White House to Universities:
Tighten Up Security

by M. E. Kabay, PhD, CISSP
Associate Professor, Computer Information Systems
Norwich University, Northfield VT

As I mentioned in the previous report in this series, one of the most interesting lectures at the Sixth National Colloquium on Information Systems Security Education (see http://www.ncisse.org) in Seattle (3-6 June 2002) was a speech by Dick Clarke, the Special Advisor to the President for Cyberspace Security. He stated that cyberspace security would depend primarily on the private sector and that academia will play a vital role in raising the level of security in the United States both in research and in education.

Clarke said, “The national infrastructure protection plan is being written not by bureaucrats but rather by the people in the private sector, universities and state and local governments who are experts in their section of the critical infrastructure. We have asked higher education to participate in this effort. First, help us design the research projects. We inherited the Internet, which does not incorporate security features. We don’t have to accept it as it is; we can rebuild it. We need secure operating systems; Bill Gates says he will devote the resources of this enormous corporation to developing a security operating system. We need redesigned routers. In a billion-node Internet, do we still want to use TCP/IP? Today’s wireless protocols? So one of the elements of the national plan is a research agenda.”

He continued, “The second thing we need from the academic sector is to teach. We have an entire generation of computer users who, in the absence of security education, will continue to make their parents’ mistakes. We will have about 450 cyber-corps scholarship recipients next year; we need ten time that number. We need evidence that the program is effective. We’re looking forward to approval of the Congress for $19B of dollars in increased scholarships.”

Finally, Mr Clarke called for a radical improvement in university computer security: “The third element is securing the universities’ own networks, which are the major source of hack attacks today: probably three-quarters of the total number of attacks. The attacks may not originate there, but most of them jump through them. Perhaps because of a distorted sense of academic freedom, universities do not in general apply strong security measures to their own systems. These enormous networks will continue to be hosts for attacks by hackers and, perhaps, terrorists. Those of you teaching security in universities need to champion security in your own organizations. If the university is a launching pad for attacks, it may cause hundreds of millions of dollars of damage to the national economy.”

Clarke announced that his office has supported setting up an association of university presidents and that he thinks that spending on university security is only 10% of what it should be. He said, “We need to change universities so that they are no longer the worst-secured component of the American economy.”

***
As a university professor, I can affirm that academics are often among the worst violators of what one would think were common-sense rules for protecting information. In a number of institutions, I have seen professors repeatedly leave their office doors open and their laptop computers logged on without any kind of protection – sometimes for hours at a time. Honor code or not, the temptation to students to modify their own grades (and, as camouflage, the grades of some of their peers) must be intense.

What is clear is that universities, like any other organizations wishing to be good Internet participants, should implement at least the following principles for their networks:

1. Firewalls should be configured for egress filtering that prevents all TCP/IP packets with forged origination addresses from leaving the system;
2. Firewalls should forbid entry of all packets with forged origination addresses within the university’s own IP address space;
3. All SMTP servers should be configured to prevent spam relays through those points.
4. Some specific named individual(s) should be explicitly responsible for monitoring appropriate resources (e.g., CERT/CC alerts <http://www.cert.org> or the ICAT Metabase / Common Vulnerabilities and Exposures database <http://icat.nist.gov/icat.cfm>) and patching critical vulnerabilities as appropriate.

As for monitoring and controlling staff, student and faculty use of university computers – university property, after all – discussion groups abound with what seems to me to be denial of the problems caused by irresponsible use of the Internet. Preventing or punishing users for trafficking in stolen music and software, downloading or uploading pornography, or writing scurrilous postings to Usenet groups using their university-assigned e-mail identities are perceived by some in the university community as unacceptable limitations on speech. But this topic is so vast that I will reserve a detailed exploration for a possible later series of articles.

* * *


M. E. Kabay, PhD, CISSP is Associate Professor in the Department of Computer Information Systems at Norwich University in Northfield, VT. Mich can be reached by e-mail at <mkabay@compuserve.com>. He invites inquiries about his information security and operations management courses and consulting services. Visit his Web site at <http://www.mekabay.com/index.htm> for papers and course materials on information technology, security and management.

Copyright © 2002 M. E. Kabay. All rights reserved.

Permission is hereby granted to Network World to distribute this article at will, to post it without limit on any Web site, and to republish it in any way they see fit.