irritate. [Why did you do that?] Oh I don't know, I just got irritated. The victim called the Public Regulatory Commission and complained (he knew I was pissed at him). But it turned out that I hadn't broken any laws.

Mike told the story about how he asked his phone company for a list of his local phone calls and they said they didn't keep that information. Give me a break! The FBI can walk in and get anything they want.

[Keith, tell me about thumbing your nose]. I see government encroaching more and more every day, taking away rights. Since junior high school, speaking my mind about government would put my teachers into an uproar. They wouldn't face the problems. I think all this stuff should be made public. There are lots of secrets they hold and it's not for our own good. [Is there a right to corporate privacy?] Yes, there's a definite right to

Copyright 1996, 2004 M. E. Kabay. All rights reserved.

corporate privacy. I think the government tends to stick its nose into ordinary businesses. Taxation without representation.

[What's your ethical stance about trashing data?] If things got to a state of martial law, I would do everything I could to make the other side fall. There are hundreds of people more capable of that; I'm a better observer than actor. But I could visualize circumstances where there would be a need--if the phone company took over and gave the government everything, I'd take out some fiber optic cables.

[Note: someone offered a dozen free donuts to the 200 people present; in the melee that followed, several people who arrived first took two each.]

General observations: interesting mixture of grey-haired experts and callow beardless youths. Some of the younger folk, sporting the obligatory backward baseball caps, look positively chlorotic. One chap has mid-back green hair; the organizer, Drunkfux, is a tiny young man wearing red suede shoes, a red baseball cap, and a red tee-shirt labelled NARC. He has a thin gold ring through his left nostril. The registration line was single-threaded, resulting in a huge lineup; there must be about 200 people here.

The crowd has been waiting patiently for the organizers to get going; we're already over an hour late. The people behind me assure me that this is much better than last year, when the room was half the size.

Bruce Sterling, author of The Hacker Crackdown. Member of EFF.

I've been called to talk about why I like potatoes on a stick. I like potatoes on a stick, but I _hate_ fucking viruses. I've returned from the virus capital of the world--Russia. I've heard people excuse writing viruses because it's a challenge. They just don't understand intelligence. If you're so smart you're one in a million, go compete with the other 5000 brilliant people, not grandmothers with computers.

I can't take a disk off the street from some weirdo any more. I can take paper; but I can't take a diskette because it might be infected with a virus.

I met the top anti-virus guy in Russia; Mr Lijinski. He's a scientist, he's a nice guy. He's spending all his time running around writing anti-virus programs. He's the little Dutch boy sticking his thumb in the leak that is DOS. He has 64 pages of viruses that he has to battle. There's this kid who just takes viruses and changes the text. They say things like "Hi, I'm from Tallin and I wrote this virus." There are Tolkein viruses that say, "The Uruk-Hai are attacking your computer. The Winged Nazgul have seized your machine."

Copyright 1996, 2004 M. E. Kabay. All rights reserved.

Listen to this one: it's a Chinese virus that prints a long tirade and a poem about the Tienanmen massacre. Now look, imagine some Chinese system administrator reading the message the first time; Yeah, he says, maybe they're right. It's a political virus. So he takes it off and it comes back--because they always come back--from the backups. Then he takes it off again and it comes back again. And again. And again. By the sixth time the damned poem appears, the admin says "I'm glad they ran over those little fuckers."

I've heard people argue that they need viruses to attack corporations. But that's ridiculous. If you want to screw over a corporation, rip out their phone lines. Take out their electric power. Flush sponges down their toilets.

I asked Lijinski what message he'd like to give to Americans. He said, "You have every opportunity to do useful things with your skills. Don't write viruses."

I'm distributing free copies of _The Hacker Crackdown_ on diskette here. You know what to do. Someone with a laptop can have the miracle of the loaves and fishes. In January it's going on the Internet. Don't ask me why I am abandoning the profits from the most popular book I've ever written.

Ray Kaplan

I'm here because I like the technology. I'm not a criminal. I'm not here to bust anyone.

I believe it is time for us as a community to begin to collect, distribute and widely distribute vulnerability information. We need an intrusion report and vulnerability tracking database. It would live on the net and we could contribute in some verifiable way. We don't need some shithead contributing rumours. I don't know why anyone here would contribute.

I want to be able to send a query to the database stating which operating system I'm running and want the definitive list on what I have to watch out for.

I will serve as a locus for such a database. Anyone who can contribute can talk with me. I'm concerned about BugTrack on the net; I figure that someone is going to try to slap him down.

To hack or not to hack is NOT the question. But my private information is none of your fucking business. These days, I'm investing in crypt and large-calibre weapons.

Copyright 1996, 2004 M. E. Kabay. All rights reserved.

When God invented hacking, She invented hacking. So I'd like to talk about when to hack, how to hack.

Why to hack? There's many reasons. Because you have nothing else? Because you like it? To change the world? For the better I hope. Some are born to hack--Draper, where are you.

I think this is beautiful discipline.

How to hack? Safely, by the rules, with care, forethought, intelligence and passion. Dedication to what's needed, what's not needed, and to your values.

When to hack? Always? No. If you hack all the time, it removes your ability to smell the roses. When appropriate? Sure, seems reasonable. But who decided when it's appropriate? You and I do. It's a personal decision. But there's a societal dimension. Consider driving and drunk driving, rape and consensual sex. Appropriate means not being a bully. Your success in breaking a system may be because the victim is brain-damaged. No one has told the victim they're vulnerable. Or no one has told the victim that they're responsible for protecting their information. The world is full of simpletons. And victims may be under seige. I haven't met a security specialist who isn't working 80 hours a week.

It's so incredibly easy to destroy things that it's stupid to do so.

By what rules to hack? Do unto others? Within the law? Don't fucking complain to me unless you have been talking to your senators, congressman, policeman. By your own rules? How many of you have had formal training in ethics? Very few. By society's rules and ethical guidelines? Sheeeit.

Who is the hacker? Hero to society? Neither Kevin Mitnick nor I think that what he did was anything but fucked. In 1990, he tried to present himself to the legitimate security community; I tried to help him and as a result I filed for Chapter 7 bankruptcy in May of this year. Are you necessarily evil? Maybe--but at least don't be a pain in the ass. Malicious malcontents? You bet. Scumbag reprobates? [Audience: clapping; "Put that on a T-shirt and I'll buy it."]

I am not preaching, moralizing or beating anyone up. I just turned 47; take this as a commentary from an aging hack. Do illegal things and the feds will get you. Do illegal things and you will damage your career.

Copyright 1996, 2004 M. E. Kabay. All rights reserved.

Do immoral things and your desired peer group will shun you. That will also harm your job prospects. It breaks my heart to see a talented hack being refused a job where they could do good for society.

Do unethical things and the same thing will happen.

There are many people in the world who know a lot about security. The easy thing is making them mad. Systems are easy to hack. You may think that you're doing a brilliant high-tech hack--or you might just be masturbating.

Go to your community college ethics in computing class and contribute your point of view. Some of these classes are broken.

You are being perceived as evil. Are you? [Yeah, Yeah from audience]. If you do bad things, the cops will get on you.

Let's try to get to know each other instead of fucking around. I don't want the world to continue seeing you as a bunch of geeks instead of the talented people that you are.

Questions:

Q: You told us several times that you want us to open a dialogue with the legitimate security community without getting busted. How?

A: We could maybe organize a humungous meeting--maybe at Interop.

A: (MK) Be civil, follow standards of discourse.

Q: How to contribute our knowledge without being busted?

A: Intermediaries, anonymous remailers.

Q: This holier-than-thou attitude about making us come to them is what keeps us away.

A: The community's attitude sucks.

A: I want to answer the question about why the hacker community have to force the suits to listen and risk being busted?

First, the guys earning their living are scared shitless of you. Secondly, they can't find you--you hide very well.

Copyright 1996, 2004 M. E. Kabay. All rights reserved.

....

Boston hackers (LOFT)

2600 meetings so popular that 40 people showed up in pizza restaurant. Thrown out and now meeting in a mall.

Kingpin: cell phone reprogramming. Quick reference list on reprogramming 100 types of phones.

Jolly Box originally produced by Jolly Roger in Sweden. Similar to demon dialer. Handles all the standard colour-box tones. It's pretty cool. Has a password-protected phone book stored in EPROM. Runs with 8039 processor. Sell them assembled for $80. Will add LCD.

Legal Issues: Brian Oblivion

Wrote first code in 1968. Got into Princeton; then RCA Laws in 1970. Works on computer committee of Texas Bar. Found that the head of computing of the Bar Assoc doesn't know what the Internet it. Asked to address DECUS with a pro-hacker view. Spoke on computer law.

Laws protect hackers, too. Law is an expression of social consensus; and we're working out the new rules right now. Prosecutors are only now trying to struggle with applying old laws to cyberspace.

He helped Steve Jackson sue the Secret Service--taught them a $50,000 lesson plus legal fees. Now considering appeals.

The Internet will radically change computer law; now have many courses on different legal issues in cyberspace. Will radically alter copyright law, etc.

At 39, his generation is in power now. Resisted Clipper so strongly that the initiative is dead. Will not be mandatory.

Enforcement officials as stacking charges on suspects because they don't know how to handle computer crime. Don't talk to the police; demand to talk to your lawyer. If you can't afford one, contact the EFF. We even invited Gail Thackeray so we could laugh at her. She thinks everything ought to be illegal. Information wants to be in jail.

Copyright 1996, 2004 M. E. Kabay. All rights reserved.

I'd like to talk about netpigs: network police. Many admins are still back in the mainframe era, where they set the rules and if you don't follow the rules you're off. University authorities can sometimes bust people by calling the cops--they do things that the police can't do legally. So watch out for these people. In one case, a university threw a student off the system but gave him two hours to download his files. He also got a user-level users\etc file without passwords. But he got thrown out anyway--not enough money for court battle.

Don't fool around with academic computers; can really ruin your career. Join public Internet sites for $20/month.

Internet growing about 10%/month according to news magazines; but his experience is more like 20%/month. Approaching knee of the curve--you can tell because the big boys are getting into this. The National Information Infrastructure is getting a lot of news--but there will be costs because the NII will be under private ownership. Good news is that the govt will have to open up its files to the public. The bad news is that they intend to scrap the Internet because it's too hard to bill for services.

This room has more talent than Microsoft on a Monday morning. You're in the position of assembly-level hackers for the 8088 in 1980. At least 10 of you should be millionaires in a decade.

Another attack will be from the religious right. The CEO of CompuServe was asked why he doesn't give full access to the Internet. He asked, "Why should we allow our fine network to link to a sewer like the Internet?" But the Internet is the repository for the collective consciousness of the modern world.

Q: How will the globalization of the net affect issues of censorship?

A: As I used to tell people when they complained about porno on TV, there's a big off switch on the set. Parents have to take responsibility for their children. If you don't like it, don't fuckin' watch. The religious right makes the US a laughingstock.

I am concerned about nets like CompuServe, which won't grant a user-ID unless you have a credit card. The EFF has strong positions on universal access at reasonable cost.

You and people like you will have a huge impact on the future of the Internet and the world. There are things we'll be doing that have never been seen on this planet. We'll be able to talk to people around the world using IRC. But I want us controlling it, not AT&T.

Copyright 1996, 2004 M. E. Kabay. All rights reserved.

I make an analogy to the road system. If we had to pay for each mile we travel, the overhead would be awful. So we pay 5 cents with every gallon of gas we buy. The Internet is logically run by a government, not the private sector.

Every person in this room is important in this battle. We are going to make a whole new world out of this.

Q: What about the Alansky case in Hartford where the cops are attacking a BBS for having bomb-making info?

A: [Deth Vegetable] I wrote those files when I was 15; and the files are in the news again in Montreal. Some kids used my files and blew up their fingers. I feel bad about that. In Canada they don't have guaranteed free speech, so the cops are taking boards down for having this stuff on them. Alansky got 28 months in jail. His lawyer said he didn't want to get involved with the First Amendment. So Alansky plea-bargained and then went to jail. There were other irregularities; e.g., they didn't inform the lawyer of the location for the indictment.

Q: [MK] Why did you publish the files at all?

A: [Written by Voyageur] We provide the files in order to protest our rights to the freedom of information. If we voluntarily censor ourselves, we do as much as if the government were doing it itself. We maintain our rights through the exercise and use of our rights.

In addition, many adults enjoy pyrotechnics as a recreational activity. Quality information provided at low or no cost greatly reduces the risk of pyrotechnic experimentation resulting in unfortunate accidents.

Brian Oblivion continues:

I recently went to China and gave some lectures in Shanghai. I wanted to find the hackers, so I asked where I could copy some floppies. When I walked in they were a little nervous, so I plugged a serial cable into their AST 386/25 and downloaded some shareware--well, not exactly, but you know what I mean [laughter]. I left some Microsoft programs there and I hope that when MS gets into China, they'll find that people have been hacking their products for 5 years.

Copyright 1996, 2004 M. E. Kabay. All rights reserved.

[Image seen in passing: small woman wearing tight decollete backless leotard showing lots of cleavage, black crinoline skirt, and striped black net stockings. Capped by hair dyed purple-red in a pony-tail.]

Q: Why do you want government support (and interference) in the Internet? The greatest growth is in the .com sector, and that's the sector that is least constrained by government regulation. If you insist on publicly funded access to the Internet you'll undercut commercial organizations who are doing a good job right now of bringing inexpensive access to everyone.

A: I didn't mean to imply that all access should be funded by the govt, just that there should be subsidized access for those who don't know about the net yet.

[plenary session ends]

Discussion about posting bomb files with Deth Vegetable and others

[When I asked the audience "Why post such a file at all?" several people turned around instantly and said that it wasn't illegal, therefore it was OK. Their reactions were heated. Some repeated the mantra, "Information wants to be free."]

[Why did you post such files?] It was funny to me at the time [when he was 15, 4 years ago].

[What about now?] I wouldn't do it now. I can't say exactly why. I'm a different person now.

[What if you could humiliate your 73-year old Aunt Gladys by making fun of her. Would that be good? After all the information is there--and information must be free.]

I think there must be discussion of these issues. I haven't seen this in the discussions yet.

DV: The government has the power; so publishing the anarchy files is important. It's as if one day the revolution will come and these files will arm the masses to rise up against the establishment.

[Suppertime]

Netta, the editor of *Gray Areas Magazine,* announced that the organizers of the conference were spending a great deal of money on live strippers. There would also be

Copyright 1996, 2004 M. E. Kabay. All rights reserved.

pornographic films showing coprophagia. Last year, the organizers showed films of bestiality. These seem to appeal to the adolescents in the group. We guess that the median age might be around 17 or so.

[Overnight]

As I was warned by Winn Schwartau, some youngsters were out of control. Around 2 am, someone pulled a fire alarm; I heard the engines coming and worried about the occasional deaths during responses to false alarms. In the hall, behind the pillows I had to place at the bottom of the door to keep cigarette smoke out, I heard snickers. There were loud conversations in the hallway throughout the night. I gave up trying to sleep around 3 am and turned the TV on softly, resisting the urge to make it blare and wake up my neighbours. I imagined setting the TV at maximum volume just as I left the room, perhaps adding the din of the radio alarm buzzer as counterpoint. However, years of socialization are not so easily overcome, and I couldn't bring myself to be so crude.

Hacker Perspectives on Law and Order

Criminal hackers often express horror at having laws apply to them. They're not so shocked, however, at having laws protect their own interests.

An important publication catering to criminal hackers is *2600*, a magazine that appears on the news stands at many computer shops. It takes its name from the 2600 Hz tone which Cap'n Crunch used to fool phones into thinking he had paid for phone services. The magazine routinely includes detailed information on phreaking, coupled with hypocritical warnings to its readers not to use the techniques it so painstakingly includes. The magazine is viewed as practically mainstream, and the editor, Eric Corley (who demands to be called "Emmanuel Goldstein") has become a media darling, appearing on TV news shows and granting interviews to mainstream reporters as if he were a spokesman for the entire hacker underground. The magazine has prompted the formation of several monthly 2600 gatherings around the U.S., including the main one in New York City, where socially-maladjusted teenagers meet to exchange views and parade their trophies before each other--and the occasional law enforcement official.

The most recent farce concerning *2600* is that another magazine, *Blacklisted! 411,* has apparently been reprinting a good deal of material from old issues of *2600* without attribution. Corley posted messages on the Internet to complain about such blatant disregard for intellectual property rights:

Copyright 1996, 2004 M. E. Kabay. All rights reserved.

Recently a number of people have contacted 2600 concerning another hacker magazine called "Blacklisted! 411". Having more hacker publications has always been something we've tried to encourage. Zines like Cybertek, 40Hex, Hack Tic, and Private Line have been helped or inspired by 2600 over the years, not to mention numerous other zines that we have trade arrangements with. The current zine scene is healthy and prospering. So we were happy to see that there was another hacker rag in the works.

Then we got our first look at "Blacklisted! 411". To say it's similar in appearance to 2600 would be an incredible understatement. Anyone looking at the two publications will notice a very disturbing amount of unattributed duplication which, we regret to say, goes far over the line to the category of blatant ripoff.

> This is not about style similarity. True, their zine is the same size as ours. They use the exact same font style and size, their text boxes are the same, the staff box looks almost identical (except, of course, for the staff). Not too original, but so what. The real problem comes from the fact that this publication has taken numerous pieces of 2600 and published them as their own without any credit given and without ever asking permission. We've nearly always granted permission for zines to reprint selected articles of ours, as long as the author and 2600 are credited. Our primary goal, after all, is to get the word out. But this goes way beyond any conceivable 'sharing of information' between two publications.
>
> The two feature articles in the current issue of "Blacklisted! 411" were both printed years ago in 2600. One of the articles (on 5ESS switches) was also printed in Phrack a few years back. No mention of this fact is made, no credit to the authors is given. Both articles appear to have been written by the staff of "Blacklisted! 411". We've heard reports that most of the other articles were also lifted from other publications or the net, again without accreditation and leaving the impression that "Blacklisted! 411" is the originator.
>
> "Blacklisted! 411" has a section very similar to the 2600 Marketplace. They call theirs the Marketplace. Our wording for our marketplace advertising is: "Marketplace ads are free to subscribers! Send your ad to: <address>. Ads may be edited or not printed at our discretion." Their wording reads: "Marketplace Ads are FREE to subscribers! Send your ad to: <address>. Ads may be edited or not printed at our discretion." Not only that, but these people have actually gone so far as to reproduce our subscribers' ads without their permission, no doubt as part of a plan to obtain more advertising by appearing to have many customers. They did such a poor job covering this up that one of "their" ads has a line reading "All 2600 subscribers gain complete access". Throughout its pages, "Blacklisted 411" reproduces our house ads *word for word* as if they were their own.

Copyright 1996, 2004 M. E. Kabay. All rights reserved.

Perhaps the most disturbing examples of this magazine's ill intent lie in the replies to their letters. Not surprisingly, some of their readers think they're somehow affiliated with 2600 and address them as such. In one reply, the editor says, "I wonder why everyone keeps addressing us as 2600? Are we THAT much alike? haha."

So now we're faced with the unpleasant prospect of what to do about this. To do or say nothing would be a disservice to our magazine, our readers, and all that we've accomplished over the last 11 years. At the same time, we have no desire to emulate the corporate giants who try to intimidate us into not publishing what we publish, even though a number of people are advising us to take some sort of legal action.

The truth is, we haven't decided yet on a course of action. Suggestions would be welcomed. Our only goals are to get these people to stop printing material from our magazine without permission or credit, to stop copying our in-house and subscriber advertisements, and to stop representing themselves fraudulently to the hacker community.

Emmanuel Goldstein

Editor, 2600 Magazine

(516) 751-2600

emmanuel@2600.com

In a comment in the thread that developed in the NCSA Forum on CompuServe, I posted the following:

You have to admit that it takes some nerve--or stupidity--for a bunch of criminal hackers to write, "The real problem comes from the fact that this publication has taken numerous pieces of 2600 and published them as their own without any credit given and without ever asking permission."

This from people who habitually crow about publication of stolen proprietary information?? Who do everything they can to encourage deception and dishonesty? Who deny that property rights exist (at least, other people's property rights)?

It's ludicrous, it's wonderful: the fundamental hypocrisy of the criminal hacker community is demonstrated once again in terms no one can deny. The same attitude underlies the whining self-justification of people like Mark Abene, shown in a recent video by Annaliza Savage

Copyright 1996, 2004 M. E. Kabay. All rights reserved.

("Unauthorized Access") complaining pathetically that the legal system is engaged in a witch hunt--and he pleaded guilty to all charges before being sentenced to jail time.

> My father in law, a professor of social psychology, has encountered the same double standard in his classes. The popular cant holds that no one can impose values, that all values are the arbitrary expression of a powerful class of oppressors. Some students in his course use the familiar phrase to express their outrage at the mere mention of normative values: "But-but-but that's a VALUE judgement!!" He has developed a clever response that usually shocks the kids into a new understanding: he says, "I see.... so there are no values that we, as a society or as a community or even as a psychology class can agree to. OK. Using your approach, I will therefore abandon all assignments and grading for this course and will simply assign your final grades at random."
>
> You can imagine the cries of horror and "That's not FAIR!!" that erupt from the classroom.
>
> "Ah," says Pop, "so you _do_ think there are values we have to share...."
>
> Eric Corley has the _right_ to demand that other people respect his intellectual property rights; he just doesn't have the moral stature to expect anyone outside his circle of criminal sycophants to take his outrage seriously.
>
> In the immortal words (edited for NCSA Forum consumption) of the French castle guards in *The Holy Grail* by the revered Monty Python, "His mother was a hamster, and his father smelt of eldeberries!"
>
> I also invited Mr Corley (by e-mail) to respond:
>
> Dear Mr Corley:
>
> Your recent cry from the heart about violations of intellectual property rights has generated considerable amusement in the NCSA Forum on CompuServe.
>
> I wrote the following this morning and invite you to rebut my point of view.
>
> If you do not have a CompuServe ID, you are welcome to call Stephen Sands, the NCSA Membership Director, for information on obtaining one legally. You can reach him at 717-258-1816 at our headquarters in Carlisle, PA.
>
> If you do join us, please follow Forum guidelines and use your full name, not a pseudonym. You'll find the discussions going on in the News/Case Studies section of

Copyright 1996, 2004 M. E. Kabay. All rights reserved.

NCSA FORUM (GO NCSAFO). By all means look around and participate in all the discussions that seem interesting. I'm sure that you will have much to contribute to the Ethics section and the PBX/Telco Security section.

After you read the current message base, I'm sure that it will be clear that we do not allow detailed instructions on how to break security; contributions which help users and managers protect their systems against attack are always welcome.

If you wish to upload the table of contents of your publication, please do so in the PR section (13) as a posting; you may also upload files as you see fit provided that you have the copyright on them or have permission from the copyright holders.

You and I disagree on many aspects of the criminal hacker culture <smile>; however, it will be a pleasure to engage in civil debate with you over fundamental issues of morality in cyberspace. I can assure you of a polite, if not friendly, reception in our Forum.

As of the time of writing (a week later) Mr Corley had not responded.

5 Hacker Psychology

Maxfield (1985) classifies different groups of hackers as follows:

o Pioneers: people who were fascinated by the evolving technology of telecommunications and explored it without knowing what they were going to find. These people included few criminals;

o Scamps: hackers with a sense of fun. These people do no overt harm (but see later in `Who Cares?');

o Explorers: motivated by their delight in finding out what computer system they have broken into--the further away physically or the more secure, the better. The children in the movie `War Games' were excited because they broke into NORAD computers;

o Game players: enjoy defeating copy protection and seek systems with games to play. Hacking may seem like an intelligence test to them--a way to demonstrate their power. One hacker was trapped by enticing him with a game deliberately left on a bank computer--he played for hours while the police and the phone company traced his phone call;

Copyright 1996, 2004 M. E. Kabay. All rights reserved.

o Vandals: these malicious folk deliberately cause damage for no apparent gain to themselves. The 414 Gang from Milwaukee broke into the Sloan-Kettering Institute's computers and wiped out cancer patients' records and scientists' research data--some fun, eh?

o Addicts: these compulsive nerds may also be addicted to narcotics, and some hacker BBS post information on drugs as well as on modems, passwords and vulnerable systems.

5.1 Narcissists?

What strikes me about hackers their arrogance and their self-centered focus on their own wishes to the exclusion of anyone else's needs or rights. These people seem to feel that their own pleasures or resentments are of supreme importance and that normal rules of behaviour simply don't apply to them. Take the recent case in which the 17-year old caused $2.4 million damage because he didn't get a poster from *Gamepro* magazine for video game players (Alexander, 1990b). Is this the response of a balanced adolescent to failure to receive a free poster?

The standard reference work on psychiatric disorders (APA, 1980) defines the Narcissistic Personality Disorder in these terms:

`The essential feature is a Personality Disorder... in which there are a grandiose sense of self-importance or uniqueness; preoccupation with fantasies of unlimited success; exhibitionistic need for constant attention and admiration; characteristic responses to threats to self-esteem; and characteristic disturbances in interpersonal relationships, such as feelings of entitlement, interpersonal exploitativeness, relationships that alternate between the extremes of overidealization and devaluation, and lack of empathy....

...In response to criticism, defeat or disappointment, there is either a cool indifference or marked feelings of rage, inferiority, shame, humiliation, or emptiness.... Entitlement, the expectation of special favors without assuming reciprocal responsibilities, is usually present. For example, surprise and anger are felt because others will not do what is wanted; more is expected from people than is reasonable.

Notice that the 17-year old who trashed the voice-mail system had a confederate aged 14; we can imagine the sort of hero-worship the older boy basked in as he boasted about damaging the publisher's interests.

In another case, three Atlanta men in their early 20s were convicted of repeatedly breaking into BELLSOUTH computer systems, listening to private conversations, and stealing confidential data (Alexander, 1990c). They were members of `The Legion of Doom,' a group of about 15 expert hackers. The three were sentenced to 14, 14, and 21 months in jail respectively. They

Copyright 1996, 2004 M. E. Kabay. All rights reserved.

must pay restitution of $233,000 each. It is significant to me that, aside from belonging to the comic-book style Legion of Doom, these people identified themselves on the hacker networks using grandiose `handles' such as `The Leftist,' `The Prophet,' `The Urvile,' and `Necron 99.' `Urvile' means something like `ultimate evil' and `Necron' has connotations of death and computers mixed together (sounds like a new heavy-metal band). Does this sound mature?

5.2 Anti-social personality disorder?

During the 1990 December holiday season, some 25 hackers gathered for their `Christmas Con' in a hotel near Houston airport (Anonymous, 1990). `After consuming too many beers and pulling fire alarms, the group was kicked out of the hotel.' This sort of behaviour may be associated with Antisocial Personality Disorder.

`The essential feature is... a history of continuous and chronic antisocial behavior in which the rights of others are violated.... (APA, 1980).'

Dr Percy Black, Professor of Psychology at Pace University in New York, commented that there may be an underlying theme in all of these cases: the search for a feeling of power, possibly stemming from a deep-seated sense of powerlessness (Black, 1991). These acts therefore serve as over-compensation for inferiority feelings. He added that the apparent immaturity of the hacker may be an expression of unresolved feelings of resentment and powerlessness that all of us must overcome as we grow up. The hackers are trying to tell themselves, `I can too.' These ideas are associated with the work of the psychologist Alfred Adler.

5.3 Endorphin addicts?

Hackers may be seeking a high--a peak experience. There is some evidence that young people require a higher level of stimulation than most adults. Some people have an abnormally high need for stimulation even in adulthood. Dr Black explained that antisocial behaviour may be related to inadequate endogenous stimulation; i.e., these people's brains don't provide the normal arousal that keeps normal people feeling that life is interesting. Thus some children and adults may engage in unacceptable acts because they crave any kind of stimulation, regardless of whether it is noise, acclaim or even punishment.

I heard a fascinating lecture by Professor Mihalyi Csikszentmihalyi at the February 1987 Annual Meeting of the American Association for the Advancement of Science. Csikszentmihalyi described `autotelic' experiences as those in which the goal lay within the activity itself. Such actions are carried on for long periods without obvious extrinsic rewards. Some examples he cited include painters, composers, rock-climbers, surgeons and mathematicians. Many of us who have programmed know full well how absorbing the work can be; I remember looking at my

Copyright 1996, 2004 M. E. Kabay. All rights reserved.

watch at 17:30, turning back to a program I was writing, then looking at my watch again what seemed like a moment later. It was 23:30. Now, that was an autotelic experience.

Perhaps for hackers, hacking is an autotelic experience. After all, they have unambiguous goals and feedback (two of the characteristics Csikszentmihalyi identified) and seem to persist in their attacks. Stoll tracked his German hackers for a year. Hacking may be in part an exaggeration of the normal response to the give and take of computer usage.

6 Why Should We Care?

At the simplest level, hackers steal. They steal resources that could be used for more productive work. Some hackers cause obvious damage: they destroy or damage data. But Cliff Stoll identified the fundamental problem caused by hackers: they destroy the climate of trust which allows effective communications via computer networks.

Stoll was originally reluctant to cooperate with law-enforcement officials. Anyway, he got little encouragement from them at first. Nonetheless, he finally came to the conclusion that the hackers were hurting him and every other user of INTERNET, the loosely-run, non-commercial network linking thousands of scientific and educational institutions around the world:

'Networks aren't made of printed circuits, but of people. Right now, as I type, through my keyboard I can touch countless others.... My terminal is a door to countless, intricate pathways, leading to untold numbers of neighbors. Thousands of people trust each other enough to tie their systems together....

Like the innocent small town invaded in a monster movie, all those people work and play, unaware of how fragile and vulnerable their community is. It could... consume itself with mutual suspicion, tangle itself up in locks, security checkpoints, and surveillance; wither away by becoming so inaccessible and bureaucratic that nobody would want it anymore.'

7 What Should We Do?

Everyone concerned about the health of the computer-using community can contribute to making it harder for hackers to hack.

- First, protect your own system.
- Use passwords properly; change them monthly.

Copyright 1996, 2004 M. E. Kabay. All rights reserved.

o Don't give away passwords or modem telephone numbers without good reason.

o If you run a computer system, convince yourself and management of the value of a good security monitor and audit trail.

o Keep your system clock accurate so you can coordinate with other users if you have to track a hacker.

o Keep helpful hints out of your logon sequence.

o Identify holes (e.g., passwordless users with powerful capabilities) in your security system; use commercially-available audit programs and plug the holes.

o Put a warning message into your logon welcome text to threaten legal action against unauthorized users of your system.

Finally, report attacks against your system to your local police force or to the FBI. In commenting on the Atlanta case (Alexander, 1990), William Cook, Assistant US Attorney in Chicago, had a message to victims: `...it is worthwhile for you to cooperate when unjustly violated by people who hack into your system....' All of us share responsibility for combatting hackers. Let's work to prevent their nefarious deeds and respond decisively when our systems are attacked.

8 Prosecution

Hiding a problem makes it worse. A patient who conceals a cancer from doctors will die sooner rather than later. Organizations that conceal system security breaches make it harder for all system managers to fight such attacks. Victims should report these crimes to legal authorities and should support prosecution.

As discussed in Chapter 2, thanks to under-reporting, estimates of the extent of the problem are nebulous and unconvincing to upper management. No one knows exactly how much security breaches costs the world economy. Only those crimes which are discovered at all can be reported. Of those that are discovered, very few are reported to the police, let alone announced to the news media.

Security specialists guess that 75% to 85% of all attacks on data confidentiality and integrity are by employees authorized to use the systems and systems they abuse. Despite this consensus, news stories, popular books and movies about security breaches usually focus on outsiders. `War Games' showed teenaged computer nerds cracking military systems. *The Cuckoo's Egg* dealt

Copyright 1996, 2004 M. E. Kabay. All rights reserved.

with a real attack by West German hackers on scientific networks. The recent film `Sneakers' deals with a `Tiger Team' hired to test a bank's system security against outside penetration.

So official statistics are inaccurate and the popular view is wrong. This distorted picture of system security interferes with rational allocation of resources. Because of the poor quality of published evidence, system managers have a hard time convincing their superiors to invest in adequate security measures. CIOs are more likely to favour requests for anti-hacker measures than for protection against insider crime--despite the best estimates of specialists. Even if hardware and software access controls and system logging are installed, the lack of public statistics makes it difficult to invest in security training and enforcement within most organizations.

9 The CERT

Counter-measures should already be in place and defensive plans formulated in advance. When the system is actually under attack, there is no time for long debates and discussion. Because of the difficulty of catching and prosecuting computer criminals, to improvise is to fail.

Every organization should build a Computer Emergency Response Team (CERT) which includes system specialists. The team itself and its efforts during a crisis should be kept as secret as possible. Members will have to keep meticulous records and log all system and file accesses on disk and paper. The CERT will also have to synchronize system time-stamps with official government time signals so they can coordinate more effectively with telephone companies to trace attacks from outside. System programmers will have to provide alerts for specific events such as unauthorized reads and writes in specific databases.

The CERT should include lawyers who can help identify what types of evidence need to be collected to prosecute system breaches as crimes and how that evidence should be documented. The CERT should cooperate closely with law-enforcement authorities. In the U.S. and Canada, any attack from the outside is likely to involve breaches of federal criminal law; the FBI and the RCMP are therefore the agencies to contact.

Ensure that your computer systems' welcome message includes explicit warnings against abuse; e.g., `This system is for the exclusive use of authorized users. All unauthorized access may be prosecuted to the full extent of the law.'

Prosecution establishes a legal precedent for following up later abuses by other employees or intruders. If there is no history of prosecuting security infractions, dishonest employees who are fired for their behaviour can claim that their dismissal is harassment instead of punishment.

Copyright 1996, 2004 M. E. Kabay. All rights reserved.

In some cases, prosecution may lead to recovery of (some of) the lost resources. Prosecution may also be part of the a legal obligation to protect shareholders in a public company. In a wider sense, prosecution is an expression of our outrage; it is a contribution to public morality.

There are admittedly risks in prosecuting system security breaches publicly in the courts. Criminal hackers may become malicious if they detect traps and audit trails. Catching system abusers is expensive, requiring overtime, consultants, and special equipment. And litigation is never cheap.

Worse yet, the attempt to catch the nasties may simply fail. Upper management may object to what will then look like a wild-goose chase. Failure may affect the security team's credibility in other areas and battles. As organization-wise employees know, it's important to choose one's battles--and to win the ones we choose.

The greatest concern when deciding whether to prosecute malefactors is corporate reputation. Regrettably, many victims fear that they will lose credibility. Managers can argue that prosecution is tantamount to admitting incompetence in corporate security. If security had been adequate, the crime wouldn't have occurred. However, one can argue just as well that prosecution is a demonstration of *competence* in corporate security. If security had been inadequate, the abuse would not have been detected.

In order to prevent foot-in-mouth disease, the CERT should include staff from your public relations department. These specialists should be the only ones to have any contact with the press if and when the security breach is disclosed. Contradictory statements from people with incomplete information will serve to damage the credibility of your organization.

What if the security breach does become public knowledge? The best strategy for maintaining corporate credibility is for your spokespersons to deal honestly and effectively with the press and the public. For example, pharmaceutical companies whose medications were poisoned have maintained their market share by acting openly and decisively to withdraw even potentially tainted products. Furthermore, they gained public respect by instituting effective measures for preventing similar incidents. Security managers can learn from their experience.

10 The CERT-CC

Regardless of whether you decide to go public about a computer attack, you should contact the CERT Coordination Center (CERT-CC) at Carnegie-Mellon University. This team of experts was organized in December 1988 as a result of the Internet Worm incident and another attack on the Internet in November 1988. Today, the CERT-CC is online 24 hours a day to receive

Copyright 1996, 2004 M. E. Kabay. All rights reserved.

information about any king of attack on an information system. You can phone their hot-line or send electronic mail at any time. Your confidentiality will be preserved.

It is time to stop hiding crimes against systems. Warn intruders that they will be prosecuted if they breach system security. Build and train a Computer Emergency Response Team that can deal with attacks on your systems. Cooperate with law enforcement officials. Help build a solid base of public knowledge for fighting abuse.

And give the criminals something to regret.

11 A personal note

I never realized how easy it would be to become a hacker. The experience was sobering. I realized once again that criminal hacking is a social problem, not merely a technical issue.

We had checked out of the Vancouver hotel room before noon as planned and I went to the deserted lounge on the 29th floor to work. I wanted to check my email, but the wall phone's handset had no dial or buttons. The line was clearly intended for inbound calls only. This impediment irritated me.

"I bet I can use the computer dialer for my call," I thought defiantly. After all, I reasoned, it's not as if the hotel had to pay anything for my outbound local call. It's not hurting anyone. It's no different from my habit of plugging a modem into the hotel room's phone jack or dismantling a non-modular wall unit to patch in an RJ-11 connector for my modem. No harm done--I always put everything back together again without damage. The hotel staff never even notice anything amiss.

I finished my downloads and uploads and unplugged my equipment. I snapped my fingers in triumph. "Hah!" I said smugly. I felt satisfaction at having accomplished my goals despite the hotel's silly restrictions.

We went to lunch.

Now, I am at my most irritable when hungry. However, as I ate my way back to rationality, I began to think about what I had done with that phone. I had used somebody else's phone for my own purposes--without permission and in defiance of their security measures. I had excused myself by rationalizations: the network access node was just sitting there doing nothing; it (probably) wouldn't cost the owner anything for me to use it; and they'd never know anyway.

Just like a criminal hacker, I had ignored the fundamental social and legal principle that an owner has the right to control their property. Instead, I had behaved as if my desire was more

Copyright 1996, 2004 M. E. Kabay. All rights reserved.

important than anything else. Despite my hunger-induced rationalizations, I had *no right* to decide how the hotel used its phone system, any more than some teenaged spoiled brat has the right to use my computer system without my permission.

I went to the hotel guest services desk and spoke with a pleasant young woman for about a minute. After I explained what I wanted to do, she graciously allowed me to use the phone jack for local calls.

What if she hadn't agreed?

I would have spoken with the hotel manager. I would have verified that the call wouldn't cost them anything and pointed out that I had just been a guest for five days at a cost considerably beyond that of a local call. Would she grant me permission as a gesture of good will? If so, I would carry away with me a memory of service beyond the letter of a mere contract. I would get a phone call, they would get a loyal guest.

If that approach didn't work, maybe I'd write a letter to the CEO of the hotel chain suggesting a change in their policies. But in any case, whether I agreed with them or not, it was their phone, not mine.

What about criminal hackers?

The youngsters and emotionally-arrested adults who break into other people's computer systems and networks argue just as I did in my hunger-induced irritability and goal-directedness. They want to explore cyberspace; other people own the equipment and the channels. They feel that their desire for education, utility and excitement outweighs the costs to owners and users of the systems they invade.

Rubbish.

There is no mutually-satisfactory transaction between criminal hackers and network owners. Their needs are not our obligations, just as my desire placed no obligation on the hotel to satisfy it. The universe does not owe criminal hackers a free network node.

Criminal hackers often claim that their depredations serve a useful social purpose by bringing security weaknesses to light. If they are sincere, they should negotiate with the owners of networks for mutually satisfactory testing arrangements.

All of us should be reaching out to educate young people about the rules of network usage--in schools, in colleges and universities--even in youth clubs and scout troops. We have to extend the rules of morality and civility--of respect and communication--into cyberspace.

Copyright 1996, 2004 M. E. Kabay. All rights reserved.

We support driver-education classes; how about network-education classes?

12 The Computer Ethics and Responsibility Campaign

In 1994, the NCSA joined with the Computer Ethics Institute to begin building a twenty-year program on computer ethics and responsibility. We feel that instead of simply responding to criminality in cyberspace, we ought to be doing something about reducing the number of criminals. That, to us, means awareness and education. Our models are the long-running anti-littering and anti-drunk-driving campaigns which have significantly altered public perception and public behaviour in the last two generations in the United States and Canada.

With a determined effort to reach and involve all sectors of society, the Computer Ethics and Responsibility Campaign will reduce, if not eliminate, the incidence of computer crime. For more information about the Campaign and how to support it, please call NCSA headquarters at 717-248-1816.

Copyright 1996, 2004 M. E. Kabay. All rights reserved.

13 Chapter Notes

1 Background on criminal hackers and their depredations (and warnings about internal attack):

Bloombecker, J. (1986). A security manager's guide to hacking. ***Datapro Reports on Information Security,*** report #IS35-450-101.

Burger, D. (1995). Catching hackers becoming more difficult: RCMP. *Computing Canada* 21(8):7

Flanagan, G.& B. McMenamin (1992). "The playground bullies are learning how to type." *Forbes* 150(14):184

Freedman, D.H.(1993). The goods on hacker hoods. *Forbes* 152(6):S32

Hafner, K. & J. Markoff (1991). ***Cyberpunk: Outlaws and Hackers on the Computer Frontier.*** Touchstone Books, Simon & Schuster (New York). ISBN 0-671-77879-X. 368 pp. Index

Maxfield, J. (1985). Computer bulletin boards and the hacker problem. ***EDPACS, The EDP Audit, Control and Security Newsletter,*** Oct 1985. Automation Training Center (Arlington, VA)

Menke, S. M. (1995). Electronic highwaymen on the attack. *Government Computer News* 14(7):20

Rothke, B. (1993). Internal computer larceny is not as far fetched as some might think. *InfoWorld* 15(50):46

Slatalla, M. & J. Quittner (1995). *Masters of Deception: The Gang that Ruled Cyberspace.* HarperCollins (New York). ISBN 0-06-017030-1. 225 pp.

2 Clifford Stoll has shared his experiences in cracking the West German spy ring that attacked the Internet in the mid 1980s:

Stoll, C. (1987). What do you feed a Trojan horse? ***Proceedings* of the 10th Annual National Computer Security Conference**. Association for Computer Machinery (??)

Stoll, C. (1988). To catch a hacker: traceback techniques. ***Datapro Reports on Information Security*** report #IS35-290-101, based on Stoll (1987)

Copyright 1996, 2004 M. E. Kabay. All rights reserved.

Stoll, C. (1989). ***The Cuckoo's Egg: Tracking a Spy through the Maze of Computer Espionage.*** Pocket Books (New York). ISBN 0-671-72688-9

Anonymous (1990). Stoll to star in NOVA adaptation. ***Computerworld*** 24(38):18

3 Some stories about criminal hackers in the 1990s:

Alexander, M. (1990). Devising matrix-based computer security. ***Computerworld*** 24(46):22

Alexander, M. (1990). 'Finger hackers' charged with voice-mail crime. ***Computerworld*** 24(46):46

Alexander, M. (1990). Hackers draw stiff sentences. ***Computerworld*** 24(48):1

Anonymous (1990). What was in their stockings? INSIDE LINES section, ***Computerworld*** 25(1):98

Eckerson, W. (1990). IS security exec tells of risks, strategies. ***Network World*** 7(36):21

Evans, D. (1994). CIA traps Tottenham hacker. *Computer Weekly* (July 28):6

Evans, D. (1993). The case of the 'artful dodger?' *Computer Weekly* (March 25):12

Fisher, S. (1990). Bringing Bill of Rights into Computer Age. ***BYTE*** 15(9):28

Gold, S. (1993). UK hacker did it for kicks, court hears. *Newsbytes* NEW02240008

Kelly, S. (1995). Highway to Hell? *Computer Weekly* (March 2):30

McCarthy, S. P. (1994). Overseas hackers force DOD to revise system security. *Government Computer News* 13(15):8

McMullen, B. E. & J. F. McMullen (1990). Harassment threatened IDG phone system. *Newsbytes* pNEW11070016

4 About Kevin Mitnick

Anonymous (1989). Hacker under guard. ***PC Week*** 6(1):63

Fisher, S. (1992). Hackers say fun is in the cracking. ***CommunicationsWeek*** (431):1

Copyright 1996, 2004 M. E. Kabay. All rights reserved.

Kellner, M. A. (1989). Hacker is jailed for theft: allegedly steals DEC VMS code. ***MIS Week*** 10(1):1

Kellner, M. A. (1989). Judge denies bail to 'dangerous' hacker. ***MIS Week*** 10(2):5

Powell, D. (1993). Confession proves good for the soul as network hackers tell all. ***Networking Management*** 11(2):12

Savage, J.A. (1989). Hacker prosecution; suspect held, denied phone access by district court. ***Computerworld*** 23(1):2

Sterling, B. (1992). ***The Hacker Crackdown: Law and Disorder on the Electronic Frontier.*** Bantam Books (New York). ISBN 0-553-08058-X. xiv + 328 pp. Index

Walker, C. (1995). One hack too many puts addict in the FBI's hands. *Computer Weekly* (March 2):100

5 Insights into the hacker subculture and psyche

Barlow, J. P. (1990). Crime and puzzlement: in advance of the law on the Electronic Frontier. ***Whole Earth Review*** (68):14

Piglia, P. & A. J. S. Rayl (1992). Secrets of the cyberculture. ***Omni*** 15(2):58

6 Are hackers crazy?

APA (1980). **DSM-III:** ***Diagnostic and Statistical Manual of Mental Disorders, Third Edition***. American Psychiatric Association (Washington, DC). P. 315 ff.

Black, P. (1991). Personal communication.

Copyright 1996, 2004 M. E. Kabay. All rights reserved.

Csikszentmihalyi, M. (1990). *Flow: The Psychology of Optimal Experience.* Harper & Row (New York). ISBN 0-06-016253-8. xii + 303. Index.

7 CERT-CC / Computer Emergency Response Team Coordination Center / Software Engineering Institute / Carnegie Mellon University / Pittsburgh, PA 15213 / Hotline: 412-268-7090 / Internet: cert@cert.org and FTP site file://info.cert.org/pub/.

8 Reporting computer crimes

Kabay, M. E. (1992). Send hackers a strong message by reporting security breaches. ***Network World*** 9(39):95

<<end>>

14

The NCSA Guide to Enterprise Security
By M. E. Kabay (1996)

Chapter 10: Encryption

Objectives:

After studying this chapter, readers should be able to

1. Explain why encryption is so useful in modern information security.
2. Explain the risks of using proprietary (secret) encryption algorithms.
3. Discuss the history and nature of the Data Encryption Standard.
4. Explain how the Public Key Cryptosystem works.
5. Describe the current status and application of Pretty Good Privacy for ensuring confidentiality, integrity, authenticity and non-repudiation.
6. Review the history of the Digital Signature Standard and Public Key Partners.
7. Discuss Privacy Enhanced Mail, the Public Key Cryptography Standards and NorTel's ENTRUST as tools for encryption of e-mail.
8. Explain the U.S. government's Capstone project, including the Skipjack algorithm and the proposed Key Escrow system ("Clipper Chip") and the controversy surrounding this proposal.
9. Describe and evaluate the International Traffic in Arms Regulations and their effect on cryptography.
10. Discuss electronic commerce, including electronic data interchange, electronic payment systems and digital cash.

Why Encrypt?

Regardless of the access control systems in place, every computer system and network that stores and transmits readable information ("in the clear" or "cleartext") has the same vulnerability: too many people can read other people's data. Examples of this problem of ensuring *confidentiality*:

- Top executives worry about having highly-sensitive strategic information stored on a system when they don't have absolute faith in their system managers.

- System administrators worry about having unwanted access to highly-sensitive strategic information when they do not need to be suspects if there is a breach of security.

- On many networks, it is possible to eavesdrop on communications. Using *sniffer* programs, for example, it is possible to intercept cleartext data in packets transmitted through local area networks by putting nodes into *promiscuous mode.* Electronic mail sent through the Internet is subject to interception and inspection in every node that provides store-and-forward functions.

- Some older operating systems store passwords in the clear, meaning that users with *root, GOD, system manager* or *superuser* capability can learn the passwords for any other

Copyright © 1995, 2005 M. E. Kabay. All rights reserved.

user's logon and then impersonate them. This capability meant that harmful activities carried out with any given user ID could be *repudiated* on the grounds that system management could have misused the ID in question.

Another use for encryption is to guarantee the *integrity* of information. If Albert sends Betty a message, how does Betty know that the message she receives is exactly what Albert sent? One approach to this is to create a checksum based on the content of the message. If anyone changes the content of the message, the checksum based on the new content will differ from the original checksum. However, this approach has a weakness if the algorithm for creating the checksum is known to Charles, the cryptographer's *man in the middle* who can intercept Albert's message. Charles can capture the original message, change it and create a new checksum, and then send both along to the innocent Betty. On the other hand, if the checksum, now usually known as a *message digest*, is created using a secret key that Charles does not know but that both Albert and Betty do know, Charles is out of luck in falsifying the message. It is even possible to generate a useful message digest using a secret key that only the sender knows, making life even harder for Charles, the man in the middle.

Looking again at communications, it is possible that the *authenticity* of a message is as important as its integrity. If two trading partners are sending each other instructions for the transfer of goods or funds, a fraudulent order can be a disaster. Imagine that Deltoid Industries has an electronic trade agreement with Echolalia Inc. and that criminal hacker Fudgebrain discovers their communications channel. Fudgebrain, a psychologically deficient jerk, carries out the electronic equivalent of the 100-pizza joke beloved of college fraternity geeks: he orders 100,000 left-handed hyberbolic infractors from Echolalia's main factory to be delivered to Deltoid's Plant 12. Two days and 2000 km later, the convoy of three tractor-trailers pulls into the loading bay of Factory 12 only to find every bay full, no room for the infractors, and some very puzzled Deltoid employees. Having a *digital signature* for verifying the authenticity of such a message would evidently be valuable. By the same token, providing cryptographically-sound digital signatures for authentication can also lead to *non-repudiation* of transactions: either the originator has to admit that they sent the message but made a mistake or they have to admit that the secrecy of their digital signature has been compromised.

Copyright © 1995, 2005 M. E. Kabay. All rights reserved.

Substitution Ciphers

For reference, here are the key concepts and terms used in discussing encryption.

Encryption converts data *(cleartext)* into gibberish *(ciphertext)*--reversibly, using an *encryption key* and an *encryption algorithm.* Turning data into unreadable gibberish permanently is no trick at all. *Cleartext* is sometimes known as *plaintext.*

Decryption converts ciphertext back into the original cleartext using a *decryption key* and a *decryption algorithm.*

Keys are alphanumeric or numeric sequences used to start the encryption or decryption process.

Symmetric encryption uses the same key for both encryption and decryption.

Asymmetric encryption uses a different key for decryption than for encryption.

Monoalphabetic Substitution Ciphers

Many ciphers depend on displacing the cleartext by a fixed or variable offset. For example, the ancient Caesar cipher simply converted each letter in a text by shifting it to the one three letters further in the alphabet. For example, A became D, B became E, C became F; at the far end of the alphabet, X became A, Y became B and Z became C. Using this monoalphabetic substitution cipher and the "key" offset = 3, one has a substitution table that looks like this:

Plaintext: A B C D E F G H I J K L M N O P Q R S T U V W X Y Z
Ciphertext: D E F G H I J K L M N O P Q R S T U V W X Y Z A B C

So with a cleartext (spaces removed) as follows:

MARYHADALITTLELAMBITSFLEECEWASWHITEASSNOW

the corresponding ciphertext is

PDUBKDGDOLWWOHODPELWVIOHHFHZDVZKLWHDVVQRZ

Copyright © 1995, 2005 M. E. Kabay. All rights reserved.

Using known frequencies of letters in the language of the cleartext, it is possible to deduce the offset. For example, in English, the most common letters are *e*, *t* and *a*. In our tiny example, the letter frequencies are

6 D, 5 H, 4 V, 4 W, 4 O, 3 Z, 3 L...

and in fact, D = A, H = E, and W = T. This example is not realistic, but it makes the point that monoalphabetic substitutions are vulnerable to cryptanalysis.

A monoalphabetic substitution cipher limited to the letters of the English alphabet has only 25 possible variations; this is known as having a *keyspace* of only 25. Such a small keyspace means that it would take at most 25 attempts to decrypt any ciphertext created with any of the possible keys. This hardly even qualifies as *brute-force attack* (breaking a cipher by trying all possible keys until one finds the cleartext).

Polyalphabetic Substitution Ciphers

There are refinements of this approach to encryption; for example, *polyalphabetical ciphers* use a different offset for each position in the plaintext. The key can be repeated until the key sequence is as long as the message; for example, a Vigenère cipher consists of 26 Caesar ciphers, each one with a different offset. The key determines which of the offsets to use for each letter in the cleartext. Unfortunately, such ciphers are also vulnerable to cryptanalysis.

The ultimate extension of polyalphabetic substitution ciphers is the *one-time pad.* In this technique, the sender and recipient securely exchange a key consisting of a random sequence of offsets as long as the plaintext. Such a random sequence can be printed as a set of sheets in a pad of paper; as each sheet is used for encryption and decryption, it is destroyed: thus the name *one-time pad.* As long as there are no non-random sequences in the key pad and no part is ever re-used, the cipher is unbreakable because there is no statistical information about the plaintext in the randomized ciphertext. The difficulties with this system are that the one-time pad itself has to be exchanged and stored securely and that each pair of correspondents presumably needs a different pad to preserve confidentiality and authenticity.

In general, any symmetric encryption algorithm using such *private keys* causes problems of *key distribution.* For *n* people who must communicate securely in pairs, there are

$$n * (n-1) / 2 = (n^2 - n)$$

secret keys required. For example, for 5 people there would be 10 different keys required; but for a corporation with 1000 communicators there would be about half a million pairs. Exchanging, securing and correctly locating this many keys would be more trouble than simply delivering the original messages in person. The asymmetrical Public Key Cryptosystem described below a few pages on in this chapter helps reduce the difficulties of key management.

Linear Congruential Pseudo-Random Number Generators

Many amateur cryptographers make the mistake of supposing that if a one-time pad is secure, then any cipher based on a long string of offsets must qualify as a one-time pad. A typical approach to such encryption is to create a sequence of numbers that look random (*pseudo-random* numbers). For example, a algorithm that works quite well is

Copyright © 1995, 2005 M. E. Kabay. All rights reserved.

$u_i = \text{fract}(\pi + u_{i-1})^8$

where u_i = current pseudo-random number in sequence

u_{i-1} = previous pseudo-random number in sequence

fract(x) = fractional portion of a number (i.e., fract(x) = x - int(x) where int(x) is the integer function). As an example, fract(1.5) = 0.5 .

I studied this algorithm out to ten thousand calculations using a programmable calculator with 15 significant digits and found that there was no statistical deviation from randomness in the frequencies of digits, pairs of digits, and triplets of digits. There was no autocorrelation (relationship between numbers) of orders 0 (numbers adjacent to each other) through 5. Nevertheless, encrypting text with such a sequence is not secure. For one thing, the numerical precision of the computer on which one performs the calculations profoundly affects the pseudo-random numbers sequence; as a result, encryption performed on one platform may not be decipherable on a different platform. In addition, these algorithms, as a class, are likely to generate specific values from more than one origin; e.g., two or more different values may lead to the same number. As soon as this happens, the algorithm produces a loop of numbers. This looping severely limits the effective keyspace of the algorithm because it allows statistical analysis of frequencies of letters in the ciphertext using known frequencies of letters and pairs of letters (*digraphs*) in the language of origin.

On the other hand, for non-language data, such an encryption system becomes much harder to decrypt. One of the in practical difficulties for the cryptanalyst attempting to decrypt a ciphertext based solely on numerical data is that it can be impossible to figure out when they have actually located the correct cleartext.

Security by Obscurity: The Potential Weakness of Proprietary Algorithms

Some companies provide encryption but keep their algorithms secret. The consensus among cryptographers seems to be that this is a bad idea. Many algorithms thought at first to be *strong* (resisting cryptanalysis) have turned out to be *weak* (easy to decipher) when they were subjected to scrutiny by experts. For example, in 1978, Xerox PARC scientist Ralph Merkle invented an encryption algorithm called the Knapsack. He offered a reward of $100 to the first person to show how to break the algorithm; within four years, "di Shamir, a renowned cryptographer (and co-inventor of the RSA Public Key Cryptosystem) broke it. Even a more difficult form of the Knapsack Algorithm (this one with a $1000 prize for the first to crack it) took only two years to be broken.

On a more trivial level, encryption schemes used in word processing programs and other popular software are often cracked quickly despite their secrecy. A variety of password-cracking programs are available to foil their elementary (albeit secret) encryption algorithms. Depending on such encryption may be perfectly acceptable for low-sensitivity materials in low-threat environments (e.g., on home computers where there are young children); however, they cannot substitute for well-tested algorithms that have withstood the attacks of experts.

The point is that the effectiveness of an encryption algorithm should not depend on its secrecy. When evaluating encryption functions, users should look for evidence that documented, well-known and suitably strong algorithms are used.

Copyright © 1995, 2005 M. E. Kabay. All rights reserved.

Cryptanalytic Attacks

Saying that one should use "suitably strong algorithms" begs the question of how to measure the strength of algorithms. For some algorithms, like the one-time pad, mathematical cryptologists have been able to demonstrate that there is no way to decipher the ciphertext without the knowing the key used for encryption. For others, there have been varying degrees of success in demonstrating algorithmic strength.

Cryptologists have classified attacks on ciphertext as follows (quoted from the sci.crypt FAQ--Frequently-Asked Questions--with minor changes to spelling, punctuation and formatting):

> 3.8. What are the basic types of cryptanalytic attacks?
>
> A standard cryptanalytic attack is to know some plaintext matching a given piece of ciphertext and try to determine the key which maps one to the other. This plaintext can be known because it is standard (a standard greeting, a known header or trailer, ...) or because it is guessed. If text is guessed to be in a message, its position is probably not known, but a message is usually short enough that the cryptanalyst can assume the known plaintext is in each possible position and do attacks for each case in parallel. In this case, the known plaintext can be something so common that it is almost guaranteed to be in a message.
>
> A strong encryption algorithm will be unbreakable not only under known plaintext (assuming the enemy knows all the plaintext for a given ciphertext) but also under "adaptive chosen plaintext" -- an attack making life much easier for the cryptanalyst. In this attack, the enemy gets to choose what plaintext to use and gets to do this over and over, choosing the plaintext for round N+1 only after analyzing the result of round N.
>
> ....

To summarize, the basic types of cryptanalytic attacks in order of difficulty for the attacker, hardest first, are:

ciphertext only: the attacker has only the encoded message from which to determine the plaintext, with no knowledge whatsoever of the latter.

A ciphertext-only attack is usually presumed to be possible, and a code's resistance to it is considered the basis of its cryptographic security.

known plaintext: the attacker has the plaintext and corresponding ciphertext of an arbitrary message not of his choosing. The particular message of the sender's is said to be >compromised.=

In some systems, [knowing even only] one known ciphertext-plaintext pair will compromise the overall system, both prior and subsequent transmissions; ... resistance to this is characteristic of a secure code.

Under the following attacks, the attacker has the far less likely or plausible ability to >trick= the sender into encrypting or decrypting arbitrary plaintexts or ciphertexts. Codes that resist these attacks are considered to have the utmost security.

Copyright © 1995, 2005 M. E. Kabay. All rights reserved.

chosen plaintext:	the attacker has the capability to find the ciphertext corresponding to an arbitrary plaintext message of his choosing.
chosen ciphertext:	the attacker can choose arbitrary ciphertext and find the corresponding decrypted plaintext. This attack can show in public key systems, where it may reveal the private key.
adaptive chosen plaintext:	the attacker can determine the ciphertext of chosen plaintexts in an interactive or iterative process based on previous results. This is the general name for a method of attacking product ciphers called "differential cryptanalysis."

Stronger Encryption

In our brief introduction to encryption, the only algorithms discussed so far have been substitution ciphers: one symbol at a time, the cleartext is transformed into a ciphertext. With the exception of the one-time pad, more powerful algorithms use a variety of techniques to jumble data and make the cryptanalyst's job harder.

Transposition Ciphers

Transposition ciphers permute (change the order of) the letters in the cleartext according to some secret rule. In the "rail fence" technique, one defines a matrix (say, 4 columns by 5 rows) and arrays the cleartext in one direction (in our example, let's write the text out along the rows). The ciphertext is then constructed by reading along the other direction (in our example, down the columns. Here's an example using cleartext "Mary had a little lamb" with the spaces removed:

Copyright © 1995, 2005 M. E. Kabay. All rights reserved.

M	a	r	y
h	a	d	a
l	i	t	t
l	e	l	a
m	b		

Then the ciphertext would be "Mhllmaaiebrdtlyata." As Stallings points out in his excellent introduction to cryptography (Stallings, 1995, chapter 2), this ciphertext has the same letter frequencies as the cleartext, making it possible to lay the text out on different matrices until a readable form is attained. However, as Stallings explains, additional stages of such transpositions can make the ciphertext even harder to analyze.

Block Ciphers and Chaining

Another level of sophistication in cryptographic algorithms derives from treating more than one letter at a time. The text is grouped into *blocks* which are encrypted using a cryptographic key and the encryption algorithm. Such *block ciphers* can be strengthened by *block cipher chaining,* where an additional factor in generating the ciphertext comes from preceding ciphertext blocks. Chaining ensures that the ciphertext corresponding to a specific block of cleartext will not be the same as the ciphertext for the same cleartext from a different part of the message.

For example, suppose an imaginary block cipher encryption algorithm were applied to the numeric sequence

12345 67890 23456 67890

with a block size of five. If a block cipher *without* chaining were applied, we could imagine a ciphertext of, say,

98102 78924 88240 78924.

Identical blocks of cleartext produce identical blocks of ciphertext. If the cleartext is long enough and includes enough structured material (e.g., record headings), it is possible for a cryptanalyst to begin compiling tables of likely cleartext/ciphertext pairs and thus break the cipher.

However, when the ciphertext depends on previous ciphertext blocks, the ciphertext corresponding to the original cleartext above might end up looking like

98102 13234 85742 34357.

Product Ciphers

Another class of block ciphers combines a number of transpositions and substitutions to create a more powerful overall encryption algorithm. Unfortunately, mathematical cryptologists have not yet found a general approach to proving that product ciphers are unbreakable; in the words of the cryptology FAQ,

Copyright © 1995, 2005 M. E. Kabay. All rights reserved.

> Nobody knows how to prove mathematically that a product cipher is completely secure. So in practice one begins by demonstrating that the cipher "looks highly random." For example, the cipher must be nonlinear, and it must produce ciphertext which functionally depends on every bit of the plaintext and the key.... In this sense a product cipher should act as a "mixing" function which combines the plaintext, key, and ciphertext in a complex nonlinear fashion. The best-known and most widely-used product cipher is the Data Encryption Standard (DES).

Data Encryption Standard

In 1971, IBM completed a project to develop strong encryption algorithm called "Lucifer" that was applied to banking machines of Lloyd's of London. Over the next few years, IBM scientists developed Lucifer into a practical commercial encryption algorithm that was eventually selected by the National Bureau of Standards (later named the National Institute of Standards and Technology) as the basis for the U.S. standard encryption algorithm. The Data Encryption Standard (DES) was formally announced in 1977 in the *Federal Information Processing Standard Number 46* (FIPS 46).

The DES became the government standard for unclassified information and was adopted by business and for financial transactions and other applications requiring strong encryption. Although the official standard stipulated hardware implementations of the algorithm because of speed considerations in the late 1970s, improvements in computers quickly led to equally effective software implementations of the DES.

The DES can be used in four different modes:

- EBC, or Electronic Code Book, in which the same encryption key is independently applied to succeeding 64-bit blocks of plaintext. This method is not secure for long text.

- CBC, or Cipher Block Chaining, where the DES combines the current 64-bit block of ciphertext with the next 64 bits of plaintext to generate the next ciphertext. This technique is the most frequently used mode for encrypting files.

- CFB, or Cipher Feedback, which allows one to encrypt arbitrarily-defined blocks of text (usually 8 bits) by combining the ciphertext of the current block with the plaintext of the next block to be encrypted. This mode is often used for data transmissions.

- OFB, or Output Feedback, which is very similar to CFB, uses the whole 64-bit output of the DES encryption phase instead of just the block of ciphertext itself to help encrypt the next block of plaintext. Because the ciphertext blocks themselves are not used in decryption, transmission errors affecting a given block do not cause errors of decryption in subsequent blocks. For this reason, OFB is preferred for transmission of ciphertext over noisy channels.

Not all implementations of the DES are secure. Phil Zimmermann, creator of the popular PGP program (see below), cautions in one of his PGP documents,

The Government specifically recommends not using the weakest simplest mode for messages, the Electronic Codebook (ECB) mode. But they do recommend the stronger and more complex Cipher Feedback (CFB) or Cipher Block Chaining (CBC) modes.

Copyright © 1995, 2005 M. E. Kabay. All rights reserved.

Unfortunately, most of the commercial encryption packages I've looked at use ECB mode. When I've talked to the authors of a number of these implementations, they say they've never heard of CBC or CFB modes, and didn't know anything about the weaknesses of ECB mode. The very fact that they haven't even learned enough cryptography to know these elementary concepts is not reassuring. And they sometimes manage their DES keys in inappropriate or insecure ways.

In line with Zimmermann's warning, readers are urged to examine more than just marketing materials before committing to purchase DES-based software. Independent evaluations by reputable organizations are usually a better guide to reality than promotional texts.

CCEP and the DES

In 1988, the United States Department of Commerce and the National Security Agency proposed that government agencies abandon the DES in favor of the CCEP (Commercial COMSEC Endorsement Program). The CCEP includes a variety of encryption tools:

- Windster: secure voice communications
- Indictor: low-speed classified data applications
- Foresee: high-speed classified data
- Tepache classified computer networks.
- Edgeshot: sensitive, unclassified voice and low-speed data transmissions
- Brushstroke: high-speed data transmission
- Bulletproof: networking applications.

There was much agitation against the proposal to abandon the DES and the effort was eventually dropped. In 1994 the National Institute of Standards and Technology extended government approval for official use of the DES until 1999.

How Strong is the DES?

One of the recurring debates about the DES is its cryptographic strength. Conspiracy theorists have posited dark implications from the design's early reduction of key lengths. The original design had 128 bits, but the DES uses 56 bit keys; with today's high-speed parallel computational networks, it is possible in theory to crack a specific DES-enciphered message using brute-force attack (always supposing that the cleartext is machine-recognizable). Even worse, the full details of all components of he DES are not yet declassified; in particular, the "S-boxes" which execute the many cycles of permutation in and of 64-bit blocks by the algorithm are classified.

In a recent theoretical study of how a brute-force attack on the DES could be engineered, a cryptanalyst described how fast parallel processing could execute a known-plaintext attack to find a DES key. Depending on the number of processors, it might be possible to build a DES-cracker for $10,000,000 in 1993 currency that would find the key for an encrypted DES message in about 20 minutes. This is a theoretical issue, since it does not take into account the difficulty of identifying plaintext, especially numerical plaintext, using automated methods.

Copyright © 1995, 2005 M. E. Kabay. All rights reserved.

Despite these concerns, general opinion among professional cryptologists seems to be that the DES is in fact a secure algorithm. In the words of William Stallings, "The author feels that, except in areas of extreme sensitivity, the use of DES in commercial applications should not be a cause for concern by the responsible managers."

Triple DES

For those concerned about the supposed vulnerability of the DES, a popular variant is triple DES, in which there are multiple phases of encryption. Mathematically, it has been shown that encrypting a plaintext by two or more different DES keys does *not* produce ciphertext that could be generated by some other single DES key. In other words, the keyspace of sequential DES encryption is much larger than the usual DES keyspace. The usual form of triple DES actually uses only two keys:

- Encrypt the plaintext with key number one;
- "Decrypt" the ciphertext with key number two (actually, this is just a form of encryption with the second key);
- Encrypt the resulting ciphertext one more time with key number 1 again.

The reason this form of triple DES uses a "decryption" phase in the middle is that when there is only one key instead of two, the result of triple DES is identical to a single round of DES with one key. Thus a triple-DES user can apply the same software to decrypt a ciphertext from a single-DES user (because the first two steps of triple DES cancel out if key one = key two).

Unfortunately, even triple DES is not, in theory, safe from attacks. Several approaches have been proposed but are beyond the scope of this introduction. I=ll simply close by reaffirming that single DES is fine for commercial use and *a fortiori* so is triple DES.

RSA Public Key Cryptosystem

As mentioned in a preceding section, symmetric encryption algorithms use the same key to encrypt and to decrypt. If unique encryption keys are to be generated for each pair of correspondents, the number of keys grows as the square of the number of people who may wish to communicate. Keeping track of all these different keys becomes increasingly difficult as the number of users grows. Key distribution becomes a real headache, since every pair or group of people who want to sent encrypted messages to each other must arrange for the secure transmission of their particular keys.

In 1976, Whitfield Diffie and Martin Hellman published a landmark paper showing that it would be possible to generate *pairs* of encryption keys that would be complementary: what one key encrypts, the other key decrypts, and vice versa. They proposed that each user of such an asymmetric encryption system would keep one key private and make the other key public.

Suppose Alice wants to send Bob a message that only Bob can read. She encrypts her plaintext with Bob's public key; then only Bob can decrypt the ciphertext (he has to use his private key, which he has carefully protected from everyone else in the world).

Suppose Alice wants to send Bob a message which provably comes only from her. She can encrypt her message with her own private key; then everyone can decrypt the ciphertext using her

Copyright © 1995, 2005 M. E. Kabay. All rights reserved.

public key to be sure that she really sent the message and that it is unchanged. The confidence people will have in the authenticity of such a message will depend on how confident everyone is that the public key ostensibly belonging to Alice really is her public key. If someone were to post a public key and fraudulently *claim* that this key came from Alice, it would be possible to impersonate Alice electronically.

Suppose Alice wants to authenticate her message but also insists on its being readable only by Bob. Then she could start by encrypting the plaintext with her own private key (this authenticates it) and then encrypt the first-stage ciphertext using Bob's public key (this makes it unreadable by anyone except Bob--assuming that the public key really is Bob's).

RSADSI

A year after Diffie and Martin's pioneering paper, the mathematicians Ronald Rivest, Adi Shamir and Len Adleman came up with an implementation of Diffie and Hellman's suggestions. The scientists founded RSA Data Security Inc (RSADSI) and patented their algorithm, which has been known ever since as the RSA Public Key CryptosystemJ (RSA PKC). The system depends on the properties of large prime numbers; decrypting a ciphertext can be reduced to the effort required to factor very large numbers (200 decimal digits and beyond) into prime factors.

Since 1992, RSADSI has invited cryptographers to work on factoring various products of primes as a method of keeping everyone aware of progress in computational attacks on the RSA PKC. In 1994, several computer scientists orchestrated a systematic attack on a 129 (decimal) digit (429 bit) number. The team arranged for massively parallel computation involving 600 volunteers working in 24 countries over eight months on hundreds of 80486 processors (and also more powerful workstations). Estimates of the processing power for this effort ran to about 5000 MIPS-years (millions of instructions per second * years) of computation. The report on the project by its organizers, Derek Atkins, Michael Graff, Arjen Lenstra and Paul Leyland, began whimsically,

> We are happy to announce that
>
> RSA-129=114381625757888867669235779976146612010218296721242362562561842935706935245733897830597123563958705058989075147599290026879543541
> = 3490529510847650949147849619903898133417764638493387843990820577 *
> 32769132993266709549961988190834461413177642967992942539798288533

Although some critics of RSA claimed that this report cast doubt on the strength of the RSA PKC, others insisted that on the contrary, the difficulty involved in cracking a *single* public/private key pair showed how *strong* the algorithm is. The attack dealt with a particular key; in no sense did it show a fundamental weakness in the encryption algorithm itself.

PGP: Pretty Good Privacy

In June of 1991 Phil Zimmermann, a computer programmer and civil libertarian from Boulder, Colorado released version 1 of Pretty GoodJ Privacy, an encryption program, to the Internet. Phil Zimmermann apparently got the idea of calling his software "Pretty Good" from the famous National Public Radio program, *A Prairie Home Companion,* where Ralph's Pretty Good Grocery has been an imaginary sponsor for years. Since that humble start, PGP has become a world-wide success. It may be the single most popular encryption program in the world today. Specialized for use with electronic mail systems, it provides strong protection for encrypting and authenticating

Copyright © 1995, 2005 M. E. Kabay. All rights reserved.

messages and e-mail. Its strength and elegance are, ironically, attested to by government concern over international distribution of this product and its descendants.

The following indented sections quote extensively from the introduction to PGP 2.6.2 distributed by the Massachusetts Institute of Technology. I thank Phil Zimmermann for permission to include his work verbatim in this chapter. All references in the first person are by Mr Zimmermann.

Quick Overview of PGP

> Pretty Good(tm) Privacy (PGP), from Phil's Pretty Good Software, is a high security cryptographic software application for MSDOS, Unix, VAX/VMS, and other computers. PGP allows people to exchange files or messages with privacy, authentication, and convenience. Privacy means that only those intended to receive a message can read it. Authentication means that messages that appear to be from a particular person can only have originated from that person. Convenience means that privacy and authentication are provided without the hassles of managing keys associated with conventional cryptographic software. No secure channels are needed to exchange keys between users, which makes PGP much easier to use. This is because PGP is based on a powerful new technology called "public key" cryptography.
>
> PGP combines the convenience of the Rivest-Shamir-Adleman (RSA) public key cryptosystem with the speed of conventional cryptography, message digests for digital signatures, data compression before encryption, good ergonomic design, and sophisticated key management. And PGP performs the public-key functions faster than most other software implementations. PGP is public key cryptography for the masses.

PGP does not provide any built-in modem communications capability. You must use a separate software product for that.

Why Do You Need PGP?

It's personal. It's private. And it's no one's business but yours. You may be planning a political campaign, discussing your taxes, or having an illicit affair. Or you may be doing something that you feel shouldn't be illegal, but is. Whatever it is, you don't want your private electronic mail (E-mail) or confidential documents read by anyone else. There's nothing wrong with asserting your privacy. Privacy is as apple-pie as the Constitution.

Perhaps you think your E-mail is legitimate enough that encryption is unwarranted. If you really are a law-abiding citizen with nothing to hide, then why don't you always send your paper mail on postcards? Why not submit to drug testing on demand? Why require a warrant for police searches of your house? Are you trying to hide something? You must be a subversive or a drug dealer if you hide your mail inside envelopes. Or maybe a paranoid nut. Do law-abiding citizens have any need to encrypt their E-mail?

What if everyone believed that law-abiding citizens should use postcards for their mail? If some brave soul tried to assert his privacy by using an envelope for his mail, it would draw suspicion. Perhaps the authorities would open his mail to see what he's hiding. Fortunately, we don't live in that kind of world, because everyone protects most of their mail with envelopes. So no one draws suspicion by asserting their privacy with an envelope. There's safety in numbers. Analogously, it would be nice if everyone routinely used encryption for all their E-mail, innocent or not, so that no

Copyright © 1995, 2005 M. E. Kabay. All rights reserved.

one drew suspicion by asserting their E-mail privacy with encryption. Think of it as a form of solidarity.

Today, if the Government wants to violate the privacy of ordinary citizens, it has to expend a certain amount of expense and labor to intercept and steam open and read paper mail, and listen to and possibly transcribe spoken telephone conversation. This kind of labor-intensive monitoring is not practical on a large scale. This is only done in important cases when it seems worthwhile.

More and more of our private communications are being routed through electronic channels. Electronic mail is gradually replacing conventional paper mail. E-mail messages are just too easy to intercept and scan for interesting keywords. This can be done easily, routinely, automatically, and undetectably on a grand scale. International cablegrams are already scanned this way on a large scale by the NSA.

We are moving toward a future when the nation will be crisscrossed with high capacity fiber optic data networks linking together all our increasingly ubiquitous personal computers. E-mail will be the norm for everyone, not the novelty it is today. The Government will protect our E-mail with Government-designed encryption protocols. Probably most people will acquiesce to that. But perhaps some people will prefer their own protective measures.

Senate Bill 266, a 1991 omnibus anti-crime bill, had an unsettling measure buried in it. If this non-binding resolution had become real law, it would have forced manufacturers of secure communications equipment to insert special "trap doors" in their products, so that the Government can read anyone's encrypted messages. It reads: "It is the sense of Congress that providers of electronic communications services and manufacturers of electronic communications service equipment shall insure that communications systems permit the Government to obtain the plain text contents of voice, data, and other communications when appropriately authorized by law." This measure was defeated after rigorous protest from civil libertarians and industry groups.

In 1992, the FBI Digital Telephony wiretap proposal was introduced to Congress. It would require all manufacturers of communications equipment to build in special remote wiretap ports that would enable the FBI to remotely wiretap all forms of electronic communication from FBI offices. Although it never attracted any sponsors in Congress in 1992 because of citizen opposition, it was reintroduced in 1994.

Most alarming of all is the White House's bold new encryption policy initiative, under development at NSA since the start of the Bush administration, and unveiled April 16th, 1993. The centerpiece of this initiative is a Government-built encryption device, called the "Clipper" chip, containing a new classified NSA encryption algorithm. The Government is encouraging private industry to design it into all their secure communication products, like secure phones, secure FAX, etc. AT&T is now putting the Clipper into their secure voice products. The catch: At the time of manufacture, each Clipper chip will be loaded with its own unique key, and the Government gets to keep a copy, placed in escrow. Not to worry, though-- the Government promises that they will use these keys to read your traffic only when duly authorized by law. Of course, to make Clipper completely effective, the next logical step would be to outlaw other forms of cryptography.

If privacy is outlawed, only outlaws will have privacy. Intelligence agencies have access to good cryptographic technology. So do the big arms and drug traffickers. So do defense contractors, oil companies, and other corporate giants. But ordinary people and grassroots political organizations mostly have not had access to affordable "military grade" public-key cryptographic technology. Until now.

Copyright © 1995, 2005 M. E. Kabay. All rights reserved.

PGP empowers people to take their privacy into their own hands. There's a growing social need for it. That's why I wrote it.

How it Works

It would help if you were already familiar with the concept of cryptography in general and public key cryptography in particular. Nonetheless, here are a few introductory remarks about public key cryptography.

First, some elementary terminology. Suppose I want to send you a message, but I don't want anyone but you to be able to read it. I can "encrypt", or "encipher" the message, which means I scramble it up in a hopelessly complicated way, rendering it unreadable to anyone except you, the intended recipient of the message. I supply a cryptographic "key" to encrypt the message, and you have to use the same key to decipher or "decrypt" it. At least that's how it works in conventional "single-key" cryptosystems.

In conventional cryptosystems, such as the US Federal Data Encryption Standard (DES), a single key is used for both encryption and decryption. This means that a key must be initially transmitted via secure channels so that both parties can know it before encrypted messages can be sent over insecure channels. This may be inconvenient. If you have a secure channel for exchanging keys, then why do you need cryptography in the first place?

In public key cryptosystems, everyone has two related complementary keys, a publicly revealed key and a secret key (also frequently called a private key). Each key unlocks the code that the other key makes. Knowing the public key does not help you deduce the corresponding secret key. The public key can be published and widely disseminated across a communications network. This protocol provides privacy without the need for the same kind of secure channels that a conventional cryptosystem requires.

Anyone can use a recipient's public key to encrypt a message to that person, and that recipient uses her own corresponding secret key to decrypt that message. No one but the recipient can decrypt it, because no one else has access to that secret key. Not even the person who encrypted the message can decrypt it.

Message authentication is also provided. The sender's own secret key can be used to encrypt a message, thereby "signing" it. This creates a digital signature of a message, which the recipient (or anyone else) can check by using the sender's public key to decrypt it. This proves that the sender was the true originator of the message, and that the message has not been subsequently altered by anyone else, because the sender alone possesses the secret key that made that signature. Forgery of a signed message is infeasible, and the sender cannot later disavow his signature.

These two processes can be combined to provide both privacy and authentication by first signing a message with your own secret key, then encrypting the signed message with the recipient's public key. The recipient reverses these steps by first decrypting the message with her own secret key, then checking the enclosed signature with your public key. These steps are done automatically by the recipient's software.

Because the public key encryption algorithm is much slower than conventional single-key encryption, encryption is better accomplished by using a high-quality fast conventional single-key encryption algorithm to encipher the message. This original unenciphered message is called

Copyright © 1995, 2005 M. E. Kabay. All rights reserved.

"plaintext." In a process invisible to the user, a temporary random key, created just for this one "session", is used to conventionally encipher the plaintext file. Then the recipient's public key is used to encipher this temporary random conventional key. This public-key-enciphered conventional "session" key is sent along with the enciphered text (called "ciphertext") to the recipient. The recipient uses her own secret key to recover this temporary session key, and then uses that key to run the fast conventional single-key algorithm to decipher the large ciphertext message.

Public keys are kept in individual "key certificates" that include the key owner's user ID (which is that person's name), a time stamp of when the key pair was generated, and the actual key material. Public key certificates contain the public key material, while secret key certificates contain the secret key material. Each secret key is also encrypted with its own password, in case it gets stolen. A key file, or "key ring" contains one or more of these key certificates. Public key rings contain public key certificates, and secret key rings contain secret key certificates.

The keys are also internally referenced by a "key ID", which is an "abbreviation" of the public key (the least significant 64 bits of the large public key). When this key ID is displayed, only the lower 32 bits are shown for further brevity. While many keys may share the same user ID, for all practical purposes no two keys share the same key ID.

PGP uses "message digests" to form signatures. A message digest is a 128-bit cryptographically strong one-way hash function of the message. It is somewhat analogous to a "checksum" or CRC error checking code, in that it compactly "represents" the message and is used to detect changes in the message. Unlike a CRC, however, it is computationally infeasible for an attacker to devise a substitute message that would produce an identical message digest. The message digest gets encrypted by the secret key to form a signature.

Documents are signed by prefixing them with signature certificates, which contain the key ID of the key that was used to sign it, a secret-key-signed message digest of the document, and a time stamp of when the signature was made. The key ID is used by the receiver to look up the sender's public key to check the signature. The receiver's software automatically looks up the sender's public key and user ID in the receiver's public key ring.

Encrypted files are prefixed by the key ID of the public key used to encrypt them. The receiver uses this key ID message prefix to look up the secret key needed to decrypt the message. The receiver's software automatically looks up the necessary secret decryption key in the receiver's secret key ring.

These two types of key rings are the principal method of storing and managing public and secret keys. Rather than keep individual keys in separate key files, they are collected in key rings to facilitate the automatic lookup of keys either by key ID or by user ID. Each user keeps his own pair of key rings. An individual public key is temporarily kept in a separate file long enough to send to your friend who will then add it to her key ring.

Signing PGP Messages

Message authentication usually consists of creating a *message digest* by applying a *hash function* to the message content and combining the results with a unique key assigned to the originator. In this way, a short sequence of (usually) ASCII characters can be appended to the message and recalculating the same message digest proves that the message is intact and that the originator used their key to generate the message digest. Here is an example of what a PGP message looks like when it is signed:

Copyright © 1995, 2005 M. E. Kabay. All rights reserved.

-----BEGIN PGP SIGNED MESSAGE-----

This message has been signed by M. Kabay.

End of message.
-----BEGIN PGP SIGNATURE-----
Version: 2.7.1

iQB1AwUBMGW1EDPd6/an40lzAQFRqwL/TN03/E1IeDi1UlbEd18Disb4FEIOpkDe
Z1/hatnbt36szMrA25OixM4/SekAT7xDhU/JTpwOQAQ37nA2EcHUKtuY6XCdtbpg
lfw5blQlgbuDr90zns3Vn7VixQJPP1uf
=xpYE
-----END PGP SIGNATURE-----

And here is the same message with a single character changed: the period after Kabay is now an exclamation point:

-----BEGIN PGP SIGNED MESSAGE-----

This message has been signed by M. Kabay!

End of message.
-----BEGIN PGP SIGNATURE-----
Version: 2.7.1

iQB1AwUBMGW2CzPd6/an40lzAQGmNgL/TSJ1RqSAOIjGGUJVMAAHy/MNBCXS
SUhwT+I6kZ7UXJq2tH4/6ORH+HkZdIH76s1lxARkVCqIHokxXRZEJVCzTXgHreoK
obA7Eqo/qSHIc+EUY0U1iB8AiQB1zbjmnJKa
=ZGWC
-----END PGP SIGNATURE-----

Naturally, any attempt to sign the message using anything other than the originator's own secret key results in an authentication failure when PGP checks the message digest.

Just to demonstrate the effect of encryption, here are the two sample messages, each encrypted using my secret key. The two messages are

This message has been signed and encrypted by M. Kabay.

End of message.

and

This message has been signed and encrypted by M. Kabay!

End of message.

Copyright © 1995, 2005 M. E. Kabay. All rights reserved.

The corresponding ciphertexts are:

```
-----BEGIN PGP MESSAGE-----
Version: 2.7.1

hGwDM93r9qfjSXMBAvkBL5FXEdHh5Jiaag91hBSzr4iuZ5AE794hoO6rmvxamvnK
hHZOg+V4Bu0XQszSsfopeuo2/Qe4q+X+RHAu+FteYb2EfCBnzafu7GkISdoOLh1h
cTa0gftVhG1W0pqAJQymAAAA5zx3DUrgK7y64QRRT5nJPon/d5P6BDif5p9vUW2/
E91Cugy8CMQQoAUnlfR8cRKdmZVq9kS0a6TZullzc259qxwHO3B8ytho5uh8gFlK
wK3/FArNuAqnhZuWuonD9L5mRKID1LeO2ZjOBaOB51rZmG5AzMNXu8M3KX5q
d0UH7dQ15MJPYmRdBLo0pM2iulA28vUIWTVlgV9pMEGnPYv1FerpFfmD3cKQeR
B/8YcamzveH7IYA46QfgYh6a9GWS4YVcqoVHjAaj0HYtlkZ3KNPgiW4xtzg7/D93vYR
D2fncY8ctAGUZ9m7A==
=0yo4
-----END PGP MESSAGE-----
```

and

```
-----BEGIN PGP MESSAGE-----
Version: 2.7.1

hGwDM93r9qfjSXMBAv49Ktos1o6XvR2zByAQYWpiti1kU2Yo84z9FJdmtajEJHWC
IwRjTeNAWzOGV+h/7C6Da+dTFlkJylPJr8aIJUgZarRSlichW/YQHhVJ48SKm2P0
YdYwCQeqVIwA0ISj6t+mAAAA53OVUM2tCrvbzRDorInLhLYlokEdIUI5KmdW3N+
pdcQEpx2owmz9aORB/oSgqvFd0gzHwoZ4kS9MNNxYuijDVYovay7jZ8Ossn0NbMQa
j49Fi7/iBFnNvvC6szicSr+lVoPFiybtizbLAMEE4bNm1R2Vfzd7KqseaAdjjE7jxlA04kIE35
DZCTffL13PCaBL58ILxi69D7KCwuUXu60m9MSvd8U6mkAEZ3pWi3h1rzw8tU+uvH
gNsdriO5wtSvlPcBENFmG4xW56B0JQbYPnC4TJR/9N/6zivQjQtwrxMvtsj9wV5rWmL
w==
=9KH8
-----END PGP MESSAGE-----
```

Export Controls on PGP

Phil Zimmerman explains the restrictions in place in the early 1990s.

> The U.S. Government has made it illegal in most cases to export good cryptographic technology, and that may include PGP. They regard this kind of software just like they regard munitions. This is determined not by legislation, but by administrative policies of the State Department, Defense Department and Commerce Department.
>
> The U.S. Government is using export restrictions as a means of suppressing both domestic and foreign availability of cryptographic technology. In particular, it is trying to suppress the emergence of an international standard for cryptographic protocols, until it can establish the Escrowed Encryption Standard (the Clipper chip) as the dominant standard.
>
> Any export restrictions on PGP are imposed by the US Government. This does not imply that I or MIT agree with these restrictions. We just comply with them. We do not impose additional licensing restrictions of our own on the use of PGP outside of the US, other than those restrictions that already apply inside the US. PGP may be subject to export controls.

Copyright © 1995, 2005 M. E. Kabay. All rights reserved.

Anyone wishing to export it should first consult the State Department's Office of Defense Trade Controls.

I will not export this software out of the US or Canada in cases when it is illegal to do so under US controls, and I urge other people not to export it on their own. If you live outside the US or Canada, I urge you not to violate US export laws by getting any version of PGP in a way that violates those laws. Since thousands of domestic users got the first version after its initial publication, it somehow leaked out of the US and spread itself widely abroad, like dandelion seeds blowing in the wind.

Starting with PGP version 2.0 through version 2.3a, the release point of the software has been outside the US, on publicly-accessible computers in Europe. Each release was electronically sent back into the US and posted on publicly-accessible computers in the US by PGP privacy activists in foreign countries. There are some restrictions in the US regarding the import of munitions, but I'm not aware of any cases where this was ever enforced for importing cryptographic software into the US. I imagine that a legal action of that type would be quite a spectacle of controversy.

ViaCrypt PGP is sold in the United States and Canada and is not for export. The following language was supplied by the US Government to ViaCrypt for inclusion in the ViaCrypt PGP documentation: "PGP is export restricted by the Office of Export Administration, United States Department of Commerce and the Offices of Defense Trade Controls and Munitions Control, United States Department of State. PGP cannot be exported or reexported, directly or indirectly, (a) without all export or reexport licenses and governmental approvals required by any applicable laws, or (b) in violation of any prohibition against the export or reexport of any part of PGP." The Government may take the position that the freeware PGP versions are also subject to those controls.

The freeware PGP versions 2.5 and 2.6 were released through a posting on a controlled FTP site maintained by MIT. This site has restrictions and limitations which have been used on other FTP sites to comply with export control requirements with respect to other encryption software such as Kerberos and software from RSA Data Security, Inc. I urge you not to do anything which would weaken those controls or facilitate any improper export of PGP.

Although PGP has become a worldwide de facto standard for E-mail encryption, and is widely available overseas, I still get calls from people outside the US who ask me if it is legal to use it in their own country, for versions that are already available there. Please don't contact me to ask me if it is legal to use PGP in your country if you live outside the US. That question is not up to me. I've got enough legal problems of my own with export control issues, without getting involved in giving you legal advice over my phone. It might even put me at some legal risk to simply answer a question like that for a foreigner. If this question concerns you, ask someone else, like a lawyer.

You may have a need to use PGP in a commercial application outside the US or Canada. Unfortunately, at the time of this writing, there is no current commercial source for PGP outside the US or Canada. I am trying to find a US-legal way to make a commercially licensed version available abroad, but right now the US export restrictions make that difficult without putting me at legal risk. This situation may change.

Copyright © 1995, 2005 M. E. Kabay. All rights reserved.

Some foreign governments impose serious penalties on anyone inside their country for merely using encrypted communications. In some countries they might even shoot you for that. But if you live in that kind of country, perhaps you need PGP even more.

Philip Zimmermann's Legal Situation

At the time of this writing [September 1994], I am the target of a US Customs criminal investigation in the Northern District of California. A criminal investigation is not a civil lawsuit. Civil lawsuits do not involve prison terms. My defense attorney has been told by the Assistant US Attorney that the area of law of interest to the investigation has to do with the export controls on encryption software. The federal mandatory sentencing guidelines for this offense are 41 to 51 months in a federal prison. US Customs appears to be taking the position that electronic domestic publication of encryption software is the same as exporting it. The prosecutor has issued a number of federal grand jury subpoenas. It may be months before a decision is reached on whether to seek indictment. This situation may change at any time, so this description may be out of date by the time you read it. Watch the news for further developments. If I am indicted and this goes to trial, it will be a major test case.

I have a legal defense fund set up for this case. So far, no other organization is doing the fundraising for me, so I am depending on people like you to contribute directly to this cause. If you care about the future of your civil liberties in the information age, then perhaps you will care about this case. The legal fees are expensive, the meter is running, and I need your help. The fund is run by my lead defense attorney, Phil Dubois, here in Boulder. Please send your contributions to:

Philip L. Dubois, Lawyer
2305 Broadway
Boulder, Colorado 80304 USA
Phone (303) 444-3885
E-mail: dubois@csn.org

Copyright © 1995, 2005 M. E. Kabay. All rights reserved.

You can also phone in your donation and put it on Mastercard or Visa. If you want to be really cool, you can use Internet E-mail to send in your contribution, encrypting your message with PGP so that no one can intercept your credit card number. Include in your E-mail message your Mastercard or Visa number, expiration date, name on the card, and amount of donation. Then sign it with your own key and encrypt it with Phil Dubois's public key (his key is included in the standard PGP distribution package, in the "keys.asc" file). Put a note on the subject line that this is a donation to my legal defense fund, so that Mr. Dubois will decrypt it promptly. Please don't send a lot of casual encrypted E-mail to him -- I'd rather he use his valuable time to work on my case.

Getting PGP

PGP is available for any non-commercial and non-governmental use in the United States from the Massachusetts Institute of Technology FTP site (start with Telnet to net-dist.mit.edu using "getpgp" as the login; then follow the instructions to retrieve the files). It is available on CompuServe in the NCSA InfoSecurity Forum (GO NCSAFO) in the Export-Restricted Library (section 12) with permission from the NCSA Sysops (see file EXPORT.TXT in sections 1 or 6 of NCSAFO for instructions on how residents of the U.S. and Canada can obtain such permission). There are many other sites world-wide which make PGP freeware available, including on the World Wide Web; open http://rschp2.anu.edu.au:8080/pgpfaq.html for a detailed list of options on where to get the program and many other PGP-related issues.

Commercial and governmental users of PGP in the United States and Canada must buy a license from ViaCrypt. Contact ViaCrypt as follows:

Paul E. Uhlhorn, Director of Marketing
ViaCrypt Products
9033 North 24th Avenue, Suite 7
Phoenix, AZ 85021 USA
Phone: 602-944-0773
Fax: 602-943-2601
E-mail: viacrypt@acm.org or 70304.41@compuserve.com

ViaCrypt have their own support section on CompuServe in the NCSA Security Vendor Forum (GO NCSAVE).

PGP Shells

A number of shareware and freeware programs are available for different platforms to reduce the need for command-line interaction with PGP. Several are available in the NCSA Vendor Forum (GO NCSAVE) and the NCSA InfoSecurity Forum (GO NCSAFO) on CompuServe. ViaCrypt's PGP 2.7.2 for Windows has an easy-to-use menu-driven interface for all aspects of key management, encryption and decryption. In addition, ViaCrypt makes available a special front-end for integration with CompuServe's special access programs, CompuServe Navigator (CSNAV) and CompuServe Information Manager (CIM). The ViaCrypt add-ons allow single-click signing, authentication, encryption and decryption of electronic mail in the In-Basket and Out-Basket of the CompuServe programs.

Documentation about PGP

William Stallings has written a superb reference manual for PGP, *Protect Your Privacy: A Guide for PGP Users* (see full reference in chapter notes). Phil Zimmermann writes in the Foreword,

Copyright © 1995, 2005 M. E. Kabay. All rights reserved.

> ...Bill Stalling's book is more comprehensive than mine, more thorough, covering more detail, with a lot more diagrams. He's really good at completely nailing it down in a book. In fact, I=ll probably use his book myself as my preferred reference to PGP.

As usual, Dr Stalling's prose is lucid and fun to read. Enough said: buy William Stalling's book and use it.

DSS

In 1991, the Computer Systems Laboratory (CSL) of the U.S. National Institute of Standards and Technology (NIST) proposed the Digital Signature Standard (DSS) as a new standard for authenticating e-mail. The DSS is based on the Digital Signature Algorithm (DSA) which in turn derives from work by ElGamal (1985) and Schnorr (1990) on the use of discrete logarithms as a basis for public-key encryption. The DSA can be used only for authentication, not for message encryption. Over time, the proposal was refined in response to criticisms of the initial definition of 512-bit keys; NIST revised the DSA to allow 1024-bit keys.

The more interesting issue, however, turned out to be legal and political rather than technical. The inventors of the Public Key Cryptosystem had already patented public key-encryption, claiming rights over any implementation of the concept, regardless of algorithms used. The group called Public Key Partners (PKP), including RSADSI, MIT, Stanford University and Claus Schnorr, protested the government's promulgation of a public-key authentication standard. In 1993, PKP and NIST came to an agreement that would see PKP holding worldwide, exclusive licensing rights to the DSS. In return, PKP granted to the U.S. government a license to use the DSS without paying royalties to PKP. All other users of software incorporating the DSS would have to pay modest royalties to PKP.

Many U.S. government agencies immediately announced plans to implement the DSS in their e-mail and electronic data interchange systems. However, on the commercial side, a storm of protest swept the world (well, it swept the sci.crypt news group, anyway). Ross Williams, a cryptographer from Adelaide, Australia, summarized the arguments against the very notion of a deal with PKP concerning the DSS. In a blistering message posted to sci.crypt on August 4, 1993, he said that there were objections to:

- software patents in general;
- publicly-funded universities= owning patents at all;
- such universities= assigning such patents to commercial companies;
- PKP's allegedly holding up the diffusion of public-key technology;
- the alleged involvement of the National Security Agency of the U.S. in creating the DSA;
- NIST's choosing the DSA as a standard instead of RSA;
- NIST's embodying the DSA in a patent;
- government agencies= assigning patents to commercial companies;
- NIST's assigning the patent to a single company;
- NIST's effectively extending PKP's patent powers;
- NIST's making it more difficult for companies wishing to fight PKP's assertion of patent.

By January 1994, NIST had received 270 comments on the proposal to grant PKP the exclusive right to license the DSA to commercial interests; 260 of the responses were critical of the proposal. By May of 1994, NIST had decided to withdraw from its agreement with PKP; NIST promulgated Federal Information Processing Standard (FIPS) 186 effective December 1, 1994 and

Copyright © 1995, 2005 M. E. Kabay. All rights reserved.

specified that the DSS and the DSA could be used free by anyone. In June 1994, the government promised to defend any contractor supplying DSA-based software to the U.S. government if they were sued by PKP for patent infringement. At the time of writing this chapter, (September 1995) the issue has still not been resolved in the courts.

The bottom line is that NIST's actions and PKP's insistence on royalties have divided the world of digital signature. As government agencies increase their use of the DSS, there will be growing pressure on the commercial sector to fall into line; however, the popularity of RSA encryption in the private sector (not least because of the explosive distribution of PGP) means that there will likely be two competing standards of authentication for some years to come. This case raises difficult problems rooted in the concepts of intellectual property rights; it will be very interesting to follow events as the legal machinations continue.

PEM

Privacy Enhanced Mail is a proposed standard for Internet e-mail. The details are defined in the Requests for Comment (RFCs) numbers 1421 through 1424 available from the Internet Activities Board (IAB); available by anonymous FTP from ftp.uu.net in /inet/rfc/* or from ftp.wustl.edu on path /doc/rfc/*. The key features of PEM are that it

- provides for message encryption of ASCII messages;
- supports authentication of message origins;
- guarantees that breaches of message integrity will be discovered;
- supports non-repudiation of origin;
- is defined to be platform independent;
- does not require changes to e-mail systems carrying the encrypted or digitally-signed messages;
- supports options in the encryption methods chosen for specific systems and messages.

PEM takes care of problems that can plague users of encrypted e-mail. For example, some e-mail systems convert carriage-return/line-feed pairs (CR/LF) into LFs only. Any such change will make message authentication codes invalid. PEM ensures that these problems will not happen; it converts all plaintext into printable ASCII codes before calculating message digests or encrypting the text. On the receiving side, PEM verifies message integrity before converting the message back into its original form.

Both PEM and PGP use a conversion routine called *radix-64*. This method of encoding any binary stream into printable characters simply reads of every group of 6 bits and assigns a corresponding character (A-Z, a-z, 0-9, +, and /) to the 6-bit group. For example, the ASCII string "ABC" corresponds to the following three bytes: 01000001 01000010 01000011. Regrouping in blocks of 6 bits instead of 8 bits, we have 010000 010100 001001 000011. These binary numbers correspond to decimal 16, 20, 9 and 3. The corresponding characters in radix-64 are Q, U, J and D. On the receiving end, "QUJD" would be converted back to "ABC" using the converse processes of regrouping bits from the 6-bit blocks into 8-bit bytes.

PKCS

The following description of the PKCS is taken directly from the RSA FAQ (Frequently-Asked Questions) written by Paul Fahn of RSA Laboratories:

Copyright © 1995, 2005 M. E. Kabay. All rights reserved.

PKCS (Public-Key Cryptography Standards) is a set of standards for implementation of public-key cryptography. It has been issued by RSA Data Security, Inc. in cooperation with a computer industry consortium, including Apple, Microsoft, DEC, Lotus, Sun and MIT. PKCS has been cited by the OIW (OSI Implementors' Workshop) as a method for implementation of OSI standards. PKCS is compatible with PEM ... but extends beyond PEM. For example, where PEM can only handle ASCII data, PKCS is designed for binary data as well. PKCS is also compatible with the CCITT X.509 standard.

PKCS includes both algorithm-specific and algorithm-independent implementation standards. Specific algorithms supported include RSA, DES, and Diffie-Hellman key exchange. It also defines algorithm-independent syntax for digital signatures, digital envelopes (for encryption), and certificates; this enables someone implementing any cryptographic algorithm whatsoever to conform to a standard syntax and thus preserve interoperability. Documents detailing the PKCS standards can be obtained by sending e-mail to pkcs@rsa.com or by anonymous ftp to rsa.com.

Entrust

In March 1994, Northern Telecom (now NorTel) introduced its Entrust encryption and digital signature products at the Federal Office Systems Expo (FOSE) in Washington, DC. Entrust 1.2 was announced in August 1995. The product family supports Macintosh, UNIX, and Windows versions and offers options for digital signatures using RSA and DSS; encryption can be accomplished using DES and a proprietary algorithm. In addition, a special version is available for international installation. This product is spreading throughout the Canadian government, with licenses already in place in several ministries. It seems to offer a palatable user interface and a good mechanism for managing encryption keys. Costs to a few thousand U.S. dollars for directory services and server software and about U$150 per client software copy. If government support for this product continues, it stands an excellent chance of becoming a de facto standard for anyone doing business with the Canadian government.

Key Management

There are three major management issues related to encryption keys:

- How do we obtain the appropriate decryption key for an encrypted message or to validate a digital signature?
- How do we know a public key ostensibly belonging to someone genuinely does belong to that person?
- How do we check the integrity and authenticity of a message encrypted or signed some time ago--when people can change their public keys at will?

Key Distribution

In symmetric encryption schemes (e.g., use of the DES to encrypt e-mail or files), the same key is applied to plaintext and to ciphertext. If the channel for transmitting ciphertext is viewed as insecure enough to warrant encryption, the same channel can evidently not be used to send the encryption/decryption key in the clear. Each group of users requiring a shared encryption/decryption key must therefore arrange for secure key exchange.

Can one use a different encryption key to encrypt the encryption key that will serve for one or more messages? Yes, but then we are on the first step of infinite regress: how will we protect the

Copyright © 1995, 2005 M. E. Kabay. All rights reserved.

"meta-key" that encrypts the "real" encryption key? Ultimately, all symmetric encryption keys share the fundamental problem of secure exchange; all such systems must rely on an additional secure channel for key exchange.

As a simple-minded example of secure key exchange for symmetric encryption, one could choose an encryption key, place it in an opaque envelope, seal it in a tamper-proof container, and ship it by a bonded service such as Federal Express or Purolator. This key could then be used for one or more messages; the degree of confidence in the confidentiality, integrity and authenticity of such ciphertexts would depend entirely on the confidence we placed in the courier service and the physical mechanisms of protection for the key. Variations on such methods might involve using additional channels of communication: steganography, for instance--hiding additional levels of encryption keys in graphics files; or sending the key using a one-time pad for encryption. However, even the one-time pad depends on the trustworthiness of the mechanisms for distributing the copies of the pad to authorized users. No, there is no way to simplify the distribution of symmetric encryption keys. One way or another, we have to use alternative channels to communicate the keys themselves securely.

The other major problem with symmetric encryption systems, as already noted in the introduction to such methods, is the quadratic increase in the number of key pairs required for secure pair-wise and group-wise encryption and decryption. That is, the number of pairs of unique keys required to allow every member of a group of size "n" to communicate secretly with any other member of the group is $n(n-1)/2 = (n^2 - n)/2$. For example, the number of pairwise encryption keys needed to let 10 people send messages securely to any of their colleagues is 45. The number of keys required for all possible groups from size 2 to size n is a much higher power relation. Again using a mere 10 people, the number of pairwise, triple, quadruple etc. keys that could be needed for all possible groupings is 1013.

Keeping track securely of all these secret keys is a management nightmare.

Consider in contrast the simplicity of the asymmetric public key systems. The number of keys to keep secret is exactly the same as the number of individuals sending and signing messages. All one has to do is provide a directory of public keys in order to provide for validation and authentication of encrypted and signed messages.

Key Authentication

The problem that remains is how to be sure that no one else pops a public key into place claiming that it is *your* key. If someone did falsely attribute their key to you, they could fool people into believing that you had sent whatever message the imposter chose to encrypt or sign.

Basically, the solution consists of certification of public keys. Two rather different approaches have been proposed and informally implemented to date. One method, described as a web of trust, is an informal method for certifying the authenticity of keys by relying on people whose keys you trust. If you need to ascertain the reliability of the public key for someone you don=t personally know and have not communicated with, you can look at who has signed his or her key. If you trust the signers, you can trust the new member of the information group. This method is by no means fool-proof; a determined attack on the trustworthiness of the system could be carried out as effectively as any other impersonation--in cyberspace or in the real world. Indeed, the question becomes moot: if someone always calls themselves Martha Washington, whether in electronic mail, postings on news groups, on her driver's license, and in all aspects of her normal existence, do we really care if she was named Barbarella Putani at birth? As long as we can trace the human being behind an identity, most of us will be happy with whatever name they always use.

Copyright © 1995, 2005 M. E. Kabay. All rights reserved.

The other method for certifying public keys is to set up a formal hierarchy of key-signing authorities. The hierarchy could reflect the governmental structure, for example. The top of the executive branch can publish its own public keys widely. The top signing authorities can then authorize a larger number of secondary signing authorities by signing their public keys. In turn, the secondary signing authorities can then establish many tertiary authorities, signing their keys. The hierarchy could go all the way down to official signing authorities in every corporation, university, non-profit, military base and post office in the land. Ordinary citizens wishing to establish their own public key for anyone to use would then present appropriate identification and authentication to, say, a clerk in the post office; the same standards might apply for acceptance of a new public key as for issuance of a passport.

Of course, there are lots of false passports around.

No doubt there would be an equal number of false public keys around too.

In either method, the informal web of trust or the hierarchy of authorities, fraud could be fought by authenticated repudiation of false or compromised public keys. Say you accidentally allow your secret pass-phrase--the one required to use your PGP secret key--to be known to someone else. All future communications using that secret key would be compromised. You would then issue a public cancellation notice for the original public key and issue a new one, duly authenticated by signature from someone whose word would be trusted (or from a duly-designated signing authority).

Digital Time Stamps

Another practical problem comes to mind for public/private key cryptography. What if you have to sign legal documents using a digital signature? What if the years roll by and someone has to show that you really did sign those documents--that is, that the digital signature is authentic? If your public key has not changed, there is no problem. However, if you are now on the sixth public key since the one you used years ago, how could anyone find the key in use back in the past? Is everyone supposed to keep a record of all the public keys everyone else ever uses?

To eliminate this problem, several proposals have been offered that discuss a public time-stamping and authentication service. A secure server somewhere receives any electronic message and validates it using the current public key of the sender. The server then signs the message using a key constructed securely from its own secret key and a date/time-stamp. As long as the server remains trustworthy, it is possible for it to re-affirm the validity of any of its own time-stamps at any time in the future, regardless of changes in the public keys of the message originator. Essentially, the server guarantees that the digital signature was correct when the signed message was submitted; no record of the sender's public key need be maintained thereafter.

Copyright © 1995, 2005 M. E. Kabay. All rights reserved.

The Key Escrow Proposal

In April 1993, the Clinton administration issued the following announcement and arranged to have it posted on the sci.crypt news group on the Internet. Because of continued interest in and importance of the Key Escrow Proposal, I have included several original documents verbatim (with permission of the authors where necessary). Minor changes in layout have been made to improve clarity.

> Date: Fri, 16 Apr 1993 15:19:06 GMT
> From: clipper@csrc.ncsl.nist.gov (Clipper Chip Announcement)
> Organization: National Institute of Standards & Technology
> Sender: news@dove.nist.gov
> Subject: text of White House announcement and Q&As on clipper chip encryption
> News groups: sci.crypt
> Distribution: na
> Lines: 282

Note: This file will also be available via anonymous file transfer from csrc.ncsl.nist.gov in directory /pub/nistnews and via the NIST Computer Security BBS at 301-948-5717.

THE WHITE HOUSE

Office of the Press Secretary

_____
For Immediate Release April 16, 1993

STATEMENT BY THE PRESS SECRETARY

The President today announced a new initiative that will bring the Federal Government together with industry in a voluntary program to improve the security and privacy of telephone communications while meeting the legitimate needs of law enforcement.

The initiative will involve the creation of new products to accelerate the development and use of advanced and secure telecommunications networks and wireless communications links.

For too long there has been little or no dialogue between our private sector and the law enforcement community to resolve the tension between economic vitality and the real challenges of protecting Americans. Rather than use technology to accommodate the sometimes competing interests of economic growth, privacy and law enforcement, previous policies have pitted government against industry and the rights of privacy against law enforcement.

Sophisticated encryption technology has been used for years to protect electronic funds transfer. It is now being used to protect electronic mail and computer files. While encryption technology can help Americans protect business secrets and the unauthorized release of personal information, it also can be used by terrorists, drug dealers, and other criminals.

A state-of-the-art microcircuit called the "Clipper Chip" has been developed by government engineers. The chip represents a new approach to encryption technology. It can be used in new, relatively inexpensive encryption devices that can be attached to an ordinary telephone. It

Copyright © 1995, 2005 M. E. Kabay. All rights reserved.

scrambles telephone communications using an encryption algorithm that is more powerful than many in commercial use today.

This new technology will help companies protect proprietary information, protect the privacy of personal phone conversations and prevent unauthorized release of data transmitted electronically. At the same time this technology preserves the ability of federal, state and local law enforcement agencies to intercept lawfully the phone conversations of criminals.

A "key-escrow" system will be established to ensure that the "Clipper Chip" is used to protect the privacy of law-abiding Americans. Each device containing the chip will have two unique "keys," numbers that will be needed by authorized government agencies to decode messages encoded by the device. When the device is manufactured, the two keys will be deposited separately in two "key-escrow" data bases that will be established by the Attorney General. Access to these keys will be limited to government officials with legal authorization to conduct a wiretap.

The "Clipper Chip" technology provides law enforcement with no new authorities to access the content of the private conversations of Americans.

To demonstrate the effectiveness of this new technology, the Attorney General will soon purchase several thousand of the new devices. In addition, respected experts from outside the government will be offered access to the confidential details of the algorithm to assess its capabilities and publicly report their findings.

The chip is an important step in addressing the problem of encryption's dual-edge sword: encryption helps to protect the privacy of individuals and industry, but it also can shield criminals and terrorists. We need the "Clipper Chip" and other approaches that can both provide law-abiding citizens with access to the encryption they need and prevent criminals from using it to hide their illegal activities. In order to assess technology trends and explore new approaches (like the key-escrow system), the President has directed government agencies to develop a comprehensive policy on encryption that accommodates:

-- the privacy of our citizens, including the need to employ voice or data encryption for business purposes;

-- the ability of authorized officials to access telephone calls and data, under proper court or other legal order, when necessary to protect our citizens;

-- the effective and timely use of the most modern technology to build the National Information Infrastructure needed to promote economic growth and the competitiveness of American industry in the global marketplace; and

-- the need of U.S. companies to manufacture and export high technology products.

The President has directed early and frequent consultations with affected industries, the Congress and groups that advocate the privacy rights of individuals as policy options are developed.

The Administration is committed to working with the private sector to spur the development of a National Information Infrastructure which will use new telecommunications and computer technologies to give Americans unprecedented access to information. This infrastructure of high-speed networks ("information superhighways") will transmit video, images, HDTV programming, and huge data files as easily as today's telephone system transmits voice.

Copyright © 1995, 2005 M. E. Kabay. All rights reserved.

Since encryption technology will play an increasingly important role in that infrastructure, the Federal Government must act quickly to develop consistent, comprehensive policies regarding its use. The Administration is committed to policies that protect all Americans' right to privacy while also protecting them from those who break the law.

Further information is provided in an accompanying fact sheet. The provisions of the President's directive to acquire the new encryption technology are also available.

For additional details, call Mat Heyman, National Institute of Standards and Technology, (301) 975-2758.

QUESTIONS AND ANSWERS ABOUT THE CLINTON ADMINISTRATION'S TELECOMMUNICATIONS INITIATIVE

Q: Does this approach expand the authority of government agencies to listen in on phone conversations?

A: No. "Clipper Chip" technology provides law enforcement with no new authorities to access the content of the private conversations of Americans.

Q: Suppose a law enforcement agency is conducting a wiretap on a drug smuggling ring and intercepts a conversation encrypted using the device. What would they have to do to decipher the message?

A: They would have to obtain legal authorization, normally a court order, to do the wiretap in the first place. They would then present documentation of this authorization to the two entities responsible for safeguarding the keys and obtain the keys for the device being used by the drug smugglers. The key is split into two parts, which are stored separately in order to ensure the security of the key escrow system.

Q: Who will run the key-escrow data banks?

A: The two key-escrow data banks will be run by two independent entities. At this point, the Department of Justice and the Administration have yet to determine which agencies will oversee the key-escrow data banks.

Q: How strong is the security in the device? How can I be sure how strong the security is?

A: This system is more secure than many other voice encryption systems readily available today. While the algorithm will remain classified to protect the security of the key escrow system, we are willing to invite an independent panel of cryptography experts to evaluate the algorithm to assure all potential users that there are no unrecognized vulnerabilities.

Q: Whose decision was it to propose this product?

A: The National Security Council, the Justice Department, the Commerce Department, and other key agencies were involved in this decision. This approach has been endorsed by the President, the Vice President, and appropriate Cabinet officials.

Copyright © 1995, 2005 M. E. Kabay. All rights reserved.

Q: Who was consulted? The Congress? Industry?

A: We have on-going discussions with Congress and industry on encryption issues, and expect those discussions to intensify as we carry out our review of encryption policy. We have briefed members of Congress and industry leaders on the decisions related to this initiative.

Q: Will the government provide the hardware to manufacturers?

A: The government designed and developed the key access encryption microcircuits, but it is not providing the microcircuits to product manufacturers. Product manufacturers can acquire the microcircuits from the chip manufacturer that produces them.

Q: Who provides the "Clipper Chip"?

A: Mykotronx programs it at their facility in Torrance, California, and will sell the chip to encryption device manufacturers. The programming function could be licensed to other vendors in the future.

Q: How do I buy one of these encryption devices?

A: We expect several manufacturers to consider incorporating the "Clipper Chip" into their devices.

Q: If the Administration were unable to find a technological solution like the one proposed, would the Administration be willing to use legal remedies to restrict access to more powerful encryption devices?

A: This is a fundamental policy question which will be considered during the broad policy review. The key escrow mechanism will provide Americans with an encryption product that is more secure, more convenient, and less expensive than others readily available today, but it is just one piece of what must be the comprehensive approach to encryption technology, which the Administration is developing.

The Administration is not saying, "since encryption threatens the public safety and effective law enforcement, we will prohibit it outright" (as some countries have effectively done); nor is the U.S. saying that "every American, as a matter of right, is entitled to an unbreakable commercial encryption product." There is a false "tension" created in the assessment that this issue is an "either-or" proposition. Rather, both concerns can be, and in fact are, harmoniously balanced through a reasoned, balanced approach such as is proposed with the "Clipper Chip" and similar encryption techniques.

Q: What does this decision indicate about how the Clinton Administration's policy toward encryption will differ from that of the Bush Administration?

A: It indicates that we understand the importance of encryption technology in telecommunications and computing and are committed to working with industry and public-interest groups to find innovative ways to protect Americans' privacy, help businesses to compete, and ensure that law enforcement agencies have the tools they need to fight crime and terrorism.

Copyright © 1995, 2005 M. E. Kabay. All rights reserved.

Q: Will the devices be exportable? Will other devices that use the government hardware?

A: Voice encryption devices are subject to export control requirements. Case-by-case review for each export is required to ensure appropriate use of these devices. The same is true for other encryption devices. One of the attractions of this technology is the protection it can give to U.S. companies operating at home and abroad. With this in mind, we expect export licenses will be granted on a case-by-case basis for U.S. companies seeking to use these devices to secure their own communications abroad. We plan to review the possibility of permitting wider exportability of these products.

CPSR Responds

The reaction was immediate. The Computer Programmers for Social Responsibility (CPSR) fired off the first salvo:

> Date: Fri, 16 Apr 1993 21:46:37 GMT
> From: Dave Banisar <Banisar@washofc.cpsr.org>
> Organization: CPSR, Civil Liberties and Computing Project
> Sender: usenet@eff.org (NNTP News Poster)
> Subject: CPSR Statement on White House Crypto Plan
> News groups: sci.crypt,alt.privacy,comp.org.eff.talk,alt.security,alt.dcom.telecom Lines: 60
> Xref: wrldlnk sci.crypt:12501 alt.privacy:6539 comp.org.eff.talk:16847 alt.security:9991 alt.dcom.telecom:1778
> ---
> April 16, 1993
> Washington, DC
>
> COMPUTER PROFESSIONALS CALL FOR PUBLIC DEBATE ON NEW GOVERNMENT ENCRYPTION INITIATIVE
>
> Computer Professionals for Social Responsibility (CPSR) today called for the public disclosure of technical data underlying the government's newly-announced "Public Encryption Management" initiative. The new cryptography scheme was announced today by the White House and the National Institute for Standards and Technology (NIST), which will implement the technical specifications of the plan. A NIST spokesman acknowledged that the National Security Agency (NSA), the super- secret military intelligence agency, had actually developed the encryption technology around which the new initiative is built.
>
> According to NIST, the technical specifications and the Presidential directive establishing the plan are classified. To open the initiative to public review and debate, CPSR today filed a series of Freedom of Information Act (FOIA) requests with key agencies, including NSA, NIST, the National Security Council and the FBI for information relating to the encryption plan. The CPSR requests are in keeping with the spirit of the Computer Security Act, which Congress passed in 1987 in order to open the development of non-military computer security standards to public scrutiny and to limit NSA's role in the creation of such standards.
>
> CPSR previously has questioned the role of NSA in developing the so-called "digital signature standard" (DSS), a communications authentication technology that NIST proposed for government-wide use in 1991. After CPSR sued NIST in a FOIA lawsuit last year, the civilian agency disclosed for the first time that NSA had, in fact, developed that

Copyright © 1995, 2005 M. E. Kabay. All rights reserved.

> security standard. NSA is due to file papers in federal court next week justifying the classification of records concerning its creation of the DSS.

David Sobel, CPSR Legal Counsel, called the administration's apparent commitment to the privacy of electronic communications, as reflected in today's official statement, "a step in the right direction." But he questioned the propriety of NSA's role in the process and the apparent secrecy that has thus far shielded the development process from public scrutiny. "At a time when we are moving towards the development of a new information infrastructure, it is vital that standards designed to protect personal privacy be established openly and with full public participation. It is not appropriate for NSA -- an agency with a long tradition of secrecy and opposition to effective civilian cryptography -- to play a leading role in the development process."

CPSR is a national public-interest alliance of computer industry professionals dedicated to examining the impact of technology on society. CPSR has 21 chapters in the U.S. and maintains offices in Palo Alto, California, Cambridge, Massachusetts and Washington, DC. For additional information on CPSR, call (415) 322-3778 or e-mail <cpsr@csli.stanford.edu>.

EFF Responds

The Electronic Frontier Foundation (EFF) was not slow to follow up:

> Message-Id: <1993Apr17.190632.210@ucsu.Colorado.EDU>
> References: <1993Apr17.032828.14262@clarinet.com> <tcmayC5M2xv,JEx@netcom.com>
> <1993Apr17.061326.16130@clarinet.com> Date: Fri, 16 Apr 1993 20:42:07 GMT
> From: Danny Weitzner <djw"eff.org>
> Organization: Electronic Frontier Foundation
> Sender: usenet@eff.org (NNTP News Poster)
> Subject: Re-inventing Crypto Policy? An EFF Statement
> Newsgroups: sci.crypt
> Lines: 122
>
> April 16, 1993
>
> INITIAL EFF ANALYSIS OF CLINTON PRIVACY AND SECURITY PROPOSAL
> The Clinton Administration today made a major announcement on cryptography policy which will effect the privacy and security of millions of Americans. The first part of the plan is to begin a comprehensive inquiry into major communications privacy issues such as export controls which have effectively denied most people easy access to robust encryption, and law enforcement issues posed by new technology.
>
> However, EFF is very concerned that the Administration has already reached a conclusion on one critical part of the inquiry, before any public comment or discussion has been allowed. Apparently, the Administration is going to use its leverage to get all telephone equipment vendors to adopt a voice encryption standard developed by the National Security Agency. The so-called "Clipper Chip" is an 80-bit, split key escrowed encryption scheme which will be built into chips manufactured by a military contractor. Two separate escrow agents would store users' keys, and be required to turn them over law enforcement upon presentation of a valid warrant. The encryption scheme used is to be classified, but the chips will be available to any manufacturer for incorporation into its communications products.
>
> This proposal raises a number of serious concerns .

Copyright © 1995, 2005 M. E. Kabay. All rights reserved.

First, the Administration has adopted a solution before conducting an inquiry. The NSA-developed Clipper Chip may not be the most secure product. Other vendors or developers may have better schemes. Furthermore, we should not rely on the government as the sole source for the Clipper or any other chips. Rather, independent chip manufacturers should be able to produce chipsets based on open standards.

Second, an algorithm cannot be trusted unless it can be tested. Yet, the Administration proposes to keep the chip algorithm classified. EFF believes that any standard adopted ought to be public and open. The public will only have confidence in the security of a standard that is open to independent, expert scrutiny.

Third, while the use of the use of a split-key, dual escrowed system may prove to be a reasonable balance between privacy and law enforcement needs, the details of this scheme must be explored publicly before it is adopted. What will give people confidence in the safety of their keys? Does disclosure of keys to a third party waive an individual's Fifth Amendment rights in subsequent criminal inquiries? These are but a few of the many questions the Administrations proposal raised but fails to answer.

In sum, the Administration has shown great sensitivity to the importance of these issues by planning a comprehensive inquiry into digital privacy and security. However, the "Clipper Chip" solution ought to be considered as part of the inquiry, and not be adopted before the discussion even begins.

DETAILS OF THE PROPOSAL:

ESCROW

The 80-bit key will be divided between two escrow agents, each of whom hold 40-bits of each key. The manufacturer of the communications device would be required to register all keys with the two independent escrow agents. A key is tied to the device, however, not the person using it. Upon presentation of a valid court order, the two escrow agents would have to turn the key parts over to law enforcement agents. According to the Presidential Directive just issued, the Attorney General will be asked to identify appropriate escrow agents. Some in the Administration have suggested that one non-law enforcement federal agency (perhaps the Federal Reserve), and one non-governmental organization could be chosen, but there is no agreement on the identity of the agents yet.

CLASSIFIED ALGORITHM AND THE POSSIBILITY OF BACK DOORS

The Administration claims that there are no back doors -- means by which the government or others could break the code without securing keys from the escrow agents -- and that the President will be told there are no back doors to this classified algorithm. In order to prove this, Administration sources are interested in arranging for an all-star crypto cracker team to come in, under a security arrangement, and examine the algorithm for trap doors. The results of the investigation would then be made public.

The Clipper Chipset was designed and is being produced and a sole-source, secret contract between the National Security Agency and two private firms: VLSI and Mycotronx. NSA work on this plan has been underway for about four years. The manufacturing contract was let 14 months ago.

GOVERNMENT AS MARKET DRIVER

Copyright © 1995, 2005 M. E. Kabay. All rights reserved.

In order to get a market moving, and to show that the government believes in the security of this system, the feds will be the first big customers for this product. Users will include the FBI, Secret Service, VP Al Gore, and maybe even the President. At today's Commerce Department press briefing, a number of people asked this question, though: why would any private organization or individual adopt a classified standard that had no independent guaranty of security or freedom from trap doors?

COMPREHENSIVE POLICY INQUIRY

The Administration has also announced that it is about to commence an inquiry into all policy issues related to privacy protection, encryption, and law enforcement. The items to be considered include: export controls on encryption technology and the FBI's Digital Telephony Proposal. It appears that the this inquiry will be conducted by the National Security Council. Unfortunately, however, the Presidential Directive describing the inquiry is classified. Some public involvement in the process has been promised, but they terms have yet to be specified.

FOR MORE INFORMATION CONTACT:

Jerry Berman, Executive Director (jberman@eff.org)
Daniel J. Weitzner, Senior Staff Counsel (djw@eff.org)

Full text of the Press releases and Fact Sheets issued by the Administration will be available on EFF's ftp site.

Danny Weitzner Senior Staff Counsel, EFF +1 202 544 3077

Dorothy Denning Steps Into the Fray

The highly-respected cryptographer Dorothy Denning caused a furor by being one of the few defenders of the Clipper Chip proposal. She was on the panel of cryptographers invited to review the proposal. Her summary of the situation was succinct:

> Date: 21 Apr 93 19:26:15 -0400
> From: denning@guvax.acc.georgetown.edu
> Organization: Georgetown University
> Subject: REVISED TECHNICAL SUMMARY OF CLIPPER CHIP
> Newsgroups: sci.crypt
> Distribution: world
> Lines: 167
>
> Here is a revised version of my summary which corrects some errors and provides some additional information and explanation.
>
> THE CLIPPER CHIP: A TECHNICAL SUMMARY
> Dorothy Denning
>
> Revised, April 21, 1993
>
> INTRODUCTION

Copyright © 1995, 2005 M. E. Kabay. All rights reserved.

On April 16, the President announced a new initiative that will bring together the Federal Government and industry in a voluntary program to provide secure communications while meeting the legitimate needs of law enforcement. At the heart of the plan is a new tamper-proof encryption chip called the "Clipper Chip" together with a split-key approach to escrowing keys. Two escrow agencies are used, and the key parts from both are needed to reconstruct a key.

CHIP CONTENTS

The Clipper Chip contains a classified single-key 64-bit block encryption algorithm called "Skipjack." The algorithm uses 80 bit keys (compared with 56 for the DES) and has 32 rounds of scrambling (compared with 16 for the DES). It supports all 4 DES modes of operation. The algorithm takes 32 clock ticks, and in Electronic Codebook (ECB) mode runs at 12 Mbits per second.

Each chip includes the following components:

- the Skipjack encryption algorithm
- F, an 80-bit family key that is common to all chips
- N, a 30-bit serial number (this length is subject to change)
- U, an 80-bit secret key that unlocks all messages encrypted with the chip.

The chips are programmed by Mykotronx, Inc., which calls them the "MYK-78." The silicon is supplied by VLSI Technology Inc. They are implemented in 1 micron technology and will initially sell for about $30 each in quantities of 10,000 or more. The price should drop as the technology is shrunk to .8 micron.

ENCRYPTING WITH THE CHIP

To see how the chip is used, imagine that it is embedded in the AT&T telephone security device (as it will be). Suppose I call someone and we both have such a device. After pushing a button to start a secure conversation, my security device will negotiate an 80-bit session key K with the device at the other end. This key negotiation takes place without the Clipper Chip. In general, any method of key exchange can be used such as the Diffie-Hellman public-key distribution method.

Once the session key K is established, the Clipper Chip is used to encrypt the conversation or message stream M (digitized voice). The telephone security device feeds K and M into the chip to produce two values:

E[M; K], the encrypted message stream, and
E[E[K; U] + N; F], a law enforcement field ,

which are transmitted over the telephone line. The law enforcement field thus contains the session key K encrypted under the unit key U concatenated with the serial number N, all encrypted under the family key F. The law enforcement field is decrypted by law enforcement after an authorized wiretap has been installed.

The ciphertext E[M; K] is decrypted by the receiver's device using the session key:

D[E[M; K]; K] = M .

Copyright © 1995, 2005 M. E. Kabay. All rights reserved.

CHIP PROGRAMMING AND ESCROW

All Clipper Chips are programmed inside a SCIF (Secure Compartmented Information Facility), which is essentially a vault. The SCIF contains a laptop computer and equipment to program the chips. About 300 chips are programmed during a single session. The SCIF is located at Mykotronx.

At the beginning of a session, a trusted agent from each of the two key escrow agencies enters the vault. Agent 1 enters a secret, random 80-bit value S1 into the laptop and agent 2 enters a secret, random 80-bit value S2. These random values serve as seeds to generate unit keys for a sequence of serial numbers. Thus, the unit keys are a function of 160 secret, random bits, where each agent knows only 80.

To generate the unit key for a serial number N, the 30-bit value N is first padded with a fixed 34-bit block to produce a 64-bit block N1. S1 and S2 are then used as keys to triple-encrypt N1, producing a 64-bit block R1:

R1 = E[D[E[N1; S1]; S2]; S1] .

Similarly, N is padded with two other 34-bit blocks to produce N2 and N3, and two additional 64-bit blocks R2 and R3 are computed:

R2 = E[D[E[N2; S1]; S2]; S1]
R3 = E[D[E[N3; S1]; S2]; S1] .

R1, R2, and R3 are then concatenated together, giving 192 bits. The first 80 bits are assigned to U1 and the second 80 bits to U2. The rest are discarded. The unit key U is the XOR of U1 and U2. U1 and U2 are the key parts that are separately escrowed with the two escrow agencies.

As a sequence of values for U1, U2, and U are generated, they are written onto three separate floppy disks. The first disk contains a file for each serial number that contains the corresponding key part U1. The second disk is similar but contains the U2 values. The third disk contains the unit keys U. Agent 1 takes the first disk and agent 2 takes the second disk. Thus each agent walks away knowing an 80-bit seed and the 80-bit key parts. However, the agent does not know the other 80 bits used to generate the keys or the other 80-bit key parts.

The third disk is used to program the chips. After the chips are programmed, all information is discarded from the vault and the agents leave. The laptop may be destroyed for additional assurance that no information is left behind.

The protocol may be changed slightly so that four people are in the room instead of two. The first two would provide the seeds S1 and S2, and the second two (the escrow agents) would take the disks back to the escrow agencies.

The escrow agencies have as yet to be determined, but they will not be the NSA, CIA, FBI, or any other law enforcement agency. One or both may be independent from the government.

Copyright © 1995, 2005 M. E. Kabay. All rights reserved.

LAW ENFORCEMENT USE

When law enforcement has been authorized to tap an encrypted line, they will first take the warrant to the service provider in order to get access to the communications line. Let us assume that the tap is in place and that they have determined that the line is encrypted with the Clipper Chip. The law enforcement field is first decrypted with the family key F, giving E[K; U] + N. Documentation certifying that a tap has been authorized for the party associated with serial number N is then sent (e.g., via secure FAX) to each of the key escrow agents, who return (e.g., also via secure FAX) U1 and U2. U1 and U2 are XORed together to produce the unit key U, and E[K; U] is decrypted to get the session key K. Finally the message stream is decrypted. All this will be accomplished through a special black box decoder.

CAPSTONE: THE NEXT GENERATION

A successor to the Clipper Chip, called "Capstone" by the government and "MYK-80" by Mykotronx, has already been developed. It will include the Skipjack algorithm, the Digital Signature Standard (DSS), the Secure Hash Algorithm (SHA), a method of key exchange, a fast exponentiator, and a randomizer. A prototoype will be available for testing on April 22, and the chips are expected to be ready for delivery in June or July.

ACKNOWLEDGMENT AND DISTRIBUTION NOTICE. This article is based on information provided by NSA, NIST, FBI, and Mykotronx. Permission to distribute this document is granted.

A Parable

In the subsequent vigorous debate about the politics of encryption, Perry Metzger published a striking parable which, as it were, shed light on the situation (reprinted with permission):

> Message-Id: <C5v08w.EwK@lvsun.com>
> References: <1993Apr20.203756.20667@kronos.arc.nasa.gov>
> <rlglendeC5t133.En3@netcom.com> Date: Fri, 23 Apr 1993 22:28:49 GMT
> From: pmetzger@snark.shearson.com (Perry E. Metzger)
> Organization: Partnership for an America Free Drug
> Sender: news@lehman.com (News)
> Subject: A Parable.
> Newsgroups: alt.privacy.clipper,sci.crypt
> Distribution: usa
> Xref: wrldlnk alt.privacy.clipper:154 sci.crypt:13138
>
> scottmi@microsoft.com (Scott Miller (TechCom)) writes:
> >Strikes me that all this concern over the government's ability >to eavesdrop is a little overblown... what can't they do today? >My understanding is that they already can tap, listen, get access >exc. to our phone lines, bank records, etc. etc again.
>
> Well, they can't listen in on much of mine, since I already use cryptography for much of my electronic mail, and will start using it for my telephony as soon as practical.
>
> However, allow me to tell a parable.
>
> There was once a far away land called Ruritania, and in Ruritania there was a strange phenonmenon -- all the trees that grew in Ruritainia were transparent. Now, in the days

Copyright © 1995, 2005 M. E. Kabay. All rights reserved.

when people had lived in mud huts, this had not been a problem, but now high-tech wood technology had been developed, and in the new age of wood, everyone in Ruritania found that their homes were all 100% see through. Now, until this point, no one ever thought of allowing the police to spy on someone's home, but the new technology made this tempting. This being a civilized country, however, warrants were required to use binoculars and watch someone in their home. The police, taking advantage of this, would get warrants to use binoculars and peer in to see what was going on. Occasionally, they would use binoculars without a warrant, but everyone pretended that this didn't happen.

One day, a smart man invented paint -- and if you painted your house, suddenly the police couldn't watch all your actions at will. Things would go back to the way they were in the old age -- completely private.

Indignant, the state decided to try to require that all homes have video cameras installed in every nook and cranny. "After all", they said, "with this new development crime could run rampant. Installing video cameras doesn't mean that the police get any new capability -- they are just keeping the old one."

A wise man pointed out that citizens were not obligated to make the lives of the police easy, that the police had survived all through the mud hut age without being able to watch the citizens at will, and that Ruritania was a civilized country where not everything that was expedient was permitted. For instance, in a neighboring country, it had been discovered that torture was an extremely effective way to solve crimes. Ruritania had banned this practice in spite of its expedience. Indeed, "why have warrants at all", he asked, "if we are interested only in expedience?"

A famous paint technologist, Dorothy Quisling, intervened however. She noted that people might take photographs of children masturbating should the new paint technology be widely deployed without safeguards, and the law was passed.

Soon it was discovered that some citizens would cover their mouths while speaking to each other, thus preventing the police from reading their lips through the video cameras. This had to be prevented, the police said. After all, it was preventing them from conducting their lawful surveillance. The wise man pointed out that the police had never before been allowed to listen in on people's homes, but Dorothy Quisling pointed out that people might use this new invention of covering their mouths with veils to discuss the kidnapping and mutilation of children. No one in the legislature wanted to be accused of being in favor of mutilating children, but then again, no one wanted to interfere in people's rights to wear what they liked, so a compromise was reached whereby all homes were installed with microphones in each room to accompany the video cameras. The wise man lamented few if any child mutilations had ever been solved by the old lip reading technology, but it was too late -- the microphones were installed everywhere.

However, it was discovered that this was insufficient to prevent citizens from hiding information from the authorities, because some of them would cleverly speak in languages that the police could not understand. A new law was proposed to force all citizens to speak at all times only in Ruritanian, and, for good measure, to require that they speak clearly and distinctly near the microphones. "After all", Dorothy Quisling pointed out, "they might be using the opportunity to speak in private to mask terrorist activities!" Terrorism struck terror into everyone's hearts, and they rejoiced at the brilliance of this new law.

Copyright © 1995, 2005 M. E. Kabay. All rights reserved.

Meanwhile, the wise man talked one evening to his friends on how all of this was making a sham of the constitution of Ruritania, of which all Ruritanians were proud. "Why", he asked, "are we obligated to sacrifice all our freedom and privacy to make the lives of the police easier? There isn't any real evidence that this makes any big dent in crime anyway! All it does is make our privacy forfeit to the state!"

However, the wise man made the mistake of saying this, as the law required, in Ruritanian, clearly and distinctly, and near a microphone. Soon, the newly formed Ruritanian Secret Police arrived and took him off, and got him to confess by torturing him. Torture was, after all, far more efficient than the old methods, and had been recently instituted to stop the recent wave of people thinking obscene thoughts about tomatoes, which Dorothy Quisling noted was one of the major problems of the new age of plenty and joy.

--
Perry Metzger pmetzger@shearson.com [now perry@piermont.com]
--
Laissez faire, laissez passer. Le monde va de lui meme.

Whitfield Diffie to Congress

Famed cryptographer Whitfield Diffie, one of the inventors of public key cryptography, published the following document on his testimony at Congressional hearings about the Key Escrow Proposal:

Message-Id: <16750@rand.org>
Date: 15 May 1993 18:06:59 GMT
From: diffie@ushabti.Eng.Sun.COM (Whitfield Diffie)
Organization: Sun Microsystems Inc., Mountain View, CA
Subject: Clipper Chip Testimony
Newsgroups: sci.crypt
Keywords: clipper, skipjack, wiretapping, privacy, standards Lines: 340

The Impact of a Secret Cryptographic Standard on Encryption, Privacy, Law Enforcement and Technology

Whitfield Diffie
Sun Microsystems
11 May 1993

I'd like to begin by expressing my thanks to Congressman Boucher, the other members of the committee, and the committee staff for giving us the opportunity to appear before the committee and express our views.

On Friday, the 16th of April, a sweeping new proposal for both the promotion and control of cryptography was made public on the front page of the New York Times and in press releases from the White House and other organizations.

This proposal was to adopt a new cryptographic system as a federal standard, but at the same time to keep the system's functioning secret. The standard would call for the use of a tamper resistant chip, called Clipper, and embody a `back door' that will allow the government to decrypt the traffic for law enforcement and national security purposes.

Copyright © 1995, 2005 M. E. Kabay. All rights reserved.

So far, available information about the chip is minimal and to some extent contradictory, but the essence appears to be this: When a Clipper chip prepares to encrypt a message, it generates a short preliminary signal rather candidly entitled the Law Enforcement Exploitation Field. Before another Clipper chip will decrypt the message, this signal must be fed into it. The Law Enforcement Exploitation Field or LEEF is tied to the key in use and the two must match for decryption to be successful. The LEEF in turn, when decrypted by a government held key that is unique to the chip, will reveal the key used to encrypt the message.

The effect is very much like that of the little keyhole in the back of the combination locks used on the lockers of school children. The children open the locks with the combinations, which is supposed to keep the other children out, but the teachers can always look in the lockers by using the key.

In the month that has elapsed since the announcement, we have studied the Clipper chip proposal as carefully as the available information permits. We conclude that such a proposal is at best premature and at worst will have a damaging effect on both business security and civil rights without making any improvement in law enforcement.

To give you some idea of the importance of the issues this raises, I'd like to suggest that you think about what are the most essential security mechanisms in your daily life and work. I believe you will realize that the most important things any of you ever do by way of security have nothing to do with guards, fences, badges, or safes. Far and away the most important element of your security is that you recognize your family, your friends, and your colleagues. Probably second to that is that you sign your signature, which provides the people to whom you give letters, checks, or documents, with a way of proving to third parties that you have said or promised something. Finally you engage in private conversations, saying things to your loved ones, your friends, or your staff that you do not wish to be overheard by anyone else.

These three mechanisms lean heavily on the physical: face to face contact between people or the exchange of written messages. At this moment in history, however, we are transferring our medium of social interaction from the physical to the electronic at a pace limited only by the development of our technology. Many of us spend half the day on the telephone talking to people we may visit in person at most a few times a year and the other half exchanging electronic mail with people we never meet in person.

Communication security has traditionally been seen as an arcane security technology of real concern only to the military and perhaps the banks and oil companies. Viewed in light of the observations above, however, it is revealed as nothing less than the transplantation of fundamental social mechanisms from the world of face to face meetings and pen and ink communication into a world of electronic mail, video conferences, electronic funds transfers, electronic data interchange, and, in the not too distant future, digital money and electronic voting.

No right of private conversation was enumerated in the constitution. I don't suppose it occurred to anyone at the time that it could be prevented. Now, however, we are on the verge of a world in which electronic communication is both so good and so inexpensive that intimate business and personal relationships will flourish between parties who can at most occasionally afford the luxury of traveling to visit each other. If we do not accept the right of these people to protect the privacy of their communication, we take a long step in the direction of a world in which privacy will belong only to the rich.

Copyright © 1995, 2005 M. E. Kabay. All rights reserved.

The import of this is clear: The decisions we make about communication security today will determine the kind of society we live in tomorrow.

The objective of the administration's proposal can be simply stated:

They want to provide a high level of security to their friends, while being sure that the equipment cannot be used to prevent them from spying on their enemies.

Within a command society like the military, a mechanism of this sort that allows soldiers' communications to be protected from the enemy, but not necessarily from the Inspector General, is an entirely natural objective. Its imposition on a free society, however, is quite another matter.

Let us begin by examining the monitoring requirement and ask both whether it is essential to future law enforcement and what measures would be required to make it work as planned.

Eavesdropping, as its name reminds us, is not a new phenomenon. But in spite of the fact that police and spies have been doing it for a long time, it has acquired a whole new dimension since the invention of the telegraph. Prior to electronic communication, it was a hit or miss affair. Postal services as we know them today are a fairly new phenomenon and messages were carried by a variety of couriers, travelers, and merchants. Sensitive messages in particular, did not necessarily go by standardized channels. Paul Revere, who is generally remembered for only one short ride, was the American Revolution's courier, traveling routinely from Boston to Philadelphia with his saddle bags full of political broadsides. Even when a letter was intercepted, opened, and read, there was no guarantee, despite some people's great skill with flaps and seals, that the victim would not notice the intrusion.

The development of the telephone, telegraph, and radio have given the spies a systematic way of intercepting messages. The telephone provides a means of communication so effective and convenient that even people who are aware of the danger routinely put aside their caution and use it to convey sensitive information. Digital switching has helped eavesdroppers immensely in automating their activities and made it possible for them to do their listening a long way from the target with negligible chance of detection.
Police work was not born with the invention of wiretapping and at present the significance of wiretaps as an investigative tool is quite limited. Even if their phone calls were perfectly secure, criminals would still be vulnerable to bugs in their offices, body wires on agents, betrayal by co-conspirators who saw a brighter future in cooperating with the police, and ordinary forensic inquiry.

Moreover, cryptography, even without intentional back doors, will no more guarantee that a criminal's communications are secure than the Enigma guaranteed that German communications were secure in World War II. Traditionally, the richest source of success in communications intelligence is the ubiquity of busts: failures to use the equipment correctly.

Even if the best cryptographic equipment we know how to build is available to them, criminal communications will only be secure to the degree that the criminals energetically pursue that goal. The question thus becomes, ``If criminals energetically pursue secure communications, will a government standard with a built in inspection port, stop them.

Copyright © 1995, 2005 M. E. Kabay. All rights reserved.

It goes without saying that unless unapproved cryptography is outlawed, and probably even if it is, users bent on not having their communications read by the state will implement their own encryption. If this requires them to forgo a broad variety of approved products, it will be an expensive route taken only by the dedicated, but this sacrifice does not appear to be necessary.

The law enforcement function of the Clipper system, as it has been described, is not difficult to bypass. Users who have faith in the secret Skipjack algorithm and merely want to protect themselves from compromise via the Law Enforcement Exploitation Field, need only encrypt that one item at the start of transmission. In many systems, this would require very small changes to supporting programs already present. This makes it likely that if Clipper chips become as freely available as has been suggested, many products will employ them in ways that defeat a major objective of the plan.

What then is the alternative? In order to guarantee that the government can always read Clipper traffic when it feels the need, the construction of equipment will have to be carefully controlled to prevent non-conforming implementations. A major incentive that has been cited for industry to implement products using the new standard is that these will be required for communication with the government. If this strategy is successful, it is a club that few manufacturers will be able to resist. The program therefore threatens to bring communications manufacturers under an all encompassing regulatory regime.

It is noteworthy that such a regime already exists to govern the manufacture of equipment designed to protect 'unclassified but sensitive' government information, the application for which Clipper is to be mandated. The program, called the Type II Commercial COMSEC Endorsement Program, requires facility clearances, memoranda of agreement with NSA, and access to secret `Functional Security Requirements Specifications.' Under this program member companies submit designs to NSA and refine them in an iterative process before they are approved for manufacture.

The rationale for this onerous procedure has always been, and with much justification, that even though these manufacturers build equipment around approved tamper resistant modules analogous to the Clipper chip, the equipment must be carefully vetted to assure that it provides adequate security. One requirement that would likely be imposed on conforming Clipper applications is that they offer no alternative or additional encryption mechanisms.

Beyond the damaging effects that such regulation would have on innovation in the communications and computer industries, we must also consider the fact that the public cryptographic community has been the principal source of innovation in cryptography. Despite NSA's undocumented claim to have discovered public key cryptography, evidence suggests that, although they may have been aware of the mathematics, they entirely failed to understand the significance. The fact that public key is now widely used in government as well as commercial cryptographic equipment is a consequence of the public community being there to show the way.

Farsightedness continues to characterize public research in cryptography, with steady progress toward acceptable schemes for digital money, electronic voting, distributed contract negotiation, and other elements of the computer mediated infrastructure of the future.

Copyright © 1995, 2005 M. E. Kabay. All rights reserved.

Even in the absence of a draconian regulatory framework, the effect of a secret standard, available only in a tamper resistant chip, will be a profound increase in the prices of many computing devices. Cryptography is often embodied in microcode, mingled on chips with other functions, or implemented in dedicated, but standard, microprocessors at a tiny fraction of the tens of dollars per chip that Clipper is predicted to cost.

What will be the effect of giving one or a small number of companies a monopoly on tamper resistant parts? Will there come a time, as occurred with DES, when NSA wants the standard changed even though industry still finds it adequate for many applications? If that occurs will industry have any recourse but to do what it is told? And who will pay for the conversion?

One of the little noticed aspects of this proposal is the arrival of tamper resistant chips in the commercial arena. Is this tamper resistant part merely the precursor to many? Will the open competition to improve semiconductor computing that has characterized the past twenty-years give way to an era of trade secrecy? Is it perhaps tamper resistance technology rather than cryptography that should be regulated?

Recent years have seen a succession of technological developments that diminish the privacy available to the individual. Cameras watch us in the stores, x-ray machines search us at the airport, magnetometers look to see that we are not stealing from the merchants, and databases record our actions and transactions. Among the gems of this invasion is the British Rafter technology that enables observers to determine what station a radio or TV is receiving. Except for the continuing but ineffectual controversy surrounding databases, these technologies flourish without so much as talk of regulation.

Cryptography is perhaps alone in its promise to give us more privacy rather than less, but here we are told that we should forgo this technical benefit and accept a solution in which the government will retain the power to intercept our ever more valuable and intimate communications and will allow that power to be limited only by policy.
In discussion of the FBI's Digital Telephony Proposal --- which would have required communication providers, at great expense to themselves, to build eavesdropping into their switches --- it was continually emphasized that wiretaps were an exceptional investigative measure only authorized when other measures had failed. Absent was any sense that were the country to make the proposed quarter billion dollar inventment in intercept equipment, courts could hardly fail to accept the police argument that a wiretap would save the people thousands of dollars over other options. As Don Cotter, at one time director of Sandia National Laboratories, said in respect to military strategy: ``Hardware makes policy.''

Law, technology, and economics are three central elements of society that must all be kept in harmony if freedom is to be secure. An essential element of that freedom is the right to privacy, a right that cannot be expected to stand against unremitting technological attack. Where technology has the capacity to support individual rights, we must enlist that support rather than rejecting it on the grounds that rights can be abused by criminals. If we put the desires of the police ahead of the rights of the citizens often enough, we will shortly find that we are living in police state. We must instead assure that the rights recognized by law are supported rather than undermined by technology.

At NSA they believe in something they call `security in depth.' Their most valuable secret may lie encrypted on a tamper resistant chip, inside a safe, within a locked office, in a guarded building, surrounded by barbed wire, on a military base. I submit to you that the

Copyright © 1995, 2005 M. E. Kabay. All rights reserved.

most valuable secret in the world is the secret of democracy; that technology and policy should go hand in hand in guarding that secret; that it must be protected by security in depth.

Recommendations

There is a crying need for improved security in American communication and computing equipment and the Administration is largely correct when it blames the problem on a lack of standards. One essential standard that is missing is a more secure conventional algorithm to replace DES, an area of cryptography in which NSA's expertise is probably second to none.

I urge the committee to take what is good in the Administration's proposal and reject what is bad.

....

- The Skipjack algorithm and every other aspect of this proposal should be made public, not only to expose them to public scrutiny but to guarantee that once made available as standards they will not be prematurely withdrawn.

- Configuration control techniques pioneered by the public community can be used to verify that some pieces of equipment conform to government standards stricter than the commercial where that is appropriate.

- I likewise urge the committee to recognize that the right to private conversation must not be sacrificed as we move into a telecommunicated world and reject the Law Enforcement Exploitation Function and the draconian regulation that would necessarily come with it.

- I further urge the committee to press the Administration to accept the need for a sound international security technology appropriate to the increasingly international character of the world's economy.

Petition to the President

The CPSR continued its efforts to coordinate opposition to the Key Escrow Proposal. In January 1994 they published the following call to action:

Date: Mon, 31 Jan 1994 15:59:20 EST
From: Dave Banisar <banisar@washofc.cpsr.org>
Subject: Clipper Petition

Electronic Petition to Oppose Clipper
Please Distribute Widely

On January 24, many of the nation's leading experts in cryptography and computer security wrote President Clinton and asked him to withdraw the Clipper proposal.

The public response to the letter has been extremely favorable, including coverage in the New York Times and numerous computer and security trade magazines.

Copyright © 1995, 2005 M. E. Kabay. All rights reserved.

Many people have expressed interest in adding their names to the letter. In response to these requests, CPSR is organizing an Internet petition drive to oppose the Clipper proposal. We will deliver the signed petition to the White House, complete with the names of all the people who oppose Clipper.

To sign on to the letter, send a message to:

Clipper.petition@cpsr.org

with the message "I oppose Clipper" (no quotes)

You will receive a return message confirming your vote.

Please distribute this announcement so that others may also express their opposition to the Clipper proposal.

CPSR is a membership-based public interest organization. For membership information, please email cpsr@cpsr.org. For more information about Clipper, please consult the CPSR Internet Library - FTP/WAIS/Gopher CPSR.ORG /cpsr/privacy/crypto/clipper

==========

The President
The White House
Washington, DC 20500

Dear Mr. President:

We are writing to you regarding the "Clipper" escrowed encryption proposal now under consideration by the White House. We wish to express our concern about this plan and similar technical standards that may be proposed for the nation's communications infrastructure.

The current proposal was developed in secret by federal agencies primarily concerned about electronic surveillance, not privacy protection. Critical aspects of the plan remain classified and thus beyond public review.

The private sector and the public have expressed nearly unanimous opposition to Clipper. In the formal request for comments conducted by the Department of Commerce last year, less than a handful of respondents supported the plan. Several hundred opposed it.

If the plan goes forward, commercial firms that hope to develop new products will face extensive government obstacles. Cryptographers who wish to develop new privacy enhancing technologies will be discouraged. Citizens who anticipate that the progress of technology will enhance personal privacy will find their expectations unfulfilled.

Some have proposed that Clipper be adopted on a voluntary basis and suggest that other technical approaches will remain viable. The government, however, exerts enormous influence in the marketplace, and the likelihood that competing standards would survive is small. Few in the user community believe that the proposal would be truly voluntary.

The Clipper proposal should not be adopted. We believe that if this proposal and the associated standards go forward, even on a voluntary basis, privacy protection will be

Copyright © 1995, 2005 M. E. Kabay. All rights reserved.

diminished, innovation will be slowed, government accountability will be lessened, and the openness necessary to ensure the successful development of the nation's communications infrastructure will be be threatened.

We respectfully ask the White House to withdraw the Clipper proposal.

Concluding Comments about the Key Escrow Proposal

In summary, the U.S. government proposes that evil people can be prevented from hiding their communications from lawful surveillance using a voluntary scheme in which specially-equipped phones and other devices will have decryption keys available under warrant.

If key escrow is made optional, it poses no direct threat to anyone's civil liberties. Key escrow may even be useful in preventing the damage that can occur when employees genuinely forget the encryption keys they used for corporate or government data. Having a back-door key will surely be useful when disgruntled employees encrypt source files and then claim to have forgotten the keys.

However, voluntary key escrow arrangements cannot possibly stop anyone from simply using some other encryption technique. The obvious next step must be to ban all other forms of strong encryption and to prescribe criminal penalties for violations of such a ban. But such a ban would be unenforceable. Aside from constitutional and legal arguments which support the view that wholesale banning of all but government-approved encryption would be an unjustified interference in the privacy of innocent individuals wishing simply to exercise their right Ato be let alone@ (in the words of Justice Holmes, speaking of privacy), the ban simply wouldn=t stop people from communicating secretly with each other.

PGP announces its operations in a header on a signed or encrypted message; when non-key-escrow encryption is made illegal, it will be unwise to continue to use such software. But unfortunately for the proponents of making encryption illegal, it is difficult to show that a stream of binary data is genuinely encrypted data. Guerrilla cryptographers will have a number of simple techniques for hiding encrypted messages, including steganography (placing encrypted data in less-significant bits of plaintext files).

Are we going to see radio astronomers, for instance, arrested because their gigabytes of stellar data resemble ciphertext? Will every graphic file be scrutinized to see if it contains hidden data? And will communications in foreign languages automatically become suspect because they are not instantly readable plaintext?

Trying to ban non-escrowed encryption will give criminal hackers and anti-government extremists a boost in public image; their paranoid rantings will be less obviously crazy than they ought to be. I sincerely hope that the U.S. government will reject the bad advice it is receiving about encryption.

Copyright © 1995, 2005 M. E. Kabay. All rights reserved.

Codes as Munitions: The International Traffic in Arms Regulations

Cryptographic software and hardware are included in the same U.S. regulations controlling the export of strategically-significant weaponry and nuclear materials from the U.S. This is a subject that evokes saliva-spattering rage in some quarters even though very few people seem to have read the regulations they are arguing for or against. In this section, I present the significant portions of the International Traffic in Arms Regulations (ITAR) and then offer a biased and ill-tempered attack on the very *idea* of including encryption in such regulations.

The Current References to Cryptography in the ITAR

The relevant regulations are as follows:

FEDERAL REGISTER
VOL. 58, No. 139
Rules and Regulations
DEPARTMENT OF STATE
Bureau of Politico-Military Affairs
22 CFR Parts 120, 121, 122, 123, 124, 125, 126, 127, 128, and 130
[Public Notice 1832]
Amendments to the International Traffic in Arms Regulations
Part II
58 FR 39280

DATE: Thursday, July 22, 1993

ACTION: Final rule.

SUMMARY: This rule amends the regulations implementing section 38 of the Arms Export Control Act, which governs the import and export of defense articles and services. The rule clarifies existing regulations and reduces the regulatory burden on exporters of defense articles and services. Although this is a final rule public comment is welcome and will be taken into account to the extent possible.

EFFECTIVE DATE: This final rule is effective July 22, 1993.
....
SUBCHAPTER M-INTERNATIONAL TRAFFIC IN ARMS REGULATIONS
....
S 120.11 -- Public domain.

Public domain means information which is published and which is generally accessible or available to the public:

(1) Through sales at newsstands and bookstores;

(2) Through subscriptions which are available without restriction to any individual who desires to obtain or purchase the published information;

(3) Through second class mailing privileges granted by the U.S. Government;

Copyright © 1995, 2005 M. E. Kabay. All rights reserved.

(4) At libraries open to the public or from which the public can obtain documents;

(5) Through patents available at any patent office;

(6) Through unlimited distribution at a conference, meeting, seminar, trade show or exhibition, generally accessible to the public, in the United States;

(7) Through public release (i.e., unlimited distribution) in any form (e.g., not necessarily in published form) after approval by the cognizant U.S. government department or agency (see also S 125.4(b)(13) of this subchapter);

(8) Through fundamental research in science and engineering at accredited institutions of higher learning in the U.S. where the resulting information is ordinarily published and shared broadly in the scientific community. Fundamental research is defined to mean basic and applied research in science and engineering where the resulting information is ordinarily published and shared broadly within the scientific community, as distinguished from research the results of which are restricted for proprietary reasons or specific U.S. Government access and dissemination controls. University research will not be considered fundamental research if:

(i) The University or its researchers accept other restrictions on publication of scientific and technical information resulting from the project or activity, or

(ii) The research is funded by the U.S. Government and specific access and dissemination controls protecting information resulting from the research are applicable.

S 120.12 -- Office of Defense Trade Controls.

Office of Defense Trade Controls, Bureau of Politico-Military Affairs, Department of State, Washington, D.C. 20522-0602.
....
Enumeration of Articles

S 121.1 -- General. The United States munitions list.

(a) The following articles, services and related technical data are designated as defense articles and defense services pursuant to sections 38 and 47(7) of the Arms Export Control Act (22 U.S.C. 2778 and 2794(7)). Changes in designations will be published in the Federal Register. Information and clarifications on whether specific items are defense articles and services under this subchapter may appear periodically in the Defense Trade News published by the Center for Defense Trade.

(b) Significant military equipment: An asterisk precedes certain defense articles in the following list. The asterisk means that the article is deemed to be "significant military equipment" to the extent specified in S 120.19. The asterisk is placed as a convenience to help identify such articles.
....
Category XI-Military [and Space] Electronics
....
*(b) Electronic systems or equipment specifically designed, modified, or configured for intelligence, security, or military purposes for use in search, reconnaissance, collection, monitoring, direction-finding, display, analysis and production of information from the electromagnetic spectrum and electronic systems or equipment designed or modified to counteract electronic surveillance or monitoring. A system meeting this definition is controlled under this subchapter even in instances where any individual pieces of equipment constituting the system may be subject

Copyright © 1995, 2005 M. E. Kabay. All rights reserved.

to the controls of another U.S. Government agency. Such systems or equipment described above include, but are not limited to, those:

(1) Designed or modified to use cryptographic techniques to generate the spreading code for spread spectrum or hopping code for frequency agility. This does not include fixed code techniques for spread spectrum.

(2) Designed or modified using burst techniques (e.g., time compression techniques) for intelligence, security or military purposes.

(3) Designed or modified for the purpose of information security to suppress the compromising emanations of information-bearing signals. This covers TEMPEST suppression technology and equipment meeting or designed to meet government TEMPEST standards. This definition is not intended to include equipment designed to meet Federal Communications Commission (FCC) commercial electro-magnetic interference standards or equipment designed for health and safety.
....
Category XIII-Auxiliary Military Equipment
....
(b) Information Security Systems and equipment, cryptographic devices, software, and components specifically designed or modified therefor, including:

(1) Cryptographic (including key management) systems, equipment, assemblies, modules, integrated circuits, components or software with the capability of maintaining secrecy or confidentiality of information or information systems, except cryptographic equipment and software as follows:

(i) Restricted to decryption functions specifically designed to allow the execution of copy protected software, provided the decryption functions are not user-accessible.

(ii) Specially designed, developed or modified for use in machines for banking or money transactions, and restricted to use only in such transactions. Machines for banking or money transactions include automatic teller machines, self-service statement printers, point of sale terminals or equipment for the encryption of interbanking transactions.

(iii) Employing only analog techniques to provide the cryptographic processing that ensures information security in the following applications:

(A) Fixed (defined below) band scrambling not exceeding 8 bands and in which the transpositions change not more frequently than once every second;

(B) Fixed (defined below) band scrambling exceeding 8 bands and in which the transpositions change not more frequently than once every ten seconds;

(C) Fixed (defined below) frequency inversion and in which the transpositions change not more frequently than once every second;

(D) Facsimile equipment;

(E) Restricted audience broadcast equipment;

(F) Civil television equipment.

Copyright © 1995, 2005 M. E. Kabay. All rights reserved.

Note: Special Definition. For purposes of this subparagraph, fixed means that the coding or compression algorithm cannot accept externally supplied parameters (e.g., cryptographic or key variables) and cannot be modified by the user.

(iv) Personalized smart cards using cryptography restricted for use only in equipment or systems exempted from the controls of the USML.

(v) Limited to access control, such as automatic teller machines, self- service statement printers or point of sale terminals, which protects password or personal identification numbers (PIN) or similar data to prevent unauthorized access to facilities but does not allow for encryption of files or text, except as directly related to the password of PIN protection.

(vi) Limited to data authentication which calculates a Message Authentication Code (MAC) or similar result to ensure no alteration of text has taken place, or to authenticate users, but does not allow for encryption of data, text or other media other than that needed for the authentication.

(vii) Restricted to fixed data compression or coding techniques.

(viii) Limited to receiving for radio broadcast, pay television or similar restricted audience television of the consumer type, without digital encryption and where digital decryption is limited to the video, audio or management functions.

(ix) Software designed or modified to protect against malicious computer damage, (e.g., viruses).

Note: A procedure has been established to facilitate the expeditious transfer to the Commodity Control List of mass market software products with encryption that meet specified criteria regarding encryption for the privacy of data and the associated key management. Requests to transfer commodity jurisdiction of mass market software products designed to meet the specified criteria may be submitted in accordance with the commodity jurisdiction provisions of S 120.4. Questions regarding the specified criteria or the commodity jurisdiction process should be addressed to the Office of Defense Trade Controls. All mass market software products with cryptography that were previously granted transfers of commodity jurisdiction will remain under Department of Commerce control. Mass market software governed by this note is software that is generally available to the public by being sold from stock at retail selling points, without restriction, by means of over the counter transactions, mail order transactions, or telephone call transactions; and designed for installation by the user without further substantial support by the supplier.

(2) Cryptographic (including key management) systems, equipment, assemblies, modules, integrated circuits, components or software which have the capability of generating spreading or hopping codes for spread spectrum systems or equipment.

(3) Cryptanalytic systems, equipment, assemblies, modules, integrated circuits, components or software.

(4) Systems, equipment, assemblies, modules, integrated circuits, components or software providing certified or certifiable multi-level security or user isolation exceeding class B2 of the Trusted Computer System Evaluation Criteria (TCSEC) and software to certify such systems, equipment or software.

(5) Ancillary equipment specifically designed or modified for paragraphs (b) (1), (2), (3), (4) and (5) of this category;

Copyright © 1995, 2005 M. E. Kabay. All rights reserved.

....

S 126.5 -- Canadian exemptions.

(a) District Directors of Customs and postmasters shall permit the export or temporary import without a license of any unclassified defense article or any unclassified technical data to Canada for end-use in Canada by Canadian citizens or return to the United States, or from Canada for end-use in the United States or return to a Canadian citizen in Canada, with the exception of the articles or related technical data listed in paragraph (b) of this section.
....

Encryption in the ITAR: A Stupid Idea

In summary, it is illegal to export any cryptographic software or hardware outside the United States (except for final use in Canada) without explicit authorization from the Office of Defense Trade Controls, Bureau of Politico-Military Affairs, Department of State.

In the opinion of many observers, including myself, the inclusion of cryptography in the ITAR is a preposterous farce. In any major city on earth it is possible to obtain strong encryption software; the source code for implementations of strong encryption algorithms has been published in journals, books and on the Internet for years. Bruce Schneier's famous textbook on encryption, *Applied Cryptography,* includes a diskette in the U.S--but the foreign editions lack the diskette even though the same source code is written out in plain view in the pages of the book. Phil Zimmermann, as noted above in his own words, is under investigation by a grand jury for possible violations of the ITAR--even though the foreign versions of PGP were written by foreigners outside the U.S.

Trying to stop the spread of such knowledge by passing regulations is akin to insisting that the St Lawrence River cease flowing into the Atlantic Ocean.

The practical effects of the inclusion of cryptographic tools in the ITAR include

- providing advantages to non-U.S. manufacturers of cryptographic modules over their U.S. competitors in the global marketplace;

- delaying the development of international standards of strong cryptography for protection of information transmitted through the Internet;

- damaging respect for the law by promulgating unenforceable regulations.

Copyright © 1995, 2005 M. E. Kabay. All rights reserved.

Electronic Commerce

When people do business through e-mail and other forms of electronic communications, what are the rules that govern their contractual obligations to each other? And when organizations pay for goods and services electronically, how do they reduce the likelihood of fraud? What methods are currently available for paying electronically without compromising privacy?

This section reviews electronic contracts, electronic data interchange security, electronic money and electronic cash.

Electronic Contracts

Whenever people discuss doing business over the Internet or through other electronic channels of communication, the question of non-repudiation always seems to pop up. How will anyone be able to prove, goes the question, that an electronic commitment to buy or to sell is authentic? Couldn=t someone else have ordered those 10,000 widgets in the name of the innocent recipient (now being sued for non-payment)? Could the original order have been for 1,000 widgets--with a transmission error or deliberate data diddling responsible for the false ten-fold increase in quantity?

As we have seen above, the conventional assumption of cryptographic experts is that only non-repudiable cryptographic authentication can prevent such problems. Without message digests, secret and public keys, and the other paraphernalia of today's cryptography, it is supposedly impossible to avoid commercial chaos. Greedy, dishonest merchants will cheat and lie to extract a short-term gain by altering their customers= orders; greedy, dishonest customers will forge fraudulent quotes purporting to show that they should pay only half the invoice for goods received. All will perjure themselves in court without hesitation. The future of electronic commerce lies in strong cryptographic authentication.

Attorney Benjamin Wright, an expert on legal aspects of electronic commerce, assures his readers and students that all of these problems could very well occur when using electronic communications for commerce. But they can also occur in ordinary snail-mail paper document exchange. Wright summarizes the situation neatly in his paper, "The Verdict on Plaintext Signatures: They're Legal." The following portion, discusses the circumstances which lead to acceptance of documentation in a court of law:

> But wait! cry the advocates of cryptographic authentication. You can't prove that e-mail came from Joe Nightclub. Anyone could have sent it. The Artist herself could have fabricated it.
>
> True. You can write e-mail and make it appear to come from someone else. You can easily send e-mail from an address opened under a false name. But just as you can send fake e-mail, so you can send fake letters, telegrams, telexes, and faxes.

Nonetheless, regardless of the medium through which a business message is carried, the origin and genuineness of the message can usually be proven in court. Rarely are they proven from the signature that happens to be attached to the message (or document), despite what you may think from watching _Perry Mason_. Much more often, origin and genuineness are determined in court from all the facts and circumstances that surround the message -- the full relationship of the people involved.

Copyright © 1995, 2005 M. E. Kabay. All rights reserved.

We don't do business in vacuums. We do business based on relationships. When the Artist receives e-mail from Joe Nightclub, she wants to learn more before she parts with her precious discs. If she's never dealt with this customer before, she's going to check the guy out: call him on the phone, go meet him, ask for references, or ask for advance payment. Lest she be a fool, the Artist wants to collect evidence that this is a bona fide customer who is very likely to pay as promised.

All the mundane facts and circumstances she collects can be, through testimony and otherwise, used in court to lend credence to Joe's e-mail. Sure, there will be disputed evidence. And under no circumstances are the judge and jury guaranteed to believe that any given message is genuine. But that is just the way commercial law works. Proving things in law is much more sloppy than proving things in science.

Despite Attorney Wright's confidence in the process of law, many people will prefer staying out of courts altogether. Digital signatures will continue to be attractive because they allow us to detect crude attacks on data integrity and authenticity upon receipt of fraudulent messages. There are, however, alternatives to the public-key version of the future. For example, Wright has been working with Peripheral Vision Ltd, a company that has developed a biometric identification and authentication process for signing electronic documents. In his paper, "Alternatives for Signing Electronic Documents," Wright summarizes the potential and difficulties of public-key cryptography and of "Penop" biometric authentication.

In brief, says Wright, PKC suffers from several difficulties, among which are the following:

- Private keys are too hard for people to remember, so they have to be stored digitally, usually on hard disks or on smart cards. Since computers and smart cards can be stolen, they need to be protected by passwords. But passwords are unreliable, leading to problems with stolen private keys.

- A smart card can be compromised by deliberately losing it (and its password).

- Public-key encryption relies on key distribution and certification authorities to establish the credibility of public keys before they can be used to sign a document.

  There is an easier way, argues Wright. Penop depends on the availability of digitizing tablets and the ability to record the dynamics and structure of personal signatures. When a user signs their name on the tablet using a stylus, these data are captured by a signature capture service (SCS) running on their own computer and sent to a signature verification service (SVS) in a secure way. A person wishing to establish their signature in the SVS database sends several examples of the data stream from a local SCS to the SVS. Then when such a user signs an electronic document, the SCS captures information about the document itself, combines this message digest with the biometric data from the specific act of signature, and encrypts all this along with other information about the user who signed the document. This "biometric token" is then attached to the signed document.

  Later, if someone wants to check on the authenticity and integrity of the signed document, they can submit the biometric token (not the actual document) to the SVS, where an algorithm can compute the probability that the document was really signed by the person named in the signature. Even if the signer has not yet registered their signature in the SVS, it is possible to do so after having signed a document; for example, when a courier logs a signature on one of their hand-held clip-board computers, it is not necessary to validate that

Copyright © 1995, 2005 M. E. Kabay. All rights reserved.

signature at once. Validation could occur at any time once the signer has registered with the SVS.

This scheme requires widespread availability of digitizers, but it does obviate the problems with the PKC identified by Wright.

- There is nothing to remember or forget. Users just sign their names, just like on paper documents.
- The signature dynamics cannot be compromised.
- Signature of an electronic document can be performed without preparation, just like on paper documents.

Such biometric identification depends on the reliability of the statistical models for comparing examples of signatures and their dynamics against the database entries of authorized signatures. Well-known problems with biometric methods of identification and authentication include the effects of aging, changes in health, and the effects of therapeutic or recreational drugs. In addition, the details of secure transmission of biometric tokens will have to be worked out carefully to prevent classic attacks on cryptographic systems. For example, a "man-the-middle attack" would allow someone to intercept inbound and outbound data from the SVS and pervert the process. The proposed Penop system bears watching in the years ahead to see how it bears up in the real world.

Electronic Data Interchange

Electronic Data Interchange (EDI) is the exchange of business information for buying, shipping, delivering, receiving, billing for and paying for goods and services. The following sections are based in large part on the work of Robert V. Jacobson of International Security Technology Inc. Mr Jacobson, a long-time friend of the NCSA and Sysop of the NCSA Physical Security Forum on CompuServe (GO NCSAPH), wrote *Good Security Practices for Electronic Commerce and Electronic Data Interchange,* a report for the National Institute of Standards and Technology in 1993.

Definitions and Basic Concepts of EDI

In EDI, users enter data into the sender's application system and database. Software replaces paper documents by "transaction sets" which are transmitted to recipients by communications networks. Software on the recipient side translates specific transaction sets into input data for the recipient's applications and databases; data are automatically checked for inconsistencies or errors and anomalies are reported to human operators. The recipient then transmits an electronic acknowledgment of receipt to the sender.

EDI has been important since the 1960s, especially in the transport industry. Key organizations that can help readers understand and establish EDI include DISA (Data Interchange Standards Association; 703-548-7005 in Alexandria, VA) and the U.S. Professional Development Institute (301-445-4000). The industry newsletter, *EDI NEWS,* is available from Phillips Business Information, Inc. (391-340-2100 in Potomac, MD). The ANSI committee responsible for EDI standards is X12; its documentation is available from Global Engineering Documents (800-854-7179 or 714-474-3933 in Irvine, CA).

Copyright © 1995, 2005 M. E. Kabay. All rights reserved.

Pairwise connections are useful only for high-volume traffic between large trading partners; General Motors, for example, might justify having its own arrangements with major suppliers. However, to avoid having to maintain as many network parameters as trading partners, many organizations rely on Value-added Networks (VANs) for easy communications. VANs not only provide mailboxes that can be checked periodically, but they can also provide ancillary services such as automatic translation among various input and output formats. Some of the main VANs for EDI are

- CompuServe EDI Service
- REDINET (Control Data)
- EDI*EXPRESS (GEISCO)
- IBM Information Network
- EDI*NET (McDonnell Douglas Applied Communications Systems)
- ORDERNET (Sterling Software)
- ShipNet and Telenet EDI (Telenet)
- MEDIATEL (Bell Canada)
- FAS*PAC (CNCP/UNITEL).

Security Requirements

According to Jacobson, the security requirements for all EDI systems are as follows:

- content integrity
- sequence integrity
- content confidentiality
- sender authentication
- recipient authentication
- timely delivery
- exclusive delivery.

In Jacobson's words, "Much of EC [electronic commerce] security focuses on the need to find automated substitutes for the human oversight that characterizes traditional paper-based business transactions." Jacobson recommends four broad principles for ensuring such controls:

- Provide automated acknowledgment and time limits for spotting anomalies.
- Maintain audit trails and archival records of all transactions in accordance with legal and business practices for the specific industry in question.
- Define all transaction sets without ambiguity.
- Authenticate individual transactions.

Security Practices during Development

In addition, Jacobson writes, the following elements of EDI security need to be addressed during development of EDI software:

- positive message acknowledgment
- electronic document management
- audit trails
- contingency planning
- encryption of sensitive content
- unique transaction numbering
- identification of duplicate transactions

Copyright © 1995, 2005 M. E. Kabay. All rights reserved.

- intelligent error handling
- digital signatures for message authentication
- controlled message retention by the VAN involved in communications
- restricted access to transactions by VAN personnel.

Operational Security

Operational security for EDI involves

- prompt response to trouble and exceptions (e.g., a Help Desk with a roster of appropriate names and phone numbers; escalation procedures to apply for longer interruptions);
- contingency plan tests, including regular testing of specific types of outage;
- user authentication controls such as proper password or token maintenance;
- compliance audits to provide independent verification of all controls.

In summary, planning and implementing EDI requires attention to security concerns from the ground up. The consequences of error or malfeasance in such systems can be catastrophic for all parties concerned. In a recent development, RSA DSI (Stanford, CA) and Premenos (Concord, CA) signed agreements in 1994 to provide secure EDI using RS/6000 and AS/400 platforms over any desired communications network. Look for further developments in this rapidly-evolving area.

Electronic Payments

Electronic payments are now commonplace. Banks have been shuttling billions of dollars of transfers around the planet using electronic funds transfers (EFT) for years; users of credit cards and debit cards are in a real sense tapping into the speed and efficiency of such EFT; and governments and corporations have been engaged in electronic data interchange (EDI) on a staggering scale for the last thirty years. Banks have recognized the economies and profitability of electronic banking; as a result, most readers will have access to bill payment and bank transfers by phone--and some by computer.

Another advantage of electronic money is that one can pay for goods and services using non-secure communications channels. The least secure and most popular channel these days is the Internet. Anyone sending reusable information over the Internet is at risk of fraud; no one should ever send their credit card information through electronic mail without strong encryption. And even when credit card information is encrypted, it can easily be misused by the recipients. Nothing stops a crook from filing fraudulent charges to a victim's credit card; the fraud may not even show up until the next monthly billing. At that point, the owner of the credit card may be able to show that the charges are fraudulent; they will then not be liable for those charges--but everyone using that brand of credit card bears the cost in service and interest charges.

In November 1994, Microsoft and VISA International announced their collaboration in establishing a mechanism for secure payment via the Internet. The joint effort is based on RSA PKC and depends on software-based encryption. At the November 1994 COMDEX consumer electronics exposition in Las Vegas, Microsoft displayed its vision of the future: deep involvement in the everyday life of ordinary citizens. The Advanced Consumer Technology Group at Microsoft is working on such gizmos as a "wallet PC" that could interact directly with one's bank account (as well as storing family videos).

In September 1995, the two giants proposed an industry standard for on-line payments. Critics such as Netscape Communications, already active in developing their own payment mechanisms,

Copyright © 1995, 2005 M. E. Kabay. All rights reserved.

accused Microsoft and VISA of trying to create a monopoly by forcing everyone to obtain licenses for the software from the two partners.

Meanwhile, in Reston, VA, CyberCash Inc. already provides direct payment services for Internet users. CyberCash permits participants to pay for goods by instructing the payment service to pay for goods and services while protecting the participant's credit card or bank debit card information from the vendors. In a variation on this theme, rival service Net1 Inc. allows computer users to create the equivalent of an electronic check which Net1 clears for the vendor.

In Europe, Barclays Plc., Britain's biggest bank, announced in June 1995 that it was opening an electronic shopping mall ("Barclaysquare") where Internet users could buy things; no word yet on security measures to prevent fraud.

Electronic Cash

The excitement over electronic money (some call it "e-cash") arises from the new technology that allows true anonymous exchange of currency, free from concerns over misuse because of breaches of identification and authentication. Electronic money can be transferred from bank accounts to computers-on-a-card, called "smart cards." Transactions involving smart cards need not contribute to the data shadow that haunts users of credit- and debit-cards. Buy books at a bookstore with your credit card and there may be a semi-permanent electronic audit trail open to Big Brother's (or Big Marketeer's) examination; buy the same books with an electronic money-card and there is nothing to identify you in the records.

As commercial participation in the Internet has mushroomed in the mid 1990s, interest in an anonymous electronic mechanism of payment has grown apace. In July 1995, National Westminster Bank and Midland Bank of the U.K. announced their "Mondex" system of electronic cash. A plastic smart card is loaded with money through a special e-cash dispenser similar to the automated teller machines we have all become used to. Once loaded, the "electronic purse" or e-purse can be used to pay for things using a special reader supplied to vendors. The system is being tested in Swindon until the end of 1995 with another test scheduled for Hong Kong starting in January 1996. Canadian banks and the Shanghai Banking Corporation have also signed up for the project. Public, home and cellular phones have already been altered in Swindon to let Mondex users load up their e-purse by phone from their bank account. To prevent fraud, the e-purse must be unlocked using a personal identification number.

A similar system called iKP is under test by IBM in conjunction with Europay International SA of Waterloo, Belgium. Rollout is expected in 1997 in all the European banks served by Europay. The "Proton" e-purse is being tested by Banksys SA, also of Belgium; MasterCard, not to be left out, is testing smart card e-cash in Canberra Australia in 1996.

DigiCash, an Amsterdam, Netherlands firm run by David Chaum, is also in the funning and has actually been under test using play-money in an electronic casino being run over the Internet by Toronto businessman Warren Eugene. There are serious questions about whether using the Internet for gambling is legal, at least in the U.S., where federal laws prohibit the use of telecommunications ("wires") across state lines for placing bets. Possibly satellite links to offshore computers would be permitted; there will undoubtedly be much huffing an puffing in the courts and the news media by lawyers and public relations staff over this issue.

In a thoughtful article in the *Guardian* newspaper ("Defying pitfalls of a cashless society", *Guardian* 95.05.30 as quoted in the RISKS FORUM DIGEST), columnist Victor Keegan examined some of the implications of digital cash. The basic problem he identifies is summarized in his words,

Copyright © 1995, 2005 M. E. Kabay. All rights reserved.

> The place just waiting for such anonymous digital money (which would also be rather useful for kidnappers and launderers of drug money) is the Internet, the worldwide electronic cobweb of computer data bases....
>
> Should the Net be provided with its own currency, it would suddenly become not only a global market place, but a virtual economy as well. It could become the first economy without a government or even a central bank at the centre. But if there is no government, no one will pay taxes....

Such extra-governmental money could become quite independent of "real" money, continues Keegan. People could begin bartering services and expressing their value in terms of e-cash beyond the control of central banks and regulators. Evidently, banking authorities are alarmed by the prospects. Look for severe penalties to be imposed on users of such systems who fail to declare their income.

Finally, Benjamin Wright continues his sterling work in the area of electronic commerce with a good review of the legal issues for his second edition of *The Law of Electronic Commerce.* He describes in detail the First Bank of the Internet (FBOI) and First Virtual Holdings, both firms that are active in promoting electronic payment schemes. His "Emerging Topic No. 3" is entitled, "Electronic Cash and Digital Media of Exchange--An Outline of Issues" and explores legal issues surrounding this evolving technology. Topics Wright reviews include

- contract law and electronic money
- disclosure of risk
- disclosure of identity
- records and internal control
- security
- dispute resolution
- securities law
- the U.S. Electronic Funds Transfer Act
- whether electronic payments constitute negotiable instruments.

I am looking forward to reading Ben Wright's new edition and, based on his first edition and on the quality of his NCSA courses, recommend it highly to anyone interested in these issues.

Copyright © 1995, 2005 M. E. Kabay. All rights reserved.

Chapter Notes

1. General Reading on Cryptography

   Crypt Cabal, The* (1995). *Sci.crypt Frequently-Asked Questions.* *The Crypt Cabal includes at least the following contributors: Eric Bach, Steve Bellovin, Dan Bernstein, Nelson Bolyard, Carl Ellison, Jim Gillogly, Mike Gleason, Doug Gwyn, Luke O'Connor, Tony Patti, William Setzer. The sections of this FAQ are available via anonymous FTP to rtfm.mit.edu as /pub/usenet/news.answers/cryptography-faq/part[xx]. The Cryptography FAQ is posted to the newsgroups sci.crypt, talk.politics.crypto, sci.answers, and news.answers every 21 days.

   Pfleeger, C. P. (1989). *Security in Computing.* Prentice-Hall (Englewood Cliffs, NJ). ISBN 0-13-798943-1. xxi + 538. Index.

   Schneier, B. (1994). *Applied Cryptography: Protocols, Algorithms, and Source Code in C.* John Wiley & Sons (New York). ISBN 0-471-59756-2. xviii + 618. Index.

   Stallings, W. (1995). *Network and Internetwork Security: Principles and Practice.* Prentice Hall (Englewood Cliffs, NJ). ISBN 0-02-415483-0. xiii + 462. Index.

2. Historical perspective

   Hinsley, F. H. & A. Stripp (1993). *Code Breakers: The Inside Story of Bletchley Park.* Oxford University Press. xxi + 321. Index.

3. DES

   Adams, C. (1994). DES software products move market prices down. *Federal Computer Week* 8(19):8

   Adams, C. (1993). Data Encryption Standard software headed for widespread government use. *Federal Computer Week* 7(20):35

   Coppersmith, D. (1994). The data encryption standard (DES) and its strength against attacks. *IBM Journal of Research and Development* 38(3):243

   Garon, G. & R. Outerbridge (1992). The sufficiency of the data encryption standard for financial institutions. *Computer Security Journal* 8(1):37

   Khan, S. (1994). DES still sets the standard for heavy-duty desktop encryption. *PC Week* 11(20):141

   Messmer, E. (1993). Users, industry urge NIST to reaffirm status of DES: gov't. encryption algorithm up for 5-year review. *Network World* 10(2):93

   Messmer, E. (1992). NIST reviews DES under microscope; if gov't discontinues the standard, private sector users would have to reevaluate their security. *Network World* 9(39):25

Copyright © 1995, 2005 M. E. Kabay. All rights reserved.

Schwartz, K. D. (1992). Changes to encryption standard would expand fed users' options. *Government Computer News* 11(24):3

4. RSA PKC, the RSA129 challenge and the PKCS

Bass, B. (1994). Bellcore team breaks public key encryption code. Federal Computer Week 8(10):4

Fahn, P. (1995). Answers to Frequently-Asked Questions about Today's Cryptography. The RSA FAQ is available from the standard FAQ server rtfm.mit.edu via FTP in the directory /pub/usenet/news.answers/cryptography-faq/rsa/. This FAQ is posted every 21 days to the groups sci.crypt, talk.politics.crypto, alt.security.ripem, sci.answers, talk.answers, alt.answers, and news.answers.

5. PGP (technical)

Johnson, M. P. (1995). *Where to Get PGP.* FAQ file available from ftp://ftp.csn.net/mpj/getpgp.asc.

Licquia, J. (1995). *PGP Frequently Asked Questions with Answers.* Available on the World Wide Web at http://www.prairienet.org/~jalicqui/pgpfaq.txt or via FTP from ftp://ftp.prairienet.org/pub/providers/pgp/pgpfaq.? where "?" indicates the file type [clearsigned text (txt), gzipped version of clearsigned text (txt.gz), PGP-signed-and-compressed binary (pgp), or ASCII armored PGP-signed-and-compressed file (asc)]. Periodically reposted to alt.security.pgp, alt.answers, and news.answers.

Stallings, W. (1995). *Protect Your Privacy: A Guide for PGP Users.* Prentice Hall (Englewood Cliffs, NJ). ISBN 0-13-185596-4. xvi + 302. Index.

6. DSS and PKP

Adams, C. (1993). Digital Signature Standard clears final hurdle. *Federal Computer Week* 7(15):6

Fisher, S. (1994). Gov't approves digital-signature standard. *Communications Week* (507):4

Grimm, V. J. (1994). NIST approves DSS despite threat of a patent lawsuit. *Government Computer News* 13(11):1

Minahan, T. (1994). DSS users get boost from NIST; agency willing to assert in court that standard does not infringe on patents. *Government Computer News* 13(13):82

Musthaler, L. (1994). Fed approval of DSS creates data security dichotomy. *Network World* 11(30):44

Power, K. (1994). NIST vows no-fee digital signature; it's back to square 1 in search for EDI verification scheme. *Government Computer News* 13(4):1

Power, K. (1994). NIST returns to bargaining table over DSS. *Government Computer News* 13(2):58

Copyright © 1995, 2005 M. E. Kabay. All rights reserved.

Power, K. (1993). Board questions true cost of DSS standard. *Government Computer News* 12 (17):1

Power, K. (1993). With patent dispute finally over, feds can use digital signatures. *Government Computer News* 12(13):1

Temin, T. R. (1993). No bargain. *Government Computer News* 12(18):26

7. PEM

Wallich, P.(1993). Electronic envelopes? The uncertainty of keeping e-mail private. *Scientific American* 268(2):30 [This article also discusses PGP.]

8. Entrust

Olsen, F. (1995). Secure messaging products are opening new gateways. *Government Computer News* 14(15):56

Rodriquez, K. (1995). RSA conference spotlights secure electronic commerce. *InfoWorld* 17(3):47

Welch, N. (1995). Entrust 1.2 locks in data: security system spans platforms. *MacWEEK* 9(33):10

Wilson, T. (1994). Mgm't, security wares debut. *CommunicationsWeek* (498):4

9. Encryption, Key Escrow and Public Policy

Anonymous (1995). Secret plans: encryption. *The Economist* 335(7913):80

Elmer-Dewitt, P. (1994). Who should keep the keys? *Time* 143(11):90
Kelly, K.(1993). Cypherpunks, e-money and the technologies of disconnection. *Whole Earth Review* (79):40

Kleiner, K. (1994). Punks and privacy. *Mother Jones* 19(1):17

Ness, E. (1994). Big Brother at cyberspace: will your freedom and privacy be roadkill on the information superhighway? *The Progressive* 58(12):22

Sussman, V. (1995). Lost in Kafka territory. *U.S. News & World Report* 118(13):32

10. ITAR

Davis, L. E. (1993). *Amendments to the International Traffic in Arms Regulations, Part II, 58 FR 39280.* Rules and Regulations, Department of State, Bureau of Politico-Military

Copyright © 1995, 2005 M. E. Kabay. All rights reserved.

Affairs. 22 CFR Parts 120, 121, 122, 123, 124, 125, 126, 127, 128, and 130. [Public Notice 1832]. FEDERAL REGISTER 58(139). Information regarding this notice may be obtained from James Andrew Lewis, U.S. Department of State, Bureau of Politico-Military Affairs (202-647-4231), Mal Zerden or Allan Suchinsky, U.S. Department of State, Office of Defense Trade Controls (703-875-6644).

Kabay, M. E. (1993). ITAR sticks users with unfair encryption restrictions. Network World 10(45):42

11. EDI and Electronic Money

Adams, C. (1994). Security issues plague electronic commerce. (Electronic Commerce supplement) *Federal Computer Week* 8(22):S20

Anonymous (1995). Another day, another cyber currency. *Digital Media* 4(8):40

Anonymous (1994). TGV plans Multinet security addition. *Digital News & Review* 11(20):13

Dosdale, T. (1994). Security in EDIFACT systems. *Computer Communications* 17(7)532

Jacobson, R. V. (1993). *Good Security Practices for Electronic Commerce and Electronic Data Interchange.* Computer Systems Laboratory, National Institute of Standards and Technology, Gaithersburg, MD 20899. Contract #43NANB311675. Conducted by R.V. Jacobson, International Security Technology, Inc. E-mail: 102404.3650@compuserve.com

McKendrick, J. E. (1994). EDI alliance secures transmissions. *MIDRANGE Systems* 7(19):10

Nadile, L. (1994). Premenos to test secure EDI over Internet. *PC Week* 11(47):44

Power, K. (1994). Signature standard sorely needed, report says; NPR financial management team calls for more EDI and electronic fund transfers. *Government Computer News* 13(9):64

Power, K. (1993). OMB officials to agencies: you have green light for EDI. *Government Computer News* 12(19):8

Vaughan, J. (1994). Internet will shake EC, EDI status quo; Sterling rolls out TCP/IP support - Cals looks forward. *Software Magazine* 14(12):23

Wayner, P. (1994). EDI moves the data. *Byte* 19(10): 121

Wright, B. (1995). *The Law of Electronic Commerce, Second Edition.* Little, Brown and Company (Boston). ISBN to be determined. Due September 1995.

Copyright © 1995, 2005 M. E. Kabay. All rights reserved.

Developing and Implementing INFOSEC Policies

by M. E. Kabay, PhD, CISSP
Associate Professor, Computer Information Systems
Norwich University, Northfield, VT
mkabay@compuserve.com

Part 1. Social Psychology and INFOSEC: Psycho-Social Factors in the Implementation of Security Policy.

Security policies and procedures affect not only what people do but also how they see themselves, their colleagues and their world. Despite these psychosocial issues, security personnel pay little or no attention to what is known about social psychology. The established principles of human social behaviour have much to teach us in our attempts to improve corporate and institutional information security.

Information security specialists concur that security depends on people more than on technology. Another commonplace is that employees are a far greater threat to information security than outsiders.

It follows from these observations that improving security depends on changing beliefs, attitudes and behaviour, both of individuals and of groups. Social psychology can help us understand how best to work with human predilections and predispositions to achieve our goals of improving security:

- research on social cognition looks at how people form impressions about reality (knowing these principles, we can better teach our colleagues and clients about effective security);
- work on attitude formation and beliefs helps us present information effectively and so convince employees and others to cooperate in improving security;
- scientists studying persuasion and attitude change have learned how best to change people's minds about unpopular views such as those of the security community;
- studies of factors enhancing prosocial behavior provide insights on how to foster an environment where corporate information is willingly protected;
- knowledge of the phenomena underlying conformity, compliance and obedience can help us enhance security by encouraging compliance and by protecting staff against social pressure to breach security;
- group psychology research provides warnings about group pathology and hints for working better with groups in establishing and maintaining information security in the face of ingrained resistance.

The following discussion is based on well-established principles of social psychology. Any recent introductory college textbook in this field will provide references to the research that has led to the principles which are applied to security policy implementation. In this paper, references are to Lippa, R A (1990). *Introduction to Social Psychology*. Wadsworth (Belmont, CA). ISBN 0-534-11772-4.

This section of the paper was presented at the 16th National Computer Security Conference in Bethesda, MD., September 1993, where it received an *Outstanding Paper Award*.

Social Cognition

Schemas are self-consistent views of reality. They help us pay attention to what we expect to be important and to ignore irrelevant data. They also help us organize our behavior [Lippa, p. 141]. For example, our schema for relations at the office includes polite greetings, civil discussions, written communications, and businesslike clothes. The schema excludes obscene shrieks, abusive verbal attacks, spray-painted graffiti and colleagues dressed in swim suits. It is the schema that lets people tell what is inappropriate in a given situation.

Security policies and procedures conflict with most people's schema. Office workers' schema includes sharing office supplies ("Lend me your stapler, please?"), trusting your team members to share information ("Take a look at these figures, Sally"), and letting your papers stay openly visible when you have to leave your desk. Unfortunately, sharing user IDs, showing sensitive information to someone who lacks the appropriate clearance, and leaving work stations logged on without protection are gross breaches of a different schema. Normal politeness dictates that when a colleague approaches the door we have just opened, we hold the door open for them; when we see a visitor, we smile politely (who knows, it may be a customer). In contrast, access policies require that we refuse to let even a well-liked colleague piggy-back their way through an access-card system; security policies insist that unbadged strangers be challenged or reported to security personnel. Common sense tells us that when the Chief Executive Officer of the company wants something, we do it; yet we try to train computer room operators to forbid entry to anyone without documented authorization--including the CEO.

Schemas influence what we perceive [Lippa, p. 143]. For

Copyright © 2001 M. E. Kabay. *All rights reserved.*

example, an employee refuses to take vacations, works late every night, is never late, and is never sick. A model employee? Perhaps, from one point of view. From the security point of view, the employee's behaviour is suspect. There have been cases where such people have actually been embezzlers unable to leave their employment: even a day away might result in discovery. Saint or sinner? Our expectations determine what we see.

Schemas influence what we remember [Lippa, p. 145]. When information inconsistent with our preconceptions is mixed with details that fit our existing schemas, we selectively retain what fits and discard what conflicts. When we have been fed a diet of movies and television shows illustrating the premise that information is most at risk from brilliant hackers, why should we remember the truth--that carelessness and incompetence by authorized users of information systems cause far more harm than evil intentions and outsiders ever do.

Before attempting to implement policies and procedures, we should ensure that we build up a consistent view of information security among our colleagues. In light of the complexity of social cognition, our usual attempts to implement security policies and procedures seem pathetically inept. A couple of hours of lectures followed by a video, a yearly ritual of signing a security policy that seems to have been written by Martians--these are not methods that will improve security. These are merely lip service to the idea of security.

According to research on counter-intuitive information, people's judgement is influenced by the manner in which information is presented. For example, even information contrary to established schemas can be assimilated if people have enough time to integrate the new knowledge into their world-views [Lippa, p. 148]. It follows that security policies should be introduced over a long time, not rushed into place.

Preliminary information may influence people's responses to information presented later. For example, merely exposing experimental subjects to a list of words such as "reckless" or "adventurous" affects their judgement of risk-taking behaviour in a later test. It follows that when preparing to increase employee awareness of security issues, presenting case-studies is likely to have a beneficial effect on participants' readiness to examine security requirements.

Pre-existing schemas can be challenged by several counter-examples, each of which challenges a component of the schema [Lippa, p. 153]. For example, prejudice about an ethnic group is more likely to be changed by contact with several people, each of whom contradicts a different aspect of the prejudiced schema. It follows that security awareness programs should include many realistic examples of security requirements and breaches. Students in the NCSA's Information Systems Security Course have commented on the unrealistic scenario in a training video they are shown; a series of disastrous security breaches occur in the same company. Based on the findings of cognitive social psychologists, the film would be more effective for training if the incidents were dramatized as occurring in different companies.

Judgements are easily distorted by the tendency to rely on personal anecdotes, small samples, easily available information, and faulty interpretation of statistical information [Lippa, p. 155-163]. Basically, we humans are not rational processors of factual information. If security awareness programs rely strictly on presentation of factual information about risks and proposed policies and procedures, they will run up against our stubborn refusal to act logically. Security program implementation must engage more than the rational mind. We must appeal to our colleagues' imagination and emotion as well. We must inspire a commitment to security rather than merely describing it.

Perceptions of risks and benefits are profoundly influenced by the wording in which situations and options are presented [Lippa, p. 163]. For example, experimental subjects responded far more positively to reports of a drug with "50% success" than to the same drug described as having "50% failure." It follows that practitioners should choose their language carefully during security awareness campaigns. Instead of focusing on reducing failure rates (breaches of security), we should emphasize improvements of our success rate.

Beliefs and Attitudes

Psychologists distinguish between beliefs and attitudes. "A belief ... refers to cognitive information that need not have an emotional component...." An attitude refers to "an evaluation or emotional response...." [Lippa, p. 238]. Thus a person may believe that copying software without authorization is a felony while nonetheless having the attitude that it doesn't matter.

Beliefs can change when contradictory information is presented, but some research suggests that it can take up to a week before significant shifts are measurable. Other studies suggest that when people hold contradictory beliefs, providing an opportunity to articulate and evaluate those beliefs may lead to changes that reduce inconsistency. These findings imply that a new concern for corporate security must be created by exploring the current structure of beliefs among employees and managers. Questionnaires, focus groups, and interviews may not only help the security practitioner, they may actually help move the corporate culture in the right direction.
An attitude, in the classical definition, "is a learned evaluative response, directed at specific objects, which is relatively enduring and influences behaviour in a generally motivating way" [Lippa, p. 221]. The advertising industry spends over $50B yearly to influence public attitudes in the hope that these attitudes will lead to changes in spending habits--that is, in behaviour.

Research on classical conditioning suggests that attitudes can be learned even because of simple word association [Lippa, p. 232]. If we wish to move our colleagues towards a more negative view of computer criminals, it is important not to portray computer crime using positive images and words. Movies like "Sneakers" may do harm indirectly by associating pleasant, likeable people with techniques that are used for industrial espionage. When teaching security courses, we should avoid praising the criminals we describe in case studies.

Copyright © 2001 M. E. Kabay. *All rights reserved.*

One theory on how attitudes are learned suggests that rewards and punishments are important motivators. Studies show that even apparently minor encouragement can influence attitudes. A supervisor or instructor should praise any comments that are critical of computer crime or which support the established security policies. Employees who dismiss security concerns or flout the regulations should be challenged on their attitudes, not ignored.

Persuasion and Attitude Change

Persuasion--changing someone's attitudes--has been described in a terms of communications [Lippa, p. 258]. The four areas of research include

- communicator variables: who is trying to persuade?
- message variables: what is being presented?
- channel variables: by what means is the attempt taking place?
- audience variables: at whom is the persuasion aimed?

Attractiveness, credibility and social status have strong effects immediately after the speaker or writer has communicated with the target audience; however, over a period of weeks to a month, the effects decline until the predominant issue is message content. We can use this phenomenon by identifying the senior executives most likely to succeed in setting a positive tone for subsequent security training. We should look for respected, likeable people who understand the issues and sincerely believe in the policies they are advocating.

Fear can work to change attitudes only if judiciously applied. Excessive emphasis on the terrible results of poor security is likely to backfire, with participants in the awareness program rejecting the message altogether. Frightening consequences should be coupled immediately with effective and achievable security measures.

Some studies suggest that presenting a balanced argument helps convince those who initially disagree with a proposal. Presenting objections to a proposal and offering counter-arguments is more effective than one-sided diatribes. The Software Publishers' Association training video, *It's Just Not Worth the Risk,* uses this technique: it shows several members of a company arguing over copyright infringement and fairly presents the arguments of software thieves before demolishing them.

Modest repetition of a message can help generate a more positive response. Thus security awareness programs which include imaginative posters, mugs, special newsletters, audio and video tapes and lectures are more likely to build and sustain support for security than occasional intense sessions of indoctrination.

The channel through which we communicate has a strong effect on attitudes and on the importance of superficial attributes of the communicator. "Face-to-face persuasion often proves to have more impact than persuasion through the mass media.... [because they] are more salient, personal and attention-grabbing, and thus they often stimulate more thought and commitment to their persuasive messages" [Lippa, p. 264]. Security training should include more than tapes and books; a charismatic teacher or leader can help generate enthusiasm for--or at least reduce resistance to--better security.

Workers testing cognitive response theory [Lippa, p. 289] have studied many subtle aspects of persuasion. For example, experiments have shown that rhetorical questions (e.g., "Are we to accept invasions of our computer systems?") are effective when the arguments are solid but counter-productive when arguments are weak.

In comparing the central route to persuasion (i.e., consideration of facts and logical arguments) with the peripheral (i.e., influences from logically unrelated factors such as physical attractiveness of a speaker), researchers find that the central route "leads to more lasting attitudes and attitude changes...." [Lippa, p. 293].

As mentioned above, questionnaires and interviews may help cement a favourable change in attitude by leading to commitment. Once employees have publicly avowed support for better security, some will begin to change their perception of themselves. As a teacher of information security, I find that I now feel much more strongly about computer crime and security than I did before I created my courses. We should encourage specific employees to take on public responsibility for information security within their work group. This role should periodically be rotated among the employees to give everyone the experience of public commitment to improved security.

Prosocial Behavior

Studies of how and why people help other people have lessons for us as we work to encourage everyone in our organizations to do the right thing. Why do some people intervene to stop crimes? Why do others ignore crimes or watch passively? Latane and Darley (Lippa, p. 493) have devised a schema that describes the steps leading to prosocial behavior:

- People have to notice the emergency or the crime before they can act. Thus security training has to include information on how to tell that someone may be engaging in computer crime.
- The situation has to be defined as an emergency--something requiring action. Security training that provides facts about the effects of computer crime on society and solid information about the need for security within the organization can help employees recognize security violations as emergencies.
- We must take responsibility for acting. The bystander

Copyright © 2001 M. E. Kabay. *All rights reserved.*

effect comes into play at this stage. The larger the number of people in a group confronted with an emergency, the slower the average response time. Larger groups seem to lead "to a diffusion of responsibility whereby each person felt less personally responsible for dealing with the emergency" [Lippa, p. 497]. Another possible factor is uncertainty about the social climate; people fear "appearing foolish or overly emotional in the eyes of those present." We can address this component of the process by providing a corporate culture which rewards responsible behaviour such as reporting security violations.

- Having taken responsibility for solving a problem, we must decide on action. Clearly written security policies and procedures will make it more likely that employees act to improve security. In contrast, contradictory policies, poorly-documented procedures, and inconsistent support from management will interfere with the decision to act.

Another analysis proposes that people implicitly analyze costs of helping and of not helping when deciding whether to act prosocially. The combination of factors most conducive to prosociality is low cost for helping and high cost for not helping. Security procedures should make it easy to act in accordance with security policy; e.g., there should be a hot-line for reporting security violations, anonymity should be respected if desired, and psychological counselling and followup should be available if people feel upset about their involvement. Conversely, failing to act responsibly should be a serious matter; personnel policies should document clear and meaningful sanctions for failing to act when a security violation is observed; e.g., inclusion of critical remarks in employment reviews and even dismissal.

One method that does not work to increase prosocial behavior is exhortation [Lippa, p. 513]. That is, merely lecturing people has little or no effect. On the other hand, the general level of stress and pressure to focus on narrow tasks can significantly reduce the likelihood that people will act on their moral and ethical principles. Security is likely to flourish in an environment that provides sufficient time and support for employees to work professionally; offices where everyone responds to self-defined emergencies all the time will not likely pay attention to security violations.

Some findings from research confirm common sense. For example, guilt motivates people to act more prosocially. This effect works best "when people are forced to assume responsibility...." Thus enforcing standards of security using reprimands and sanctions can indeed increase the likelihood that employees will subsequently act more cooperatively. In addition, mood affects susceptibility to prosocial pressures: bad moods make prosocial behavior less likely, whereas good moods increase prosociality. A working environment in which employees are respected is more conducive to good security than one which devalues and abuses them. Even cursory acquaintance with other people makes it more likely that we will help them; it thus makes sense for security supervisors to get to know the staff from whom they need support. Encouraging social activities in an office (lunch groups, occasional parties, charitable projects) enhances interpersonal relationships and can improve the climate for effective security training.

Conformity, Compliance and Obedience

Turning a group into a community provides a framework in which social pressures can operate to improve our organization's information security. People respond to the opinions of others by (sometimes unconsciously) shifting their opinion towards the mode. Security programs must aim to shift the normative values (the sense of what one should do) towards confidentiality, integrity and availability of data. As we have seen in public campaigns aimed at reducing drunk driving, it is possible to shift the mode. Twenty years ago, many people believed that driving while intoxicated was amusing; today a drunk driver is a social pariah. We must move towards making computer crime as distasteful as public drunkenness.
The trend towards conformity increases when people within the group like or admire each other [Lippa, p. 534]. In addition, the social status of an individual within a group influences that individual's willingness to conform. High-status people (those liked by most people in the group) and low-status people (those disliked by the group) both tend to more autonomous and less compliant than people liked by some and disliked by others [Lippa, p. 536]. Therefore the security officers should pay special attention to those outliers during instruction programs. Managers should monitor compliance more closely in both ends of the popularity range. Contrariwise, if security practises are currently poor and we want allies in changing the norm, we should work with the outliers to resist the herd's anti-security bias.

"The norm of reciprocity holds that we should return favours in social relations" [Lippa, p. 546]. Even a small, unexpected or unsolicited (and even unwanted) present increases the likelihood that we will respond to requests. A security awareness program that includes small gifts such as a mug labelled "SECURITY IS EVERYONE'S BUSINESS" or an inexpensive booklet such as the *Information Systems Security Pocket Guide* (available from the NCSA) can help get people involved in security.

The "foot in the door" technique suggests that we "follow a small initial request with a much larger second request" [Lippa, p. 549]. For example, we can personally ask an employee to set a good example by blanking their screen and locking their terminal when they leave their desk. Later, once they have begun their process of redefinition of themselves ("I am a person who cares about computer security"), we can ask them for something more intense, such as participating in security training for others (e.g., asking each colleague to blank their screen and lock their terminal).

Group Behaviour

Early studies on the effects of being in groups produced

Copyright © 2001 M. E. Kabay. *All rights reserved.*

contradictory behaviour; sometimes people did better at their tasks when there were other people around and sometimes they did worse. Eventually, social psychologist Robert Zajonc [Lippa, p. 572 ff.] realized that "The presence of others is arousing, and this arousal facilitates dominant, well-learned habits but inhibits nondominant, poorly-learned habits." Thus when trying to teach employees new habits, it is counter-productive to put them into large groups. Individualized learning (e.g., computer-based training, video tapes) can overcome the inhibitory effect of groups in the early stages of behavioural change.

Another branch of research in group psychology deals with group polarization. Groups tend to take more extreme decisions than individuals in the group would have [Lippa, p. 584]. In group discussions of the need for security, polarization can involve deciding to take more risks--by reducing or ignoring security concerns--than any individual would have judged reasonable. Again, one-on-one discussions of the need for security may be a more effective approach to building a consensus that supports cost-effective security provisions than large meetings.

In the extreme, a group can display groupthink, in which a consensus is reached because of strong desires for social cohesion [Lippa, p. 586 ff.]. When groupthink prevails, evidence contrary to the received view is discounted; opposition is viewed as disloyal; dissenters are discredited. Especially worrisome for security professionals, people in the grip of groupthink tend to ignore risks and contingencies. To prevent such aberrations, the leader must remain impartial and encourage open debate. Experts from the outside (e.g., respected security consultants) should be invited to address the group, bringing their own experience to bear on the group's requirements. After a consensus has been achieved, the group should meet again and focus on playing devil's advocate to try to come up with additional challenges and alternatives.

Conclusions

By viewing information security as primarily a management issue, we can benefit from the mass of knowledge accumulated by social psychologists. We can implement security policies and procedures more easily by adapting our training and awareness techniques to correspond to human patterns of learning and compliance.

Summary of Recommendations

1. Before attempting to implement policies and procedures, we should ensure that we build up a consistent view of information security among our colleagues.

2. Security policies should be introduced over a long time, not rushed into place.

3. Presenting case-studies is likely to have a beneficial effect on participants' readiness to examine security requirements.

4. Security awareness programs should include many realistic examples of security requirements and breaches.

5. We must inspire a commitment to security rather than merely describing it.

6. Emphasize improvements rather than reduction of failure.

7. A new concern for corporate security must be created by exploring the current structure of beliefs among employees and managers.

8. Do not to portray computer crime using positive images and words.

9. Praise any comments that are critical of computer crime or which support the established security policies.

10. Employees who dismiss security concerns or flout the regulations should be challenged on their attitudes, not ignored.

11. Identify the senior executives most likely to succeed in setting a positive tone for subsequent security training.

12. Frightening consequences should be coupled immediately with effective and achievable security measures.

13. Presenting objections to a proposal and offering counter-arguments is more effective than one-sided diatribes.

14. Security awareness programs should include repeated novel reminders of security issues.

15. In addition to tapes and books, rely on a charismatic teacher or leader to help generate enthusiasm for better security.

16. Encourage specific employees to take on public responsibility for information security within their work group.

17. Rotate the security role periodically.

18. Security training should include information on how to tell that someone may be engaging in computer crime.

19. Build a corporate culture which rewards responsible

Copyright © 2001 M. E. Kabay. *All rights reserved.*

behaviour such as reporting security violations.

20. Develop clearly written security policies and procedures.

21. Security procedures should make it easy to act in accordance with security policy.

22. Failing to act in accordance with security policies and procedures should be a serious matter.

23. Enforcing standards of security can increase the likelihood that employees will subsequently act more cooperatively.

24. A working environment in which employees are respected is more conducive to good security than one which devalues and abuses them.

25. Security supervisors should get to know the staff from whom they need support.

26. Encourage social activities in the office.

27. Pay special attention to social outliers during instruction programs.

28. Monitor compliance more closely in both ends of the popularity range.

29. Work with the outliers to resist the herd's anti-security bias.

30. Include small gifts in your security awareness program.

31. Start improving security a little at a time and work up to more intrusive procedures.

32. Before discussing security at a meeting, have one-on-one discussions with the participants.

33. Remain impartial and encourage open debate in security meetings.

34. Bring in experts from the outside when faced with groupthink.

35. Meet again after a consensus has been built and play devil's advocate.

Part 2. Building a Security Policy

Information management today is based on the availability of data throughout the enterprise. Data communications makes up a growing part of the investment in information technology. It follows that network security is at the heart information systems security. Network managers therefore have to work closely with colleagues in framing and implementing information security policies. You contribution to the information security team is essential for success.

Your mission in devising network security policies is to ensure that network components support the basic principles of information security: to protect information from unauthorized or accidental modification, destruction and disclosure and to ensure timely availability and usability of those data.

The task is complicated by human and organizational resistance. Technology alone doesn't work. In changing human behavior, substance is not enough. Style makes the difference.

This section of the paper was originally published as the article "Securing a net security plan: Workable guidelines for devising network security policies." in *Network World* 10(15):44.

The Zen of Network Security?

Security is always described as being everyone's business. Actually, security *interferes* with everyone's business. As a network manager, you have worked hard to make your networks user-friendly. You've done everything you can to make life easier for users; you've provided network access routines with a graphical user interface, client-server systems with hot-links between local spreadsheets and corporate databases, and a gateway to the Internet for your engineering users.

So why is there anything different about securing your networks? Superficially, you might think that network security simply involves defining access controls, applying encryption, and providing people with hand-held password generators. What's so hard about that?

What's hard is that security policies offend deep-seated ways of seeing ourselves. We form close-knit work groups in which people *trust* each other. We don't lock our desks when we leave them for a few minutes; why should we obey the network security policy that dictates locking our keyboards? We lend people our car keys in an emergency; why should it be such a big deal if we lend them our access codes and passwords in an emergency?

Network users have to change the way they *think* about information. To implement security policies and procedures without focusing on attitudes and beliefs is to ensure non-compliance. If you impose security restrictions without convincing the users that they *need* to protect the networks, you will get lip-service and nothing more.

Every password written on a Post-It(TM) note under the keyboard is proof that security policies are meaningless unless users believe in them. At one training session on security, an executive commented, "I feel as if I've gotten religion!" He wasn't far off the truth.

Copyright © 2001 M. E. Kabay. *All rights reserved.*

Turf Wars

As you try to develop and implement your network security strategy, you will cross boundaries within your organization. If you try to *impos*e more stringent security procedures for network use, you will be perceived as making people's jobs harder-- and they don't even work for you. In many cases, you will be resisted with the comment, "Network security? That's *your* problem, not mine."

The only approach that works is to co-opt your colleagues. Convince your users that network security is in their own interest. Involve them in developing security policies. You depend on them to implement the procedures you work out collectively. Make sure that users recognize that they *own* their security procedures and you'll have partners instead of opponents.

Phase 1: Preliminary evaluation

Before you can do anything else, you have to know what needs to be protected. Nobody keeps firewood in the safe and securities in the garden shed. A preliminary inventory will help you convince upper management that the enterprise needs to develop a corporate information security policy that reflects the risks your needs. Within that policy, your preliminary analysis will alert management to areas that need immediate attention.

The preliminary evaluation should be quick and inexpensive. Think in terms of days of work by a few people. You don't want to waste your time in expensive detail work before you get approval and support from your upper management.

As a network manager, you have clear ideas about what your networks are designed for. You know how they ought to be used. However, your users are the best source of insight into the ways your networks are *really* used.

Work closely with your human resources (HR) staff in developing the research instruments: they know (or should know) the key managers you should contact in each department. You'll need to get the managers on your side to be able to interview their staff. Provide a White Paper to everyone in the organization that lays out your reasons for asking for their time and energy.

Some of the HR people are likely to have the professional skills and experience required to provide accurate and cost effective evaluations of beliefs, attitudes and behavior affecting security. They may be able to help you construct unbiased questionnaires, organize focus groups and help during interviews.

If you and your HR staff are not confident about this preliminary data collection, you should hire a consultant with proven expertise in collecting and analyzing social attitudes. Discuss such a study with a firm specializing in security audits and organizational analysis. If you don't know where to start looking, you can contact local universities and colleges and ask for the management studies group (school, faculty, department or institute).

The following key issues should be part of your preliminary study, as they will be in more detail in subsequent phases.

Sensitive Systems

What shouldn't be universal knowledge? Imagine that you have an enterprise-wide electronic mail system. No one has ever asked you to put any particularly tight security on email. You think of it as mostly administrative stuff. But suppose you talk with your sales department staff. You learn that they send detailed reports on their prospects to their manager through your email. The prospect reports would be worth a fortune to your competition.

Critical systems

What cannot be wrong without catastrophic effects? As part of your preliminary investigation, you chat with the users in your engineering department. They supply the new drawings required to respond to changes in major government contracts. They tell you the entire shop floor depends on these drawings.

Exposure

How bad could things get if sensitive data were disclosed or critical data were wrong or unavailable? For example, if a competitor were to see the prospect reports you discussed with the sales staff, they could underbid you and win your business. Suddenly a whole new security dimension opens up in your thinking about the security of email. Similarly, you ask the engineering staff what would happen if any of their drawings were to be modified or damaged during transmission over the unsecured LAN. They explain that if someone were to alter dimensions or tolerances in any way, an entire production run could be ruined. Costs could run in the millions of dollars and lead to punitive damages for failing to meet specifications. Too many errors and you could be out of business. Suddenly it's clear that the integrity of those bits flowing through your network is worth a lot of protection.

Physical Security

What measures are in place already to safeguard equipment and people? I once found a network server in the wardrobe down where visitors put their muddy boots. No, because last year, you built a new enclosure for your LAN servers and gateways. OK, did anyone tell the security guards to check that room now that it has half a million dollars worth of data communications gear in it?

Access control

Copyright © 2001 M. E. Kabay. *All rights reserved.*

How are you currently ensuring that material and data are available only to those people who have legitimate reasons to get at them? Think about the unauthorized disclosure of the information moving through your data channels. Where could a dishonest employee or consultant tap into your channels? Where could outsiders gain entry to your networks? When was the last time you changed your modem telephone numbers? How heavily are the modems used? What kinds of information get transferred? How confidential are those data? There was a case some years ago in which an oil exploration company kept losing a series of bids for drilling rights. This was an odd problem; they made a point of using the best available geological data and financial cost estimates when setting their bids. In fact, they were highly competitive because of their use of modern technology--their financial estimates were transmitted to head office by modem. Over time, the company grew suspicious of the small margins by which they kept losing. Investigators found the reason for the run of bad luck: the modem transmissions showing how much to bid for those rights had been intercepted by wire-tappers for the competition.

Management and employee security awareness

What do your colleagues believe about network security, how do they feel about the situation, and what do they actually do to protect corporate information? The best security apparatus on the planet can be defeated by uncooperative users. Knowing what they think (rightly and wrongly) will give you a heads-up warning on where your biggest challenges lie.

Throughout the preliminary evaluation, keep notes that will help you estimate the time required to put together an effective security policy and specific procedures. You need to know how many people will have to be interviewed once you get approval for the detail work. How many networks will you have to examine? How many network applications systems are there to analyze? Keep track of how long it's taking you to complete your initial interviews. Estimate how long it will take to interview everyone--then add a fudge factor for the unexpected (I habitually make my best guess and multiply by two, but you surely have your own experience to draw on). Keep a running tally of approximate costs for salary of your own staff during the preliminary analysis and use that tally to project the cost of a full-scale analysis.

Phase 2: Management Sensitization

Support from upper management is essential for further progress. Your goal in this phase is to get approval for an organization-wide audit and policy formulation project. In conjunction with the rest of the information security project team, plan on a meeting that lasts no more than one or two hours. Start the meeting with a short statement about the crucial role of information in your organization's business.

Use professional aids such as a management-oriented training video to sensitize the managers to the consequences of poor information security. After the video film, present your findings from the preliminary evaluation. Define an information security working group to set priorities, determine an action plan, define a timetable and milestones and formulate policies and procedures to protect corporate information resources. Name the people you want to see on your working group. In your part of the presentation, emphasize the value of protecting networks.

Provide estimates of the time involved and the costs of consulting services and software.

You can end the briefing by offering the managers background reading about security. Some of them may be intrigued by this field; they more they learn, the more they will support your security efforts.

Phase 3: Needs Analysis

The information security working group should include representatives from every sector of your organization. As you investigate your networks' security requirements, you need their experience and perspective to decide which areas to protect most strongly. More important, their involvement is a concrete expression of your concern for fundamental attitude change in the corporate culture. Henceforth, security will be an integral part of the corporate mission.

For example, in a manufacturing firm, you'd include managers and staff from the factory floor, the unions, engineering, equipment maintenance, shipping and receiving, facilities management (including those responsible for physical security), administrative support, sales, marketing, accounting, personnel, the legal department and information systems. Each of these members of the working group will help you improve your network security.

If your organization is very large, you may have to set up subcommittees to deal with specific sectors. Each subcommittee evaluates to what degree the systems and networks are vulnerable to breaches of security. For example, one group could focus on local and campus communications, another on wide-area enterprise networks, and a third on electronic data interchange with clients and suppliers.

A typical audit covers the facilities, personnel policies, existing security, application systems, and legal responsibility to stakeholders (owners, shareholders, employees, clients and the surrounding community). Based on the findings, the subcommittees formulate proposals for improving security. This is where the specialized knowledge obtained from information security specialists and information security courses will prove especially useful.

Risk analysis software is also available from several sources and ranging in price from $60 to $16,000 per license. These programs, in different degrees of detail and sophistication, ask users questions about their operations and estimate degrees of risk. The more advanced, and more expensive, programs use artificial intelligence (expert systems) to provide more precise probabilities of specific dangers.

Copyright © 2001 M. E. Kabay. *All rights reserved.*

The National Institute of Standards and Technology has published the *Guide for selecting automated risk analysis tools* (NIST Publication #500-174), available from NIST at nominal cost in Washington, DC.

Phase 4: Policies and Procedures

When you have built a solid floor of understanding of your information security needs, you're ready to construct the policies and procedures that meet your needs. Don't re-invent such policies from scratch; use existing policy frameworks as your scaffolding. Charles Cresson Wood, a respected authority in the security field, publishes his widely-acclaimed *Information Security Policies Made Easy* <http://www.baselinesoft.com/ >. This invaluable tool contains almost a thousand detailed policies in written and electronic form; they cover everything one needs in establishing detailed, current information security policies and procedures. According to Wood, these policies are based on the best ideas from his security consulting practice with hundreds of organizations and they are updated every year or two to keep them current with the latest technical developments.

In my practice, I obtain a license to this work for my client and then select appropriate policies for their tailored document. I usually create a hypertext in which there are links to definitions of technical terms and comments explaining the thinking behind the policy. Since Wood provides not only concrete examples of policies, but also editorial explanations that clarify their intent, his text makes my job much easier. This excellent compendium will save you months of work.

The key issues for network managers include communications security, password management, privilege control, logging, and anti-virus policies.

Phase 5: Implementation

Once you've defined your policies, you're about half way to your goal. The hardest part is ahead of you: explaining the need for security and the value of your new policies to your fellow employees. Even if they agree intellectually, there's a good chance that their ingrained social habits will override your new rules for at least months and possibly years. Your task is to overcome these habits.

Security policies and procedures require management support and sanctions. Begin your transformation of corporate culture at the top. Organize a half-day executive briefing session. In the section on network security, you can present your contributions to enterprise security.

- **Network security:** protection against eavesdropping and tampering.
- **Access controls:** password assignment, composition, lifetime, and confidentiality.
- **Encryption:** features, dangers, provision for emergencies.
- **Backup policies** for mainframes, networks, and workstations.
- **Security agreements:** summaries of the policies and procedures to be read and signed annually.

Your next target is the technical support group, who will be the people who help explain your security policies to users. In a one-day training session, you cover

- Everything you covered in the executive briefing;
- Operating system security provisions;
- Security software features;
- Changes in operations to comply with new procedures.

Lower-level staff need a half-day session which answers the following questions in terms that apply directly to their own work:

- Why do I care about information security?
- What are my obligations as an employee?
- How do I protect the PC I'm responsible for against viruses?
- How do I back up my data?
- How do I manage my passwords?
- What must I do if I see someone violating our security policies?

The class ends with the signature of the security agreement.

Phase 6: Maintenance

Now that you've started the process of integrating a concern for network security into every aspect of your organization's work, you have to keep the issue fresh. Successful security awareness programs include amusing posters, interesting videos, occasional seminars on stimulating security topics such as recent frauds or computer crimes and regular newsletters with up-to-date information. Finally, every employee should read and sign the annual security agreement. This practice ensures that no one can argue that the organization's commitment to security is a superficial charade.

Chapter Notes

Copyright © 2001 M. E. Kabay. *All rights reserved.*

1. The original references are all to an excellent textbook,
Lippa, R. A. (1990). *Introduction to Social Psychology.* Wadsworth (Belmont, CA). ISBN 0-534-11772-4. xxiii + 643. Index.

2. I received Professor Lippa's 1994 update to his text and it seemed, if anything, even more fascinating and packed with valuable concepts, case studies, and research results:
Lippa, R. A. (1994). *Introduction to Social Psychology, Second Edition.* Wadsworth (Belmont, CA). ISBN 0-534-17388-8. xxi + 770. Index.

3. Readers will want to contact Commonwealth Films for their latest catalog of instructional films. They have a good selection of videos covering issues in security, among many other topics. Their films are always professional and usually entertaining as well--an excellent combination.

Commonwealth Films Inc.
223 Commonwealth Avenue
Boston, MA 02116
Tel. 617-262-5634
Fax 617-262-6948
Web http://www.commonwealthfilms.com/

Copyright © 2001 M. E. Kabay. *All rights reserved.*

The following paper is an edited version of Chapter 12 from
The NCSA Guide to Enterprise Security
Published in 1996 by McGraw-Hill
By M. E. Kabay, PhD, CISSP
Associate Professor of Information Assurance, Norwich University
mailto:mkabay@norwich.edu

Objectives:
After studying this chapter, readers should be able to
1. Define the three levels of information warfare.
2. Give examples of each type of infowar.
3. Discuss actions for defending organizations and society against infowar attacks.

1 Introduction

This chapter looks at information security from a different perspective. It was originally written for the Canadian Security Intelligence Service and provides an overview of how deliberate attack on information technology can affect individuals, organizations and entire societies.

1.1 Historical Perspective

Throughout the history of conflict, technology has provided both weapon and target. When warriors mounted horses, their steeds provided both threat and vulnerability to opponents. To harm a single mounted man, one could attack his horse. To imperil a nation of horsemen, one could poison the herds. Armored knights fell to crossbows, but a more subtle attack was to destroy the foundries.

The defining technology of civilization as we enter the twenty-first century is the computer. Computers are pervasive, necessary and vulnerable to attack. Computers are linked to each other through networks; one cannot pick up a daily newspaper without reading about the data superhighway that will supposedly bring cyberspace into our living rooms and allegedly bring anything from good grades to the end of civilization.

Cultures that depend on information systems are vulnerable to information warfare. Information warfare consists of deliberate attacks on data confidentiality and possession, integrity and authenticity, and availability and utility. Information warfare can harm individuals, corporations and other private organizations, government departments and agencies, nation-states and supranational bodies. Information warfare is the extension of war into and through cyberspace.

Military planners have recognized their dependence on information technology; some forces now speak of C4I: Command, Control, Communications, Computers and Intelligence. Protecting the technology of war against attack is an obvious extension of the military mind set; smart bombs require smart defenses. However, there is still no general agreement within the military

Copyright © 1995, 2001 M.. E. Kabay *All rights reserved.*

establishments of the planet on the importance of protecting civilian as well as military information infrastructure. As for civil defense, there is a long way to go in including the information infrastructure as a necessary component of protection and recovery operations. Federal government departments are at least required to pay attention to the Government Security Policy, which mandates attention to security and business resumption planning (BRP); however, the task has barely begun in most departments. Provincial and municipal governments are at different stages of awareness and implementation of security and BRP. Finally, in the civilian arena, there are still many organizations which assume that disasters--let alone deliberate attack--will never strike.

Given the degree of dependence on information systems, it is essential to erect legal, organizational, and cultural defenses against information warfare.

1.2 Conceptual Framework

Information technology has so permeated the popular culture that many people now recognize the term cyberspace. Cyberspace is the realm of communications and computation. A telephone call, for example, is said to exist in cyberspace; so does a MUD (multi-user domain, where people play games with each other and with computers) or an online database of bibliographic references. When fighter pilots use computer-generated displays to locate and destroy targets, they are working simultaneously in cyberspace and in the physical world.

Alvin and Heidi Toffler have recently published a cautionary text looking at the transformation of warfare. They explore many aspects of warfare in the age of cyberspace and have several sections dealing with information warfare proper. They provide a good introduction to the changes that must occur in military thinking as cyberspace expands.

Winn Schwartau has defined three levels of information warfare:

- Level one: interpersonal damage. Damage to individuals in recent cases includes impersonation in cyberspace (e.g., false attribution of damaging communications), appropriation of credit records (for fraud and theft), harassment (e.g., interruption of phone services) and loss of privacy (e.g., theft of medical records).

- Level two: intercorporate damage. Attacks on the financial and operational interests of corporations, government departments, universities and so on. Such attacks include industrial espionage, theft of services or money, and sabotage.

- Level three: international and inter-trading block damage. Destabilization of entire economies and societies. The techniques of information warfare levels one and two could be applied in a systematic way by terrorists, extortionists, or foreign governments.

Copyright © 1995, 2001 M.. E. Kabay *All rights reserved.*

2 Tools of Infowar

For those unfamiliar with the security of information technology (I.T.), the following sections will provide an introduction to the ways criminals, spies and saboteurs can attack such systems. This review will serve primarily to alert readers to vulnerabilities; this is not a primer on countermeasures.

Techniques of attacks on I.T. fall into four basic categories: penetration, disruption, programmatic attacks and physical interference.

2.1 Penetration Techniques

Breaching security perimeters is the first step in many, but not all, attacks on I.T. Attackers, especially criminal hackers, have developed a range of techniques generally called "social engineering." Many techniques involve eavesdropping, or unauthorized listening to communications. Weak access controls give many intruders a nearly open door into data processing and communications systems; brute-force attacks target harder perimeters. Traffic analysis, a component of SIGINT, or signals intelligence, allows an observer to deduce important information by monitoring communications flows. Finally, data leakage is the practically undetectable loss of control over or possession of information.

2.1.1 Social Engineering

Social engineering often begins with scavenging, the search through discarded materials for nuggets of valuable information. Scavengers (also known as Dumpster divers when they root through real garbage) are especially interested in security information that can help them penetrate the perimeter using identification and authentication data. Logon IDs (identification) and their passwords (authentication, or proof of legitimate use of the ID) are prizes in this search. Jerry Neal Schneider, for example, was a teenager with a peculiar propensity for rummaging through the discarded papers from his local Pacific Bell Telephone Company (PacBell) offices. Over several years, he amassed an impressive collection of only slightly out-of-date materials on PacBell policies and procedures. He infiltrated PacBell offices by pretending to be a reporter (no one checked his credentials) and obtained additional information on PacBell management of their inventory. Finally he struck: he ordered a drop off of several thousand dollars worth of PacBell equipment at an authorized spot and collected it using a repainted PacBell van he had purchase for a small sum. This stolen equipment was the start of a thriving, multimillion dollar business in used electronic gear; at one point he even sold some of the stolen materials back to PacBell for what the victims thought a good price.

In addition to physical garbage such as discarded paper and magnetic media, scavengers can search through data remnants such as erased files on disk. It's a pity the DOS "ERASE/DELETE" command was not called the "DESTROY-FIRST-BYTE-AND-LOSE-THE-POINTER" command; such a name might have taught more people that files "erased" by DOS

Copyright © 1995, 2001 M.. E. Kabay *All rights reserved.*

and WINDOWS are actually still on disk until their sectors (addressable areas on disk) are overwritten by later disk writes. Utility programs can easily recover some "erased" files because of this implementation. Even some ways of formatting a disk may not destroy pre-existing information; a “low-level format,” on the other hand, does obliterate all user data on the disk. Some file manager programs provide a “wipe” option for deletes which overwrites file sectors with random data before erasing a file, and this technique should be more widely used for sensitive data. In general, no one should exchange diskettes without wiping existing files.

In military or other high-security applications, a particular problem is magnetic remanence on defective hard disks. If a hard disk fails so that it is impossible to write data to it, there is no way to overwrite those data. There have been many cases of used disk drives being sent to a new customer by service companies as part of an exchange service; these disks may contain proprietary software and data of great value. One of the Sysops (system operator) of the NCSA Forum on CompuServe actually received such a used disk in exchange for her broken unit; it contained client lists from a competitor. If the data on the damaged disk are not encrypted, the disk drive can be subjected to degaussing (exposure to high magnetic fields). In military or government applications where highly confidential data are on the magnetic surface, even degaussing is not considered adequate. In these cases, physical destruction (oxy-acetylene torches are apparently favored) does the job effectively.

Another magnetic remnant usable by the scavenger is leftover RAM: areas of temporary memory that have been released by programs but not cleared by the operating system. Examples include terminal memory after a session has completed, file buffers, and print buffers. When terminal emulation programs are used for communications, they sometimes reserve large areas of memory for display; one can scroll through an entire session from start to finish. Logging off without clearing this memory can allow someone else to read through the previous session, print it, or save it to disk for later analysis.

Social engineering's most powerful and commonly-used technique is impersonation. Impersonation can occur on the human level or electronically. For example, “piggybacking” consists of entering a secure area at the same time as an authorized user. When an employee slips an ID card through the reader and politely ushers a colleague through the door first, the pair have fooled the security system into allowing two people into the area on one ID. Similarly, when users leave work stations logged into a network without putting up a security screen, they have encouraged logical piggybacking into the network. Both forms of piggybacking are made easier by psychosocial factors which impede the implementation of security policies. Most people are socialized into holding doors open for others, so letting one's colleague (or a visitor) in through a security screen may not even register in the perpetrator’s mind as a violation of security: it’s just normal politeness. Blanking one’s screen and locking it before getting up for a coffee may make a naive user uncomfortable: it implies lack of trust of colleagues, and society teaches people to value trust. Appropriate awareness training and practice can overcome these inappropriate scruples.

On a technical level, it is possible for a computer system to impersonate another computer. In January 1995, an Advisory from the Computer Emergency Response Team Coordination Center

Copyright © 1995, 2001 M.. E. Kabay *All rights reserved.*

(CERT-CC) at Carnegie Mellon University (Pittsburgh, PA) described a "spoofing" attack on Internet computers. The attack, aimed at SUN workstations, depended on returning false addresses to obtain unwarranted authorization for network access. In electronic mail systems, it is often easy to alter the routing information to give the illusion that a message has originated at another or even at a mythical computer. It is also possible to use so-called anonymizing servers to remail messages stripped of all original identifying information. According to a report in February 1995 from a Swedish investigation, such a system in Finland has been used by paedophiles around the world to exchange pornographic computer files and to entice children into illicit meetings.

Other social-engineering methods of obtaining information include seduction, bribery, extortion and blackmail. Susan Thunder, a notorious prostitute-turned-hacker, habitually seduced nerdish computer systems operators and then rifled through their belongings during their post-coital stupor to find personal information of use in cracking their systems. As for bribery, one of the little-recognized risks of underpaying and generally abusing employees is that it is easier to suborn a disgruntled employee than a happy one. The full backups of a corporate system may cost $100 in physical media and may required the attention of an operator paid $25,000 a year; however, the value of such backups to a competitor may be in the $millions. Payment of a few months of salary to an unhappy and dishonest operator may bring a return on investment of several orders of magnitude.

Extortion consists of threatening damage unless the victim obeys instructions. There have been cases in which criminals steal the only backups to a system after destroying the original disk copies; such attacks are much rarer now that most people make frequent backups and keep them securely off site. Another form of extortion consists of threatening to sell proprietary and highly valuable information to a competitor.

Organizations which tolerate criminal violations such as software theft are vulnerable to blackmail. Any employee can call a toll-free number to report the use of unlicensed software. Whistle-blowers can report improprieties in government using toll-free numbers and have their anonymity protected; the Securities and Exchange Commission of the U.S. also provides such 800-numbers. Obey the law to avoid any vulnerability to this kind of information warfare.

2.1.2 Eavesdropping

Surveillance equipment has become widely available through catalogs and even store-front operations. Equipment used as props in James Bond movies is now inexpensive and easy to obtain. Wiretaps can be placed on phone lines without even having to connect wires directly to the metal; tiny microphones with radio emitters can broadcast a phone conversation to a listener outside the building. But since millions of people hook modems to their phones for communications between computers, eavesdropping now provides a means for monitoring data transmission. Unencrypted data sent over phone lines can be monitored at the origin, the destination, or anywhere in between. A $600 hand-held wide-band scanner can be used to detect transmissions passing through microwave relays at distances of 50 m and more from the towers.

Copyright © 1995, 2001 M.. E. Kabay *All rights reserved.*

Satellite downlinks have “footprints” of up to 100 km in diameter where signals can easily be picked up and used. Cellular phone calls are trivially easy to monitor, as are any calls made over domestic wireless phones. Anyone concerned with security should also disable baby monitors while making confidential phone calls; the monitors broadcast everything within earshot and have no security provisions for preventing eavesdropping. Finally, van Eck freaking is the practice of detecting signals at a distance, usually from video display terminals, and reconstituting them to usable form. Demonstrations of van Eck freaking have involved equipment costing less than $100 and have succeeded at distances of hundreds of meters. It would be possible to put appropriate electronic gear in an unobtrusive van for a few $thousand and then park the vehicle in the middle of an industrial park for a windfall of information, some of it useful at face value and some of it useful for criminal hacking.

Similarly, now that local area networks (LANs) have become the basic architecture for new information systems in the client/server model, eavesdropping on LANs is a powerful method for extracting valuable information. For example, it is easy to run LAN sniffers--programs which capture all transmissions on the network instead of only the ones destined for a specific, authorized work station. By putting a work station into “promiscuous” mode, anyone can monitor traffic and solve network problems; unfortunately, they can also decode the contents of packets being sent to other workstations on the LAN. Thus a dishonest employee could buy a LAN sniffer or download it from the Internet at no cost and then monitor the system manager's workstation until that person logged on. The system manager's ID and password might be visible and usable unless the network operating system encrypted such information (i.e., made the ID and password unreadable without the proper key).

Similarly, Internet sniffers permit unscrupulous people to monitor unencrypted transmissions through the network of networks that links tens of millions of users and millions of computers. In 1993 and 1994, there have been cases of special modified programs for establishing an interaction with computer systems; these Trojan login programs captured the first 128 characters of each session--plenty to determine a user's ID and password if sent unencrypted. Over ten thousand IDs were said to have been compromised by these Trojan login programs.

2.1.3 Intrusion

Classic failures in security that are exploited by criminal hackers, spies and saboteurs include wide-open old modems, canonical passwords, Joe accounts and generally bad password policies. Any system with a modem kept powered on and appropriate communications software running is at risk of attack and penetration. Factory pre-set passwords in computer systems, telephone switches, and voice-mail systems are a major entry point for intruders. So-called “Joe” accounts, where the password is the same as the ID (e.g., account MGR.FINANCE, password FINANCE) are far too obvious to allow on a system.

Brute-force attack involves trying all likely or possible authentication codes for a given ID. Such attacks often begin with dictionary files to deal with all the easily-guessed passwords and then moving on to random patterns of letters and numbers. The main vulnerability making such

Copyright © 1995, 2001 M.. E. Kabay *All rights reserved.*

attacks possible is that system administrators place inadequate limitations on login speed; it's possible on some systems to try as many passwords as the communications speed allows. Another fundamental problem is that many systems and administrators permit a highly restricted key space; i.e., there are too few possibilities for the authorization codes. As a trivial example, readers will note that on a five-position keypad such as is commonly used to keep doors locked, there are only 120 unique sequences of five digits. Even with only a few minutes per attempt, it does not take long to try all possible sequences.

2.2 More Subtle Attacks

Once intruders or dishonest authorized users have gained entry to a restricted system or a restricted area, they can extract information in various ways. For example, even if data are encrypted, traffic analysis (noting the volume of transactions flowing between nodes in a network or data sets in a database) can reveal information that should be restricted. Even the communications bandwidth alone can tell a spy something of value; e.g., if a manufacturing firm is planning to triple the channel capacity for its Brampton plant, a dishonest competitor will know that it may be worth infiltrating that plant because there is something new happening there. Homely details such as filenames can inadvertently reveal information or indicate importance; e.g., a file named URGENT.FAX is more likely to be of interest than F782H3B.TXT. Similarly, suggestive directory or folder names can attract the attention of spies or saboteurs; e.g, files in C:\R&D\NEW_PROD might be very interesting to an industrial spy. Finally, security restrictions themselves should be considered of extremely high sensitivity; the access control lists for a file might show unauthorized users which user ID could legitimately access it and thus provide a valuable new target.

Perhaps the most pervasive and subtle attack of all is data leakage--the insensible copying of restricted information. The main reason information can be stolen so easily is poor data security among users and administrators of work stations (the term personal computer should have been banned from office environments because of the false impression it creates). Such systems have standardized data formats (e.g., spreadsheet, database and word-processing files) that can easily be read on millions of systems around the world. In contrast, mainframe files tend to be in proprietary or site-specific formats which are considerably more expensive to convert and use. In addition, work stations often have high-capacity miniature media such as 1.44 Mb (megabyte, or millions of characters) diskettes a few cm in diameter (recent products can put 10 Mb on a diskette) or removable disk drives holding up to a Gb (gigabyte, or approximately 10^9 characters) on units that can be concealed in a pocket. Typically, work stations have limited or no physical controls against data theft; they rarely have access-control software installed.

Some simple precautions can make data theft less likely. Clearly labelling all removable media with tags that indicate their level of sensitivity and their ownership would make “accidental” removal of such media less excusable. Security programs on each workstation can prevent unauthorized access to the computer and control use of the diskette drives; the auditing features of such programs can provide a record of all activity by each user ID and by so doing further discourage casual data theft

Copyright © 1995, 2001 M.. E. Kabay *All rights reserved.*

2.3 Disruption

If people want to disrupt the work of an organization in the computer-driven world of today, they have many techniques available. Programmatic attacks and sabotage are easy to implement in most computerized environments. Denial of service attacks by saturation of capacity are also very easy and harmful.

2.3.1 Programmatic Attacks

Programmatic attacks use executable code to interfere with normal processing. Executable instructions determine everything that general-purpose computers can do. Programs are sets of instructions for specific purposes. There are programs in the equipment (hardware) itself--these are the "hard-wired" functions of the arithmetic logic units and other processors. Then there are programs which are put into read-only memory (ROM) units; these are called "firmware" by analogy to hardware and software. Software generally refers to program files (on DOS based computers, these have file extensions such as .COM, .EXE, .DLL and so on), but actually there can be executable instructions in the first sector of every disk as well.

Programmatic attacks include, among others, Trojan Horse programs, logic bombs, worms, viruses, knowbots and cancelbots.

A Trojan Horse program looks like a useful tool but actually has unauthorized and possibly dangerous functions. Trojan login programs, mentioned above, silently capture passwords for later inspection while authorizing sessions. Trojan compilers convert ordinary source code into executables that can include unauthorized back doors to subvert security. Logic bombs are any unauthorized sequence of instructions with a trigger (e.g., a date) and a payload (e.g., wiping out records in a database). Without the appropriate inactivation code, the logic bomb damages data according to the programmer’s instructions. The disgruntled programmer shown in the movie Jurassic Park left a logic bomb in the system after he left; so did the mistreated programmer in the movie Single White Female.

In real life, some consultants in the CONSULT Forum of CompuServe have admitted publicly that they generally leave logic bombs in their custom-written computer programs for clients and remove the bomb only once the client has paid them in full for their work.

Worms are programs or other executables that spread through a network. Some worms send a copy of themselves into a neighboring system and then “die.” Robert T. Morris sent a worm into the Internet on November 2, 1988; unfortunately, due to programming errors, the worm reproduced madly in thousands of systems, causing havoc that consumed days of time for thousands of system administrators and users. Estimates of the damage caused run to the tens of millions of dollars in lost data and wasted time. Perhaps the only good thing coming out of the

Copyright © 1995, 2001 M.. E. Kabay *All rights reserved.*

Morris Worm incident is that it (and another worm attack in late November 1988) led to meetings of Internet experts who then helped found the

Viruses are programs which insert themselves into other executables. The most widespread viruses "live" in disk boot sectors, from which they enter RAM on DOS and Macintosh workstations during system initiation. This "boot" process always looks at the boot sectors of diskettes and disks that are accessible; thus if an infected diskette is still in the boot drive (usually A: on a DOS machine), the virus is loaded and executed before the rest of the operating system is loaded--and thus before any normal security mechanisms are engaged. Once in memory, the viral code can do anything the operating system can do. For example, some of the five thousand known virus varieties can garble printer output, make all periods disappear from DOS commands, scramble file names, erase portions of disks, and make green caterpillars crawl around computer screens. Worse still, some viruses, such as those concocted by the Bulgarian "cyberpath" who calls himself Dark Avenger, cause subtle data damage that may not be noticed for months yet can falsify results with potentially fatal effects.

Knowbots are programs which, like worms, move from system to system; they are designed to seek out specific information and report back to their originators. Cancelbots are knowbots which seek out electronic mail or postings to news groups (a kind of automated mailing list) on the Internet; when they find a specified target, they destroy the message. Cancelbots have been unleashed by cyberspace vigilantes who object to "spamming" of the Internet (the despicable practice of sending thousands of identical messages which end up inconveniencing millions of readers) with commercial or religious messages posted in unrelated forums. Unfortunately, cancelbots can equally well be instructed to destroy any other message, thus interfering with freedom of speech.

2.3.2 Denial of Service

Capacity saturation began in the early 1990s in connection with commercial spamming of the Internet. When Canter and Siegel, attorneys from Arizona, sent thousands of messages about the U.S. Dept of Immigration's Green Card Lottery into Usenet groups completely unrelated to such a topic, they angered many thousands of Internet users, many of which have to pay fees as a function of volume and most of which dislike irrelevant materials in their focussed newsgroups. One person from Australia "mail-bombed" Canter and Siegel's Internet address, sending them thousands of large e-mail messages full of abuse. The guilty pair's Internet provider crashed because it couldn't handle the volume.

A similar attack has been perpetrated on bulletin board systems (BBSs) when there are no limits to how many messages can be posted by a single user in a defined period; by automatically uploading hundreds or thousands of messages, a single individual can fill all available message slots or hard disks and prevent other people from uploading their own messages. The volume of useless messages also dilutes the value of the existing message base and drives away legitimate users. If the number of messages is fixed, the new messages can completely replace the old ones, entirely destroying the message base.

Copyright © 1995, 2001 M.. E. Kabay *All rights reserved.*

Another nasty denial of service attack is possible when repeated logon errors cause an ID to be locked out of a system or network but there are no delays imposed before trying another logon. By logging on to every ID in turn and deliberately entering invalid passwords, a single criminal hacker equipped with a programmable communications package can shut down access to all but the supervisory IDs on a system.

I mention these simple-minded attacks because they illustrate that people of bad will can far too easily disrupt the work of well-meaning but naive system administrators and users. Although we have been thinking about examples involving Internet groups and BBSs, I invite readers to contemplate the likely effects if the same techniques were to be applied to corporate inventory systems, stock exchange accounts, banking systems, the emergency 911 telephone system, or the systems which generate their own pay cheques.

By the year 2000, distributed denial-of-service (DDoS) attacks were common; they use covertly-installed programs (*zombies* or *slaves*) that listen for coded instructions from a *master* program. Massive DDoS attacks on well-known Web sites such as Amazon.com and eBay.com resulted in so much interference with legitimate traffic that the victims lost millions of dollars in sales and services. Their stocks declined significantly immediately after the attacks.

2.3.3 Physical Disruption

Finally, one can apply physical interference to I.T. Sabotage has been a constant problem for anyone depending on expensive equipment; computers have been struck with axes, bombed, burned, drowned, shot and starved of electricity. These are the kinds of attacks that have concerned military thinkers involved in electronic warfare and countermeasures for years. However, new methods involving electromagnetic interference are causing concern in infowar circles. HERF (high-energy radio-frequency) guns can stop a computer dead at 100 m--or worse, cause mysterious malfunctions or data errors. In terms of productivity, having half a dozen people wasting three hours trying to analyze the peculiar behavior of a computer is more expensive than simply having the computer stop working.

An extension of the HERF attack is the EMP/T (ElectroMagnetic Pulse Transformer) bomb. This is a device designed to emit high-intensity radiation sufficient to damage modern I.T. equipment. An small, easily concealed EMP/T bomb detonated in a van on a downtown Toronto or Manhattan street could wipe out the stock exchanges, major telephone switches, and countless businesses (the ones without disaster prevention, mitigation and recovery plans). The total damage to the north American economy could greatly exceed the consequences of a physical explosion from a physically-comparable device.

On a more personal level, most airplanes flying today have fly-by-wire systems in which control surfaces are controlled by servo-motors. Instructions to the servo-motors are generated using electronic equipment of great sophistication. Ordinary cellular phones, portable computers, and even hand-held children's video games have been shown to affect some planes' stability, especially during takeoff and landing. Given the ease with which one can manufacture a

Copyright © 1995, 2001 M.. E. Kabay *All rights reserved.*

powerful HERF gun using off-the-shelf electronic equipment (a domestic microwave oven is a start), there is reason to worry that criminals or terrorists stationed outside the security fences will eventually aim one of these devices at a plane landing at an airport.

3 Case Studies of Infowar Techniques (as of 1995)

The following sections will provide readers with some examples of the application of the information warfare techniques to Schwartau's three levels (interpersonal, intercorporate, international) of conflict. Many examples of such attacks are documented in the RISKS Forum Digest, moderated by Dr Peter Neumann of SRI. Readers can subscribe by sending e-mail to

risks-request@csl.sri.com

with the message "SUBSCRIBE."

Another source of up-to-date information is the NCSA FORUM on CompuServe. Use "GO NCSA" for information on this service. Section 2 is dedicated to news and case studies; section 6 deals with disaster recovery; and section 16 deals with operations security (OPSEC) and information warfare. At time of writing (July 1995), participation had reached 35,000 and was climbing by 500 new participants every week.

3.1 Level One: Interpersonal Attacks

Schwartau has spoken and written extensively about the cyberspace shadow and its vulnerabilities. The cyberspace shadow is the model in cyberspace of a person or of an organization; e.g., a person's credit records, medical files in a hospital database, driving records and criminal records--all are aspects of the cyberspace shadow. Harm to the cyberspace shadow falls into three main categories: invasion of privacy, impersonation and character assassination, and harassment.

3.1.1 Invasions of Privacy

Concerns over the invasion of privacy via the cyberspace shadow are many. The Internet's Computer Privacy Digest is a useful source of information about such issues; it is available by electronic mail (e-mail) by sending the e-mail message "subscribe" to its moderator at its comp-privacy-request@uwm.edu address. Government and commercial intrusions into the privacy of individuals is of great interest, but there are also cases of harm from individuals.

Privacy can be invaded in several ways. For example, managers or intruders can snoop through files and e-mail without explicit permission. On government and commercial systems, such snooping may explicitly be sanctioned by employment contracts and procedures manuals, but it nonetheless poses the risk of harming employee relations. Most employees assume that e-mail is as secure (or no more insecure) than postal mail (insultingly called snail mail by the electronic cognoscenti) and are deeply offended when their manager questions their 10 Gb databases of electronic pornography.

Copyright © 1995, 2001 M.. E. Kabay *All rights reserved.*

On a more prosaic level, market research firms are rabidly pursuing detailed information about individual's patterns of consumption. When one shops at a grocery store that supplies annotated receipts, it is highly unlikely that the data will be discarded; any purchase using a debit card or a credit card makes it almost certain that the information will be stored and possibly released to market research organizations for analysis. Eventually, it is likely that individuals will received carefully-tailored, computer-generated junk mail configured to precisely their buying habits.

If video stores and book stores store and sell such data--or even allow these data to be stolen--there is a risk of harassment from extreme political and religious fringe groups. How would consumers like to be picketed, bombed or shot for having bought a book or video entitled Especially Offensive Uses of Common Vegetables? Or for that matter, Modern Birth Control or Lyndon Larouche and the Rise of the New American Fascism?

The potential for misuse of medical information is enormous, but in many clinics in Canada and around the world, older sensitive medical information is kept on charts and newer sensitive records are on work stations. The charts are carefully kept in locked filing cabinets, often with stout security bars of stainless steel and one-pound padlocks; in shocking contrast, the computers are completely unprotected by either physical anti-theft devices or by logical access control or encryption software. This situation results from the general level of unawareness of the vulnerability of computer systems to misuse. In one recent case, a male nurse's aide called a patient at home after her hospital stay to invite her on a date; when she demanded to know how he knew her name and phone number, he admitted that he had simply tapped a few keys on the computer at the nearest nursing station on her floor after seeing her in hospital. In Florida in December 1993, two security guards stole computers containing the medical records of 8,000 carriers of HIV, the cause of AIDS. Luckily, the thieves did not try to extort money from these people--no thanks to the inadequate security at their clinic.

3.1.2 Impersonation and Character Assassination

Another key issue in Level One infowar is identity and anonymity in cyberspace. In a previous paragraph, we saw that breaches of privacy can occur when identity is too easily obtained (e.g., personalized records of purchases). However, anonymity and pseudonymity (the use of a false identity or of someone else s identity) are serious questions. In a recent case reported in the NCSA Forum on the 2.5-million user CompuServe network (GO NCSA), a university student waited four months to open the envelope from his university computer centre containing his new Internet account and password. Unfortunately someone else deduced his password (first initial, middle initial, and start of his last name!) before he opened the envelope and sent hundreds of obscene and racist messages to faculty, students and strangers with predictable results to the naive user's reputation.

Internet e-mail includes its routing information (sender, date/time stamps, systems through which the message is forwarded) as ASCII headers placed at the start of the message, anyone with access to the e-mail messages can alter those headers. A foolish university student sent a death

Copyright © 1995, 2001 M.. E. Kabay *All rights reserved.*

threat via e-mail to President Clinton; despite his attempts to disguise the origins of his message, he was arrested a few days later after some fairly easy detective work by the FBI and the Secret Service. Nonetheless, without using digital signatures and message digests (techniques for creating unique sequences that unarguably prove the identity of the sender and the integrity of the message received) as a normal component of electronic communications, these cases of fraudulent identity will continue.

Winn Schwartau himself nearly had his reputation ruined a few months ago when someone used his logon on The Well, a popular network based in San Francisco, and sent out nasty and vulgar attacks on a criminal hacker. Grady Blount, a professor at Texas A&M University required police protection and had to move his classes to different locations after a criminal hacker stole his electronic identity and sent out thousands of hateful messages under the professor's name attacking various ethnic groups. In the real world, individuals have suffered for years after thieves obtained their social insurance numbers and credit records to order credit cards in the victim's name; the thieves rack up hundreds of thousands of dollars of purchase and then default on their payments, leaving the original owner of the electronic identity to pick up the bill--and the court cases, ruined reputations and even family breakup.

Some politicians have suggested that they'd like to receive e-mail as a method of gauging public support for or opposition to various political initiatives. The obvious question is whether political judgements should be based on opinions sent by a currently tiny minority of the population--those with access to e-mail. But even apart from this problem of bias, without reliable identification and authentication, individuals and hostile agents could easily sway gullible politicians into perceiving a warped vision of reality simply by using computers to generate tides of fraudulent but realistic opinions. Science fiction author Orson Scott Card imagined just this mechanism for distorting the political process in his novel, *Xenocide.*

3.1.3 Harassment

Other ways of causing problems for individuals have been documented and qualify as Level One infowar:

- For example, Kevin Mitnick is accused of having caused someone he disliked to be invoiced for an entire hospital's phone bill.

- A church's phone was reputedly call-forwarded to a 900 sex line.

- A person accused of spamming the Internet found his company's 800 number listed as a phone-sex line in various alt.sex groups on the Internet, resulting not only in thousands of dollars of charges to his company but personal humiliation when the receptionists refused to put up with any more of the heavy-breathing callers and sent them all to his own phone extension.

Copyright © 1995, 2001 M.. E. Kabay *All rights reserved.*

- In another case of Level One harassment discussed at a criminal hacker convention in December 1993, a poor soul found that a criminal hacker had used a war dialer (a program for automatically dialling phone numbers in sequence) and had left the victim's phone number on thousands of pager accounts. The innocent pager users were irritated at having made a call for nothing, but the victim's life was made untenable for a day.

- Finally, in a recent case in Toronto, a night auditor in a commercial centre obtained computer records for 28,000 credit-card transactions from January 1989 to May 1994. Using these data, the criminal, working with dishonest business confederates, generated phony transactions and shared the proceeds, amounting to C$1.5 million.

3.2 Level Two InfoWar

At the intercorporate level, infowar consists of industrial espionage, theft, and sabotage.

3.2.1 Espionage

Espionage is not new, but electronic systems make it much easier than in the days of breaking-and-entry and tiny cameras. American Airlines, for example, is reported to have been upset when valuable tables showing the expected rate of no-shows for each of its flights in North America were allegedly stolen on diskettes and given to Northwest Airlines. Such data leakage will become more common unless organizations implement effective policies for improving security awareness and monitoring compliance with written security policies.

Another interesting example of data leakage occurred in Australia, where dishonest employees sold information to unscrupulous accountants showing how the department of revenue chose its candidates for financial audits.

Encyclopedia Britannica lost control of 3,000,000 names of subscribers and prospects, conservatively evaluated at $1,000,000 in assets; the culprits were employees in the data processing department.

Companies have been caught hiring moles in rival organizations and sending out information via electronic mail; Symantec and Borland, two well-known software companies from the West Coast of the U.S., battled each other in court over one such case. In 1992, Eugene Wang, a VP at Borland International Inc., allegedly sent his future employer, Symantec Corp. CEO Gordon E. Eubanks e-mail containing confidential Borland data. The case was dismissed in August 1993 by the Superior Court in Santa Cruz county, California, when the judge discovered that Symantec had paid some U$13,000 in expenses incurred by the public prosecutor’s office.

In this world of sharp competitive advantages, a single diskette holding a thousand pages of information can slip away in a vest pocket or a purse and be worth millions to a competitor. General Motors’ Opel division is embroiled in a legal battle with Volkswagen over information

Copyright © 1995, 2001 M.. E. Kabay *All rights reserved.*

allegedly spirited from Opel to VW by Jose Ignacio Lopez de Arriortua, a senior executive upon being hired away from Opel. Three crates of confidential VW information were allegedly discovered at his apartment by German police investigators. The accusations continue.

3.2.2 Theft

The theft of telephone services is estimated to be reaching $8 billion in North America alone. Young criminals have been found scanning for codes by using binoculars in airports and train stations; there are telephone boxes in some cities where people line up to pay $3 for 10 minutes of long-distance calls anywhere in the world--and individuals or companies pay the bill. Some criminal phone phreaks have invaded voice-mail systems, illegally setting up their own voice-mail boxes for personal use. Another kind of theft recently occurred in Germany, where two employees placed microcomputers in a switching centre and placed thousands of calls to 1-900-SEX lines in the Caribbean. Charges were randomly allocated to clients all over Germany, and the phone company had to pay tens of thousands of dollars to the overseas aural sex operations. The criminals in Germany then received part of the illegal profits from the sex-line operators in return for their nefarious deeds.

In case reported in October 1994, a ring of criminal hackers operating in the United States, England and Spain stole the telephone calling card numbers of 140,000 subscribers of AT&T Corp, GTE Corp, Bell Atlantic and MCI Communications Corp. These thefts are estimated to have resulted in U$140 million of fraudulent long distance calls. In a significant detail, Ivy James Lay, a switch engineer working for MCI, was known in criminal hacker circles as “Knight Shadow.” He is accused of having inserted Trojan horse software to record calling-card and ordinary credit-card numbers passing through MCI's telephone switching equipment. European confederates, led by 22-year old Max Louarn, of Majorca, Spain, paid him for the stolen data, then set up elaborate call centres through which users could make overseas calls. This is one of the most obvious cases where young but experienced criminal hackers appear to have planned a Level Two attack on major corporations.

Another example of Level Two theft occurred in Hartford, Connecticut in April 1993. A new automated teller machine (ATM) was installed in a suburban mall. It functioned acceptably at first, but soon began behaving peculiarly. It would accept a user’s card, ask for the personal identification number (PIN), and then announce that it was out of order, suggesting the user switch to a nearby ATM. This was an elaborate spoof, and the criminals who installed the ATM used the card numbers and PINs their machine had recorded to create bogus ATM cards. They stole over $100,000 in three weeks but were eventually caught because they didn’t realize that their picture was being recorded on video at the many ATMs where they used their fake cards. Diligent cross-matching by the police showed that all the fraudulent transactions were associated with withdrawals by the same people and so the criminals were defeated.

The latest spectacular ATM attack occurred between Friday the 18th and Monday the 21st of November 1994 in and around Portland, Oregon. Two thieves stole a bank card from a purse left in a locked van in a suburb; the owner had unfortunately written her PIN on her Social Security

Copyright © 1995, 2001 M.. E. Kabay *All rights reserved.*

card. The thieves used the stolen card within minutes at an ATM a few blocks away and retrieved the daily maximum--U$200. By what may have been a stroke of luck, the daily limit did not apply that weekend, for the Oregon TelCo Credit Union was in the midst of upgrading its ATM software. The thieves were able to "jackpot" 48 bank machines in 724 withdrawals over the next 54 hours, stealing U$346,770 in all. They occasionally fed empty envelopes into the ATMs, claiming to have deposited a total of U$820,500 into the victim's account--and again, the bank software failed to block the fraudulent deposits as it should have. Four suspects were arrested within days of the spree, but why the bank software should have been so easy to dupe is still not explained.

3.2.3 Sabotage

In the late 1980s, a New Jersey magazine publisher began receiving complaints from its customers. Voice mail messages renewing valuable and important advertising had never been heeded. Employees claimed they never received the calls at all, and the voice-mail system supplier was called in for technical support. Investigation showed everything normal, suggesting the dreaded intermittent problem. However, customers began reporting a problem which could not be accounted for by defective software or hardware: outgoing messages had been altered to include rude and sometimes lewd language and suggestions. Attention shifted to inbound calls. In a short time, investigation showed that someone was interfering with the phone system, re-recording employees' welcome messages and deleting inbound messages from clients. The culprits proved to be a 14-year old and his 17-year old cousin, both residents of Staten Island.

Why did the youngsters attack the publisher's voice mail system? It seems that the younger had ordered a subscription to a magazine dedicated to Nintendo games (don't laugh, it's no weirder than magazines about home decoration). The magazine subscription offer included a colorful poster normally costing U$5. The magazine arrived; the poster didn't. The youngsters phoned the company, were assured they'd receive the poster, and waited. No poster. So they entered the company's voice mail, cracked the maintenance account codes and took over the system. Their shenanigans resulted in lost revenue, loss of good will, loss of customers, expenses for time and materials from the switch vendor, and wasted time and effort by the publisher's technical staff. Total cost (admittedly, estimated by the victim): U$2.1 million.

However, sabotage is by no means the purview of teenagers.

A plumber in Philadelphia was arrested in January 1995 and accused of having arranged for the local phone company to install call-forwarding on several phone lines. All the calls to these numbers were duly forwarded to the plumber's office. Unfortunately, the calls were intended for several of his competitors; he and his staff skimmed the profitable cases from the influx of calls from his competitors' clients and refused service or were rude to the rest, damaging his competitors' reputations. After a few weeks, a happy client called her plumber to thank him for having repaired a pipe over the Christmas holidays; he, of course, had no record of having worked over the holidays, and after a short investigation, the criminal scam was discovered and the perpetrators arrested.

Copyright © 1995, 2001 M.. E. Kabay *All rights reserved.*

In a Washington, D.C. area office of the Bureau of Mines of the U.S. Department of the Interior, someone destroyed the data on hard disk drives of 19 microcomputers and stole two more. The incident occurred on Friday, August 12, 1994 around 18:30. The saboteur set up the instructions for formatting all 19 systems, then walked through the installation pressing the ENTER key on all the machines. The damage was complete within 15 minutes. Ironically, it appears that the criminal may have performed a dry run a week before, when two systems were inexplicably found formatted. After this incident, a few workers heeded security specialists' warnings that they should use access-control software with good passwords on their machines, but most did not. Those who passworded their computers were not hurt by the sabotage. Luckily for the Bureau, the culprit did not know enough about computers to overwrite the hard disks, and so technicians were able to salvage most of the data using disk utilities to undo the formatting.

In a recent application of HERF techniques for sabotage, a spectator was arrested for allegedly causing the crash of several large model airplanes at the Medeira races in Spain in the autumn of 1994. According to a report published in Schwartau's Security Insider Report, the accused "was using a frequency scanner to find what frequency the flier was using, then swapped the crystal of his own transmitter to match, thus causing the plane to lose control and in most cashes crash.... Just to add a bit of perspective, these planes cost upwards of $10,000 and travel at well over 100 mph. The impact energy is about three times that of a .45 bullet. I don't think there were any injuries, but there very easily could have been, to any of the thousands of spectators...."

4 Level III Infowar

Previous articles on "Economic Espionage" by Samuel Porteous in *Commentary* number 32 (May 1993) and number 46 (July 1994) discuss how governments all over the world have supported a wide range of open and clandestine espionage designed to confer benefits on national enterprises. Mr Porteous has also recently published a summary of this situation in *Intelligence and National Security* 9(4):735-752 (October 1994).

Government involvement need not be limited to espionage, however. In July 1985, two officers of the French intelligence service killed a photographer when they blew up and sank the Rainbow Warrior, a ship owned and operated by the environmental group Greenpeace, while it was in port in Auckland, New Zealand. If governments are willing to resort to this kind of action, what could possibly impede them from any other tactic, especially when it might be even harder to trace the originators? Level Three information warfare attacks could involve immediate attacks causing serious damage or insidious attacks with even more serious consequences.

4.1 Immediate Attacks

Copyright © 1995, 2001 M.. E. Kabay *All rights reserved.*

- Civil aviation: interference with control towers, radio communications, and even the avionics of commercial aircraft would paralyze huge sectors of an economy. In North America, even fog at O'Hare International Airport in Chicago or Pearson Airport in Toronto can cause repercussions to spread over the entire continent. Delays in air transport would not merely inconvenience holiday travelers or lead to cancellations at hotels and resorts; they could also interfere with business meetings, cause manufacturing slowdowns, increase congestion on land routes, and, as always, affect the stock market.

- The phone grid: when the 911 system goes down, there can be chaos. Emergency calls for medical help, fire services, or police action can go unanswered for long periods, leading to danger or social disorder. When the regular phone system fails, even for an hour, the economic consequences merely from the impossibility of completing credit card transactions can range into the millions of dollars. If a single determined criminal hacker was able to infiltrate the MCI switch in Cary, North Carolina (see above) to steal telephone codes, there is nothing to stop a trained information warfare specialist to do the same for more insidious purposes.

- National and international banking systems and stock markets depend on the unimpeded and timely flow of accurate information. The slightest perturbation in such systems could have catastrophic consequences for the world monetary and financial systems. Mexico's currency devalued by about half over a few weeks simply because of uncertainty over the country's stability; Canada may experience the same phenomenon as the debate over the secession of Quebec continues. If a foreign nation were to want to destabilize a country, interfering with the monetary networks and stock markets would be an excellent way to do so. Feeding incorrect information into the networks, deleting transactions, even spreading rumors through the Internet could cause more damage--untraceably--than bombing a building.

4.2 Insidious Attacks

As Schwartau has frequently pointed out, destroying things in an obvious way has immediate effects; however, at least the victim recognizes the problem. Once the bomb goes off, we can start repairing the damage. The really nasty attacks are the ones we don't recognize.

In his novel, *Terminal Compromise,* Schwartau explores several techniques that would be useful in Level Three information warfare. For example, he envisages viruses with long latency; that is, self-reproducing programs which do no damage for quite a long time, allowing them to spread invisibly throughout a nation's computers. Information warfare viruses, being written by serious operatives instead of by neurotics, could have insidious payloads; for example, they could subtly alter data in spreadsheets, making changes of, say, a few percent in random cells. The confusion and disruption caused by such errors would be far worse than the outright crash of a program; people would spend countless hours trying to find the errors in their (usually undocumented) spreadsheets--or suffer the consequences of incorrect budget estimates, erroneous engineering calculations, and impossible predictions from numerical models.

Copyright © 1995, 2001 M.. E. Kabay *All rights reserved.*

It would be possible to introduce errors into much of the commercial software produced in a specific country; for the U.S., for example, just arrange to infiltrate agents into Microsoft and Computer Associates (firms which produce enormous amounts of software). Even with the best will in the world, no one can stop all accidental errors; how much more difficult, then, to catch errors deliberately concealed by malicious programmers.

Another approach to ruining a specific economy would be to distribute hardware deliberately engineered to cause problems--the Pentium chip on purpose. The Pentium chip debacle occurred when Intel, maker of the 80x86 series of microprocessors used in several generations of IBM-PC compatible microcomputers, failed to notice errors in the design of their newest chip. It made mistakes in certain floating-point divisions. Unfortunately for everyone, the maker failed to announce this error publicly, and there was a brouhaha when the bug was discovered. Now imagine a foreign government arranging to plant agents in the laboratories of major hardware and software manufacturers. After a few instances of catastrophically bungled programs or chips are discovered, the reputation of an entire industry can be damaged for a long time. Even the rumor of such problems could cause disruption, loss of productivity, and international trade imbalances.

5 Discussion: Civil Defense in Cyberspace

With every advance in technology comes new vulnerabilities to attack. Civil defense contingency planning currently pays attention to preventing and recovering from damage to the physical infrastructure of society. With the growing dependence upon information technology in our complex civilizations, we must hasten to include cyberspace in our concerns.

As this article has shown, there are many ways to harm the interests of individuals, organizations and nations using the new weapons of information warfare. To strengthen our collective resistance to such threats, we should work at many levels to bring information technology and its protection into our personal, corporate and political discourse. The following suggestions will serve as a starting point and are discussed below:

- Raise individual awareness of privacy and security in cyberspace
- Raise corporate commitment to information security
- Expand fundamental orientation of risk management
- Increase military education and planning for information warfare
- Encourage cooperation between military and civil authorities
- Set national priorities to include information security

Copyright © 1995, 2001 M.. E. Kabay *All rights reserved.*

- Encourage mandatory reporting of information system attacks and failures
- Establish international agreements on jurisdiction over attacks in cyberspace

5.1 Raise Individual Awareness of Privacy and Security in Cyberspace

Some attacks in cyberspace come from relatively young people. Some children and especially teenagers find computer crime attractive because it expresses their natural tendency to rebel against adult norms, enhances their sense of affiliation with a group, emphasizes intelligence and technical skill, and can be lucrative. In addition, most parents know little about the activities of their children in cyberspace

Although there are already successful efforts in the K-12 school systems, we should collectively expand the availability of good-quality training and awareness materials for children in our educational system. For the youngest children, awareness of the social norms already evolving in cyberspace can be taught in entertaining and memorable wasys; for example, Gale Warshawsky of the Lawrence Livermore National Laboratory in the United States has created a group of charming puppet characters who introduce very young children to concepts of information privacy, data integrity and even viruses.

At the Reconstructionist Synagogue of Montreal, the congregation invited me to speak on Ethics in Cyberspace in May 1995. The program was directed to children and their parents and includes videos and discussion about the problems caused by breaches of security. Parents and children received a checklist of questions suitable for family discussion:

National Computer Security Association

Ten Questions Parents Should Ask Their Children

A. Respect for intellectual property rights

1. Do you legitimately own all of the software, games, and programs you have or use?

2. Where did the contents of your report / project / homework come from -- does any of it belong to someone else? Did you write/create/author what you're passing off as your own work? Where did you get the text and images you're using? If you copied text and images from another source, did you have permission? If you didn't need permission from the "owners" of the information you're using, did you credit them for the material?

B. Respect for other people's property rights

Copyright © 1995, 2001 M.. E. Kabay *All rights reserved.*

3. Do you ever use other people's computer, disk-space or processing capability, or look at or copy their files or information, without their knowledge or permission?

4. Do you have any prank programs, computer viruses, worms, trojan horse programs, bombs, or other malicious software?

C. Respect for social values

5. Do you have any computer graphics files, clips, movies, animations or drawings that you would be embarrassed about? Do you have them legitimately? Are they things you would be comfortable showing me? Showing your grandmother? Do you have any pictures, video clips, sound clips, articles, text, or other software or files which contain pornography, violence, dangerous instructions other distasteful material? Do you access or view any of these kinds of things when using the net?

6. Do you have any newsletters, plans, guidelines, or "how-to" documents or files that you would not be comfortable showing to your mother? For instance, making bombs, breaking into systems, stealing telephone access, stealing computer access, stealing passwords, pornographic or violent text, guides, descriptions? Do you create, contribute to or receive anything like this?

D. Questions related to network use

7. Do you ever connect your computer to a telephone, use a modem, or otherwise use a network?

If so, consider the following questions:

8. With whom do you associate when you use the Net? Tell me about your contacts.

9. Do you ever use an assumed name, a handle, or an alias instead of your real name? Do you supply a false information about yourself when using a bulletin board, a news group, a message group, or forum, any part of the net, or when using e-mail or when otherwise communicating? Do you use your real age & sex when communicating with your computer? Do you use any false information such as a fake addresses or phone numbers or use someone else's credit card number when using your computer? Do you ever send messages or e-mail in such a way that the recipient cannot tell that you sent it? Have you ever modified data, text, messages, or other computer information so that it looks like someone other than you created it or made the changes? What are you trying to hide by not using your real name? Are you trying to pretend you are something or someone you are not?

Copyright © 1995, 2001 M.. E. Kabay *All rights reserved.*

10. Do you use telephone, video, cable-TV, computer network, bulletin board, or other network services without paying for them?

5.2 Raise Corporate Commitment to Information Security and Ethics

In a recent survey (Computerworld 95.03.20, p.16; reporting on Susan J. Harrington's article, "Computer Crime & Abuse by IS Employees" in the March/April 1995 issue of the Association for Systems Management's *Journal of Systems Management*) of more than 200 programmers and other information technology professionals at nine Ohio-based manufacturing and service companies, 41% admitted that they would illegally copy software for themselves or a friend, 7% would adjust a bank account system to avoid incurring a service, and 10% saw nothing wrong with sending a virus program that would output the message, "Have a nice day."

With this level of ethical commitment in the workplace, it is no wonder there are growing problems of industrial espionage and sabotage.

One solution is to apply the same methods used to change corporate culture in the TQM (Total Quality Management) movement. Clear mandates from upper management, backed by appropriate investment in awareness and training, are crucial elements in the defense against information warfare. Robert Hauptman of St.Cloud University in Minnesota is editor of the *Journal of Information Ethics;* in a recent article ("Doing Business Online: Add Ethics To The Agenda" in *InfoWeek* 95.02.06, p. 64), he argues, "It's time to stop accepting illegal activity as the normal price of doing business in Cyberspace." Organizations must identify specific examples of illegal and unethical behavior, define sanctions against perpetrators, monitor compliance, and apply appropriate punishment, including dismissal. Incidentally, it would be a good idea to establish sound security precautions *before* firing people for unethical behavior....

5.3 Expand Fundamental Orientation of Risk Management

Threat and risk assessment has traditionally dealt with the probability of Acts of God. Fire, flood, earthquake, even burglary can be looked at as involving random events. However, in today's competitive and unethical environment, the likelihood of being attacked is an unknown and unknowable function of an organization's attractiveness and preparedness. The most successful and least secure organizations will be victim. Faced with a choice between an unkempt hovel and a palatial residence, a thief will try to rob the more lucrative target. But suppose a thief sees two palatial residences: one has Doberperson Pinchpersons (politically correct guard dogs) roaming the space inside a 3 meter fence, infrared motion detectors and a direct link to a security company; the other has locks on the doors. There's not much doubt about the selected victim.

In my courses, I like to explain the principle of appropriate defense with a story. Two hikers are walking happily along a trail in Alberta when they come upon a huge grizzly bear. Turning tail, they being running down the trail. One huffs to the other, "This is (pant, gasp) crazy. We can't

Copyright © 1995, 2001 M.. E. Kabay *All rights reserved.*

outrun a grizzly bear! They can run 30 km an hour and climb trees!" The other gasps, "I don't have to outrun the grizzly bear (pant, pant). I just have to outrun *you.*"

Organizations must make themselves unattractive targets for espionage and sabotage.

5.4 Increase Military Education and Planning for Information Warfare

The United States National Defense University already has programs in Information Warfare. Canada and other countries should follow suit. Officer training should include a thorough grounding not only in classical military applications of information technology but also in the symptoms of information warfare attacks. Computer countermeasures such as anti-virus precautions, proper quality assurance standards during software development, and anti-penetration techniques should be taught with a conscious awareness of how military systems could be compromised using information technology. Even off-the-shelf software or systems written by consultants could be conduits for information warfare attacks. The military must learn about these threats and be prepared to counter them.

5.5 Encourage Cooperation Between Military and Civil Authorities

Just as emergency preparedness in the world of bridges and roads naturally involves close cooperation between civilian and military authorities, so should emergency preparedness in the world of gateways and networks. Each level of government, each sector and department, should have its Computer Emergency Response Teams (CERTs). These CERTs should cooperate at every level, sharing information and techniques, coordinating their efforts to prevent widening rings of damage from information warfare attacks, and working effectively with their military counterparts.

Winn Schwartau was a guest of honor at the Second International Conference on Information Warfare in Montreal in January 1995. As he wrote in the January 1995 issue of *Security Insider Report,* he chatted with several military officers at the conference. "If Qaddafi (Libya) blew up the Statue of Liberty, what would our response be?" His interlocutors said, "We would... ah, respond." Schwartau went on to question them about escalating levels of attack and then asked, "Let's say that Qaddafi hacked his way into a US computer system and broke it. That is, a complete denial of service. Then what?" The military officers were less certain: "We would probably respond, maybe militarily, but that is a real policy choice." Finally, Schwartau asked, "Fine. Now let's say that the French did the same thing. They hack their way into our financial computers, and as a result, we suffer a major bank collapse. Does that event trigger a military intervention or response?" Apparently the officers were taken aback at this scenario.

Military thinking must include a thorough understanding of all the ways that a foreign enemy can harm a country. And that means understanding the value and vulnerability of civilian information technology. I would like to see military specialists in information warfare taking time to work in commerce, industry and government to gain hands-on knowledge of the role of information technology. I would like to see civilian information technology specialists,

Copyright © 1995, 2001 M.. E. Kabay *All rights reserved.*

including especially technical and managerial employees from telecommunications companies, encouraged to participate in a new kind of military reserve: a Computer Corps specializing in detecting and correcting deliberate damage to information systems, whether military or civilian. I would like to see civilian police authorities cooperating with CERTs and the military Computer Corps to strength the nation's defenses against deliberate attack on the information infrastructure of our society.

5.6 Set National Priorities to Include Information Security

Robert David Steele, another keynote speaker at the Information Warfare Conference last January [1995], has spoken out forcefully on the need for national governments to pay attention to information security. Mr Steele is President of Open Source Solutions, Inc. (Oakton, VA) and has been working on a convincing the government of the United States to establish what he calls a National Information Strategy. His draft proposal presented to the Senate of the U.S. includes the following key points:

- National Information Strategy to be coordinated by the President of the U.S.
- Chief Information Officers to be appointed for federal government and every state.
- National Information Foundation to report to the Chief Information Officer of the U.S.

His proposal includes the following paragraph:

> C4 (Command & Control, Communications and Computer) Security. The substantive elements of this program--connectivity, content and coordination--are all heavily dependent on a relatively fragile national C4 infrastructure. It is the intent of this Act to ensure that all civil communications and computing pathways, including our financial, health care, governance, public information, and defense pathways, are developed in such a way as to maximize their survivability and reliability in the face of attacks by individuals, groups and hostile nations familiar with the critical vulnerabilities of our civil and military C4 infrastructure.

Copyright © 1995, 2001 M.. E. Kabay *All rights reserved.*

5.7 Encourage Mandatory Reporting of Information System Attacks and Failures

We currently lack a clear picture of the state of information technology security in government, industry and private life. As part of a nascent national information strategy, all organizations should share details of every compromise of system security they experience. There should be mandatory reporting coupled with strict protection of sources; a government organization, law enforcement authority, or quasi-autonomous non-governmental organization should receive reports of data leakage, virus attacks, programmatic damage, eavesdropping and electromagnetic interference. It would be impossible and unnecessary to try to force individuals to report their experiences with home computers, but such reports should be encouraged. The agency entrusted with such reports must maintain strict controls over the data to prevent damage to the organizations reporting their own victimization; data could reasonably be anonymized at the time of entry to preclude even inadvertent disclosure of embarrassing details. However, such a national database of computer incidents would be invaluable in evaluating which security measures work and which don't work. With a growing database of knowledge, it should be possible to improve security measures and also to provide hard evidence and case studies to help convince managers to pay attention to security.

5.8 Establish International Agreements on Jurisdiction Over Attacks in Cyberspace

Finally, a systematic effort similar to the Law of the Sea process must be established to define multinational agreements covering computer crimes. Jurisdiction over computer crimes should rest with the federal authorities in the country where the victimized systems are physically located; extradition should be enforced by the authorities where the accused perpetrator has been arrested. Standards of evidence will have to be established; for example, norms for accepting and safeguarding digital evidence will have to be uniform across cooperating jurisdictions. Telecommunications carriers and international value-added networks will play important roles in such cooperation and must be included in the process of policy development.

6 Concluding Remarks

With every development in technology has come new forms of crime and of war. As we move into the twenty-first century, we must take the growing dimensions of cyberspace into account in our defensive strategies as individuals, as members of organizations, and as citizens. With our rapidly growing use of cyberspace, we will experience growing conflict over values: norms that evolved in the world of mail, newspapers and television will collide with those from the world of electronic messaging, newsgroups and multiuser dimensions. As in all human arenas, some of the norms evolving in cyberspace seem to have their roots in alienation and sociopathy. We can hope to protect ourselves in the future not only by countering attacks but by reducing the frequency of such attacks. It is time for society to discuss, determine and express collective values in cyberspace.

Copyright © 1995, 2001 M.. E. Kabay *All rights reserved.*

Chapter Notes

1. Most of these titles are available from the NCSA in Carlisle, PA (call 717-258-1816):

   Bologna, J. (1993). *Handbook on Corporate Fraud: Prevention, Detection, Investigation.* Butterworth-Heinemann (Boston). ISBN 0-7506-9243-X. xii + 308. Index.

   Card, O. S. (1991). *Xenocide.* Tor Books / Tom Doherty Associates (New York). ISBN 0-812-50925-0. xiii + 592.

   Cheswick, W. & S. Bellovin (1994). *Firewalls and Internet Security: Repelling the Wily Hacker.* Addison Wesley (Reading, MA). ISBN 0-201-63357-4. xiv + 306. Index.

   Haugh, J. J. R. E. Burney, G. L. Dean & L. H. Tisch (1992). *Toll Fraud and Telabuse: A Multibillion Dollar National Problem.* Telecommunications Advisors Inc (Portland, OR). ISBN 0-9632634-2-0. 399 + 431 pp.

   Hafner, K. & J. Markoff (1991). *Cyberpunk: Outlaws and Hackers on the Computer Frontier.* Simon & Schuster (New York). ISBN 0-671-68322-5. 368 pp. Index.

   Schwartau, W. (ongoing). *Security Insider Report.* Monthly newsletter on infosec and the computer underground. Inter.Pact, Inc. / 11511 Pine St. N. / Seminole, FL 34642. Tel. 813-393-6600.

   Schwartau, W. (1994). *Information Warfare: Chaos on the Electronic Superhighway.* Thunder's Mouth Press, New York. ISBN 1-56025-080-1. 432. Index.

   Schwartau, W. (1991). *Terminal Compromise* (novel). Inter.Pact Press (Seminole, FL). ISBN 0-962-87000-5. 562 pp. Available as shareware on a disk as well as in print.

   Toffler, A. & H.Toffler (1993). *War and Anti-War: Survival at the Dawn of the 21st Century.* Little, Brown and Company, Boston. ISBN 0-316-85024-1. xiii + 302. Index.

   Stallings, W. (1995). *Network and Internetwork Security: Principles and Practice.* Prentice Hall (Englewood Cliffs, NJ). ISBN 0-02-415483-0. xiii + 462. Index.

2. Internet news group c4i-pro
   The c4i-pro (C4I Professionals) mailing list covers topics of interest to those following developments in information warfare. Here is the list description:
   This mailing list was created for use by anyone interested or involved in the area of Command, Control, Communications, Computers and Intelligence (C4I). Its purpose is to serve as a central point or clearinghouse for (unclassified/non-sensitive) information and activities of interest to members of the C4I professional community. This includes military and government civilian members (both in operational, acquisition and policy

Copyright © 1995, 2001 M.. E. Kabay *All rights reserved.*

positions), C4I contractors and members of the academic community worldwide. Topics of discussion are envisioned to include:

Conference/meeting announcements
Exercise announcements (e.g. JWID)
Lists of C4I resources on the net
C4I thesis ideas and proposals
C4I lessons learned
Generic discussion on such C4I topics as:
- C4I theory
- C4I systems design and acquisition
- C4I system models and simulations
- Information technology security and protection
- C3 countermeasures
- Current C4I topics and issues
- Space and Electronic Warfare (SEW)
- Information Warfare/C2 Warfare
- Cyberwar and Netwar
- C4I equipment effectiveness

The c4i-pro list is managed by students and faculty of the Naval Postgraduate School's (NPS) Joint C4I Systems curriculum. The NPS is the U.S. Navy's graduate education university. More than 1800 students from all four U.S. Services and over 40 countries are studying for graduate degrees in a variety of curricula. The Joint C4I Systems curriculum provides U.S. students from all four services the opportunity to obtain a masters of science degree in systems technology. For more information on the NPS or the C4I curriculum, see our WWW home page described below or contact Ernie Beran at eberan@nps.navy.mil or Dan Boger at dcboger@nps.navy.mil.

To subscribe to the list, send e-mail to majordomo@stl.nps.navy.mil with the single-line message

subscribe c4i-pro <your e-mail address>

where < and > are not included in the message. Thus I subscribed using

subscribe c4i-pro 75300.3232@compuserve.com

3. Information warfare reading list.

Lt. Robert Garigue of the Canadian Department of National Defense published a reading list on information warfare in the c4i-pro news group. It provides a wealth of further reading and I have reprinted it here as published.

Date: Tue, 21 Mar 95 21:00:22 +0000
From: garigue@ncs.dnd.ca
To: 75300.3232@compuserve.com, c4i-pro@stl.nps.navy.mil
Subject: IW Bibliography - public sources

Copyright © 1995, 2001 M.. E. Kabay *All rights reserved.*

As there has been quite a debate as to the definition of IW I submit to the group the small bibliography that I have put together on the subject. They are all from open sources so there is not problem debating the definitions that are found in these documents. You will rapidly realise that there is no such thing as a final definition about something that Karl Popper would clearly class as a world 3 "construct".

If any one wants to add to the biblio send me a note of your documentation or thesis.

This could go into a FAQ

INFORMATION WARFARE - BIBLIOGRAPHY
March 9/95

Advance Planning Briefing for Industry, "Winning the Information War", United States Army Communications-Electronics Command, Fort Monmouth, New Jersey. Symposium held May 11-12, 1994, Ocean Place Hilton Resort and Spa, Agenda and Description of Sessions, 10 pages.

Arquilla, John and Ronfeldt, David, "Cyberwar is Coming!", Article copyrighted 1993 by Taylor & Francis, Bristol, PA, originally published in the Journal Comparative Strategy, Volume 12, no. 2, pp.141-165.

Busey IV, Adm. James B., USN (Ret.), "Information Warfare Calculus Mandates Protective Actions", Presidents Commentary, Signal, October 1994, Official Publication of AFCEA, p.15.

Cook, Lt. Col. Wyatt C., "Information Warfare: A New Dimension in the Application of Air and Space Power", 1994 CJCS Strategy Essay Writing Contest Entry, Lt., 37 pages.

Defense Information Systems Agency, "Defensive Information Warfare (DIW) Management Plan", 15 August 1994, Version l.2, 4 sections and Appendices.

DeLanda, Manuel, "War in the age of Intelligent Machines", Zone Books Swerve edition New York 1991

FitzGerald, Mary C., "Russian Views on Information Warfare", Army, Vol. 44, No. 5, May 1994, pp.57-60.

Franks, Frederick M.. Jr., "Winning the Information War: Evolution and Revolution", Speech delivered at the Association of the US Army Symposium, Orlando, Florida, February 8, 1994, Copyright City News Publishing Company Inc., 1994, 11 pages.

Garigue, Robert. "On Strategy, Decisions and the Evolution of Information Systems". Technical Document. DSIS DND Goverment of Canada.1992

Copyright © 1995, 2001 M.. E. Kabay *All rights reserved.*

Information Society Journal The, Volume 8, Number 1, 1992, Published Quarterly by Taylor & Francis, Printed by Burgess Science Press, Basingstoke, England.

Johnson, Craig L., "Information Warfare - Not a Paper War", Special Report, Journal of Electronic Defense, August '94, pp.55-58.

Johnson, Frederick C and Painter, Floyd C., "The Integration of Warfare Support Functions", Technology Analysis, Warfare Integration, C31:1988, pp.176-182

Kelly AFB, Tex., "EW Expands Into Information Warfare", Electronic Warfare, Aviation Week & Space Technology/October 10, 1994, pp.47-48.

Lum, Zachary A.,"Linking the Senses", Journal of Electronic Defense, August '94, pp.33-38.

Luoma, William M., "Netwar: The Other Side of Information Warfare", 8 February 1994, A paper submitted to the Faculty of the Naval War College in partial satisfaction of the requirements of the Department of Joint Military Operations, 42 pages.

Roos, John G., "Info Tech Info Power", Armed Forces Journal International, June 1994, pp.31-36.

Science Application International Corporation (SAIC), "Planning Considerations for Defensive Information Warfare - Information Assurance -", 16 December 1993, 61 pages.

Sovereign, Michael G. and Sweet, Ricki Dr., "Evaluating Command and Control: A Modular Structure", Technology Analysis, Evaluating C2, C:31 1988, pp.-156-161.

Schwartau, Winn. "Information Warfare - Chaos on the electronic superhighway " Thunder's Mouth Press, New york . 1994

Toffler Alvin & Heiddi "War and Anti War" 1992

//--
// Robert Garigue |garigue@dgs.dnd.ca
// Strategic Information Technology Specialist |Vox 1 613 992 6855
// Office of the Assistant Deputy Minister-DIS |Fax 1 613 992 1469
// Department of National Defense

4. NCSA Information Warfare Conferences

The National Computer Security Association sponsors an annual International Conference on Information Warfare. The First was held in Montreal, September 15, 1993; the Second, in Montreal January 18-19, 1995; the third, in Washington, DC on 6-8 September 1995. The complete Call for Participation for the Third International Conference as published on the Internet follows:

Copyright © 1995, 2001 M.. E. Kabay *All rights reserved.*

From: <winn@Infowar.Com>
Date: Wed, 28 Jun 1995 13:37:24 -0400
Subject: IW 95

InfoWarCon '95
Third International Information Warfare Conference
Confronting Chaos in Cyberspace
Personal, Corporate and National Perspectives
Schedule: June 26, 1995
Sheraton Stouffer's, Arlington, VA

Sponsored By:
National Computer Security Association
Winn Schwartau, INFORMATION WARFARE, Interpact, Inc.
Robert Steele, President, Open Source Solutions, Inc.

Wednesday, September 6, 1995
Registration and Cocktail Reception: (Casual) 17:00-20:00

DAY I: Thursday, September 7, 1995

7:00 - 7:45 Continental Breakfast Sponsored by IBM, Corp.
7:45 - 8:00 Introductory Remarks: Peter Tippett, President, NCSA
8:00 - 8:30 Keynote Address
Speaker of the House, Newt Gingrich (Invited)

"What Is Information Warfare?"

The morning's discussions will be moderated by Information Resources Management College, School of Information Warfare & Strategy, National Defense University. There is no consensus as to what Information Warfare means; everyone has a different definition and application which often suits specific agendas. The morning sessions are to provide attendees with a current review of what Information Warfare means to different people.

8:30 - 9:00 "Threat Analysis: The Intelligence Perspective",
Admiral William Studeman, Asst. Director, Central
Intelligence

9:00-9:30 "The Government Perspective"

How does the government view Information Warfare as the NII and GII become realities? Increasing reliance on technology brings new risks and vulnerabilities along with opportunities. What plans are in place to insure American competitiveness?
- Bruce McConnel, Office of Management and Budget (Invited)

Copyright © 1995, 2001 M.. E. Kabay *All rights reserved.*

9:30 - 10:00 "The Military View"
The military traditionally defends US interests overseas. What is the role of the military in cyberspace where borders are meaningless? How do Information Warfare paradigms fit into the the future plans of the armed services?

- Ambassador H. Allen Holmes, Asst. Secretary of Defense (Invited)

10:00 - 10:30 Morning Coffee Break, Sponsored By: _____

10:30-11:00 "The Financial View"

Technology is the underpinning of the world's economy. Systems availability is key to stability and national economic security. As global economies continue to inter-integrate, major challenges arise. How will we address them?

- Roger Pagak, National Security Advisor to the Secretary of Treasury (Invited)

11:00-11:30 "The Commercial View"

What are the organizing principles for information security and the design basis of information systems and networks? The DII is mandated to provide information services to the war-fighter. The NII initiative is enhancing the economic posture of the US. The infrastructures are inter-related and the loss of either capability could have devastating effect on the economy and security of the United States. The GII will necessarily find similar challenges where all nations must develop a viable means of cooperation. This presentation outlines high level approaches to successful implementation.

The Information Warfare Challenges of a National Information Infrastructure
Ronald A. Gove, PhD., V.P. SAIC

11:30-12:00 "Information Revolution" and "Information Powershift"

The sudden empowerment of the individual in the Post Cold War World changes the view of traditional national security. Info-states arise, and global uncertainty increases. The speakers will address the fundamental paradigm shifts that arise as nations transform themselves into knowledge based societies.

Chair: John Peterson, President, Arlington Institute

- Elin Whitney-Smith, Institute for Change and Learning, George Washington University
- Tamara Luzgin, SPO Information-Based Warfare Modeling Naval Research Laboratory

12:00 - 13:30 Sponsored Lunch: Luncheon Speech 12:30 - 13:00

"Information Terrorism," a special video presentation by Paul Strassmann, former Chief Information Officer, Xerox Corporation and former Director of Defense Information

Copyright © 1995, 2001 M.. E. Kabay *All rights reserved.*

This exciting presentation will be followed with an audience Q&A session.

13:30-14:30 Breakout Sessions:
Class I Meet The Hackers Panel

The underground, denizens of Cyberspace, the first information warriors. Meet them, hear what they have to say about their electronic wanderings. An open, interactive discussion.

Moderated by: Ira Winkler, SAIC
- Chris Goggans, founder Legion of Doom
- Phiber Optik, convicted felon, member Masters of Destruction (Invited)
- Emmanuel Goldstein, Publisher 2600: The Hacker Quarterly

Class II: "Industrial and Economic Espionage - An Update"

What's new in the world or private spying? Front line experts will what's better and what's worse. Who's spying on whom? What are they looking for? What are their techniques and tools? What can you do to protect your organization from being a victim?

Chair:- Jim Settle, Director, I-NET, Inc., former head of Natl. Computer Crime Squad, FBI (The Commercial Perspective)
- Larry Watson, Supervisory Special Agent, National Security Division, DECA Program, FBI
- Bob Friel, Special Agent, Electronic Crimes Branch, Secret Service

Class III "Denial of Service on Information Systems"

Confidentiality and Integrity, two of the three pinions of security have been technically solved with advanced encryption techniques. The third aspect, Availability remains unsolved because of daunting technical problems. What do DOS attacks look like? From the Civil-Cyber Disobedience to Accidental Acts God or Man, a failure of key system components can trigger a domino-like chain of collapses. This session examines the vulnerability of current US infrastructures and the application of such techniques in offensive military applications.

Chair: Larry Merritt, Technical Advisor, Air Force Information Warfare Center
Maj. Gerald R. Hust, USAF (Invited)
"Taking Down Telecommunications"
Maj. Thomas E. Griffith, Jr. USAF, (Invited)
"Strategic Attack of National Electrical Systems.

14:30 - 15:30 Break Out Sessions

Class I "Building a Commercial War Room"
The 'Third Wave' Approach to Managing Information Warfare

Copyright © 1995, 2001 M.. E. Kabay *All rights reserved.*

Maximizing the flow and control of information is key to competitiveness - whether it be on the battlefield or in the marketplace. An innovative tool and approach to planning and managing information in these very intense, time-sensitive environment is the advent of "war rooms." These are dynamic facilities which are optimized to channel the collection, analysis and dissemination of information. 'War rooms' can be static or field-portable and vary in ergonomic layout and technical capability.

This session will provide case studies on the use of war rooms in government and industry. State of the art automated war rooms will be described which feature the projection of computer-generated information. Tools and practices for knowledge discovery, processing and dissemination will help you understand how you go about planning and building a competitive intelligence War Room?

Chair: Steve Shaker, War Room Research
- Mark Gembecki, Technology and Security Oversight Consultant, US Dept. of State
- Dr. Robert Beckman, Alta Analytics, Inc.
- Stewart Silverstone, Graphical Linguist

Class II "Practicing Defensive Information Warfare"
Military lessons for the private sector

This exciting session will show what the military has learned about 'real time' security testing, new security policies and constant testing and vigilance The military has developed an arsenal of tools for penetration and monitoring and alerting users about intrusions. Commercial attendees will learn what life is like without these mechanisms, and how much dramatically more secure they can be with them - with a low increase in overhead. What steps are required to build a defensive posture, and just how much defense is enough?

Chair: Bob Ayers, Defense Information Systems Agency
- Col. John Sheldon, DISA
- Capt. Kevin J. Zeise, USAF, Chief Countermeasures Development, Air Force Information Warfare Center

Class III "Terrorism and Counter-Terrorism"

Terrorist attacks against the US are now occurring on our home ground. What can the modern terrorist do which will meet his goals of sowing fear and distrust? Experience from both the European perspective and the European Space Initiative (their NII) and the American side will demonstrate how infrastructures such as power grids, communications and transportation systems are attractive targets for the terrorist minded Information Warrior. What are we doing in planned response?

Chair: John Sullivan, FBI (Invited)
- SOCOM Rep. (Invited)
- Neal Pollard, "Computer Terrorism and the Information Infrastructure"

Copyright © 1995, 2001 M.. E. Kabay *All rights reserved.*

15:30-16:00 Afternoon Coffee Break Sponsored By: _____

16:00-17:00 "Hackers: National Resources or Criminal Kids "
DEBATE

Germany uses professional hackers for their domestic industrial and economic advantage. What about the US? The kindest words ever uttered by Mich Kabay, PhD, about hackers is, "Amoral, sociopathic scum." Robert Steele, President of Open Source Solutions sees them as national resources, to be cultivated as a tool for US economic security. Do they have a value in the protection of the US infrastructure, or can their specific expertise be found elsewhere? After short opening statements, the audience will be encouraged to ask provocative questions.

Moderated by Winn Schwartau, President, Interpact, Inc.
Robert Steele, President Open Source Solutions.
Mich Kabay, PhD, Director of Education, NCSA

17:00 - 19:00 Cocktail Reception, Hors d'oeuvres, and Band
Sponsored By: _____

Most speakers will be available for more intimate groups chats, and authors will be available to sign books. Great opportunity to pursue those ideas with people from different disciplines.

19:00 - 21:00 Birds of a Feather Dinners

"Dutch" dinners give attendees the chance to dig into more and more depth in areas of their particular interest.
* * * * *

DAY II: Friday, September 8, 1995

7:00 - 8:00 Continental Breakfast Sponsored by: _____
8:00 - 8:30 Keynote: "War and Anti-War in the 21st. Century"
Alvin and Heidi Toffler (Invited)

8:30 - 9:30 "Should the US Spy on the World?"

The US has been the target of economic and industrial espionage by militarily allies and 'friendly' competitors such as France, Japan, Korea, Israel, Germany, Taiwan among others. With an estimated intelligence budget of $30 Billion and arguably the most proliferate and advanced technologies, should we turn our spying 'eyes' on our global neighbors for the benefit of American economic security? Or, are Mom and Apple Pie Americans above that?

Chair: Mark Thompson, TIME Magazine (Invited)
- William Colby, former Director Central Intelligence (Invited)

Copyright © 1995, 2001 M.. E. Kabay *All rights reserved.*

- Thomas Fedorek, Managing Director, Kroll Associates (Invited)

9:30-10:00 "The First Information War: Revisiting Desert Storm"
Lessons in CyberWar for the Commercial Sector and the Military

The US plans a new military strategy of "information war" that assumes an assured ability to dominate knowledge. Knowledge war is absolutely dependent upon spectrum superiority and inviolate software. But, converting cheap and widely available commercial information technology into military capability risks ceding strategic advantage to low-tech adversaries, and, the paradox of a superbly equipped offensive force that also is the most vulnerable to the weapons of information warfare. Desert Storm and other recent military expeditions are examined in the light of evolving definitions and strategies of Cyberwar.

- Alan D. Campen, Col. USAF (Ret.), Contributing Editor, "The First Information War."
Former Director of Command and Control Policy to the Undersecretary of Defense.

10:00-10:30 "CORE WARS: Information Trade Wars"
Practicing Information Warfare in Cyberspace"

As fought today on the Internet, Core Wars represent the purest intellectual tests of pure strategy, tactics and capability. Battalions of software programs must genetically breed themselves for combat knowing that they will go up against fierce competition. Video examples will be used to portray how Core Wars is a working model for Information Warriors on the front lines. New models of Information Trade Wars expand this work as "info-nations" need to develop means to maintain global competitiveness.

Stuart Rosenberg, University of Cologne, Germany
Jo Seiler, University of Cologne, Germany

10: 30 - 11:00 Morning Coffee Break Sponsored By: _____
11:00 - 12:00 Breakout Sessions

Class I "Well Managed Propaganda"

The media is a powerful filter by which citizens and the government collect most of their information. Was the media a puppet of the US in the Gulf War? Does aggressive PR makes media policy? How can the media be used, or protect itself from being used? How can people's perceptions be manipulated to specific advantage?

Moderated by: Neil Munro, Senior Editor, Washington Technology,
- Vic Sussman, US News and World Report (Invited)
- Jim Roberts, SOLIC PSYOPS (Invited)

Copyright © 1995, 2001 M.. E. Kabay *All rights reserved.*

Class II "Threats To Electronic Commerce and Anonymous International Banking"

As the world increasingly relies on electronic commerce, every country, business and individual can be targeted or affected by financial system assaults. This session will examine these threats as well as promising safeguards and countermeasures. The threat of anonymous financial transactions is especially illuminating.

Chair: Mark Gembicki, Security Consultant, US Dept. of State
- Steve Diamond, V.P. Electronic Publishing Resources
- Eric Hughes, Financial Security Expert, co-founder Cypherpunks

Class III "The Legal Consequences of Information War"

What are the legal rights of Cyber-citizens in the US and how do those relate to the laws in other countries? What is the real criminal and civil recourse and remedies to combat industrial espionage? How do we legally handle non-physically violent attacks against the interest of the US on our own soil or overseas? Get the views of the experts.

Chair: - Daniel Kuehl, PhD, Professor, National Defense University
- Air Force General Counsel Representative (TBD)
- Scott Charney, Department of Justice

12:00 - 13:30 Lunch
12:30 - 13:00 Luncheon Speech:
"Export Control As A Proactive Defensive Information Warfare Mechanism"
Winn Schwartau, President, Interpact, Inc.

13:30 - 14:30 Breakout Sessions

Class I "An Electronic Bill of Rights"
Defining Privacy In Cyberspace

How do we as a nation balance the privacy rights of the individual against the legitimate needs of the state, and in sync with the policies of our global trading partners? The views from three differing positions will stimulate a healthy audience-panelist dialogue.

Chair: Andrew Grosso, Former Asst. US Attorney
- Scott Charney, US Department of Justice
- Cynthia Hogan, Democratic Counsel, Senate Judiciary Commitee (Invited)
- Jerry Berman, Executive Director, Center for Democracy and Technology (Invited)

Class II "Defending Against the Internet"

Copyright © 1995, 2001 M.. E. Kabay *All rights reserved.*

The chaotic ravages of the Internet constantly knock at the doors of anyone or any company is connected. What do you have to do to protect your information resources? What have others done? Is it enough and what does the future bode?

Chair: Kermit Beseke, President, Secure Computing Corp.
- John Nagengast, Deputy Chief of Network Security, National Security Agency (Invited)
- Robert Stratton, Security Services Manager, UUNet Technologies, Inc.

Class III Measuring Effectiveness of Theater IW/C2W Campaigns

Success in theater and JTF campaigns demands the full incorporation of C2W and IW. This presentation puts forth the latest research and techniques for modeling and evaluating the effectiveness (MOE) of simulations and real conflicts.

Chair: National Defense University
- Howard W. Clark and Sandra K. Wellfesh, Dynamics Research Corporation

14:30-15:00 Afternoon Coffee Break Sponsored By: _____

(The afternoon sessions will be moderated by National Defense University.)

15:00-15:30 "Protecting Information Resources in Cyberspace"
Lee Sutterfield, Division Chief, Engineering Analysis, Air Force Information Warfare Center

15:30-16:30 "What Is the Role of Government in defending National Economics?"

As evolving global conditions shift competitive value from military might to economic advantage, how should we redefine national security? The threats to the private sector increase and become more likely targets in information warfare of all three classes. What is, and what should the role of the military be in defending US interests both domestically and abroad? This session will provide plenty of opportunity for audience involvement.
- Assistant Secretary of Commerce Larry Irving
- Dr. Barry Horton, Maj. Gen. USAF (Ret.)
- Principle Dep. Asst. SecDef for C4I (Invited)

16:30 - 17:00 "The Future of Information Warfare"

Where do we go from here? After two intensive days of interaction, learning and listening, what's the next step? What do industry and the government have to do to better understand each other? What steps can each take to improve individual, corporate and national defensive postures?
Dr. John Alger, National Defense University

Copyright © 1995, 2001 M.. E. Kabay *All rights reserved.*

17:00 - 17:15 Closing remarks: Peter Tippett, President, NCSA
17:15 - 19:00 No-host reception.

To be kept informed about future Information Warfare conferences, join the NCSA by phoning 717-258-1816 or send the Membership Director e-mail at ssands@ncsa.com any time.

Copyright © 1995, 2001 M.. E. Kabay *All rights reserved.*