PETER G. NEUMANN

Computer Insecurity

Action is needed on many fronts to protect computer systems and communications from unauthorized use and manipulation.

The wonders of the Internet and the promise of the worldwide information infrastructure have recently reached headline status. Connectedness has become the Holy Grail of the 1990s. But expansion of the electronic network brings with it increased potential for harm as well as good. With a broader cross section of people logging on to the electronic superhighway and with the enhanced interconnectedness of all computer systems, the likelihood of mischievous or even criminal behavior grows, as does the potential extent of the damage that can be done.

But in spite of the higher risks and higher stakes, little attention has been paid to the need for enhanced security. The stories that appear in the press from time to time about prankster hackers breaking into a computer network or computer viruses infecting government systems focus more on the skill of the culprit than the harm done. The popular assumption is that break-ins are relatively harmless. Most computer users complacently believe that if there was real cause for alarm, government or corporate computer experts would recognize the problem and take appropriate action.

Unfortunately, experts and neophytes alike have their heads in the sand on this issue. In spite of repeated examples of the vulnerability of almost all computer systems to invasion and manipulation, very few people recognize the magnitude of the damage that can be done and even fewer have taken adequate steps to fix the problem.

Peter G. Neumann is a principal scientist in the Computer Science Laboratory at SRI International in Menlo Park, California. His new book, *Computer-Related Risks* (ACM Press/ Addison-Wesley, 1994), discusses reliability and safety problems as well as security.

Electronic mail is vulnerable to various types of mischief. Messages can be intercepted in transit, altered without the sender's or receiver's knowledge, and then delivered. Or someone could simply concoct a message and send it so that it appears to be coming from someone else. On April Fools' Day 1984, the Internet carried a message allegedly from then Soviet Premier Konstantin Chernenko announcing that the USSR had joined the Internet and that he looked forward to increased interactions and peaceful coexistence. (The originator of the spoof later made available the entertaining collection of responses to the message.)

The passwords used by individuals to gain access to systems can be stolen while stored or while in transit, either within a system or a local network or across a global network such as the Internet. Even many of the encrypted passwords now in use are not safe enough to prevent theft. Viruses can be planted to disrupt the normal operation of software, and "Trojan horses" can be embedded in systems to perform automatically what the attacker does manually—from intercepting messages and stealing passwords to copying or altering data and modifying other programs. An attacker can even modify a compiler in such a way that, with almost no visible signs, the system login program would contain a trapdoor for his subsequent use.

And each system break-in opens the door to wider and deeper penetrations. A company's system may be relatively secure against direct attack from outside but quite permeable to attackers who have entered a less secure system at an affiliated company with a computer linkup.

The simple reality is that commercially available system and network security has not improved sufficiently during the past five years. Connecting a system to the Internet is tantamount to offering an open invitation for intrusions from the world at large. We should not be surprised that since the fall of 1993, reports of Internet system penetrations have been increasing rapidly.

The systems directly connected to the Internet are not the only potential victims. Any system with dial-up access or with indirect access from another system that is connected to an accessible system can also be compromised. Even stand-alone personal computers can be compromised by computer viruses transmitted by contaminated floppy disks.

It doesn't take too much imagination to envision what could happen given the ease with which system security can be broken. Think of all the critical activities in our society that are governed to some extent by the operation of computers: nuclear power plants, telephone networks, production processes for dangerous chemicals, transfers of money, air traffic control, and credit card transactions, to name just a few. The first generation of prankster hackers was indeed more mischievous than malicious—breaking into a system was the primary goal. But the absence of serious damage has lulled computer users into a false sense of security.

Conditions are changing in ways that should cause concern. At the same time that the world's computer systems are becoming ever more interconnected, the tools for breaking in are becoming widely available on computer bulletin boards and in attacker tool kits. More people will be able to break in, and accomplishing this feat will be less satisfying. We are more likely to find people breaking in for profit and other less benign motives. Only a fool would be willing to trust the integrity of every person with a computer and a modem.

Connecting a computer system to the Internet is tantamount to offering an invitation for intrusions from the world at large.

Nothing new

This is not a new problem. On Sept. 19, 1988, the National Research Council's Computer Science and Technology Board (CSTB)—now the Computer Science and Telecommunications Board—held a meeting on computer and communication security at which Robert Morris (then of the National Security Agency) noted that "to a first approximation, every computer in the world is connected with every other computer." K. Speierman, Morris, and I each gave stern warnings that day that the state of the art in computer and network security was generally abysmal and not noticeably improving.

A few weeks later, a Cornell University graduate student provided vivid evidence of how vulnerable computer systems were to attack. He unleashed a program dubbed the Internet Worm that caused several thousand computer systems on the Internet to grind to a halt. His program did more harm than he intended and thus demonstrated how vulnerable networked systems can be to accidental runaway programs as well as to intentional penetrations.

That incident spawned much discussion and analysis. Several emergency response teams were formed to take action to improve security and prevent future incidents. Unfortunately, most computer system administrators did little more than patch a few of the obvious holes exploited by the Internet Worm. Meanwhile, the CSTB formed the System Security Study Committee to look more closely at system vulnerability. The committee report, released in December 1990 as *Computers at Risk*, found that system security was still inadequate and made various near- and long-term recommendations for improvement.

In the four years since then, some progress has indeed been made. In particular, there is a noticeable increase in the awareness levels on the part of users and administrators. Some of that report's short-term recommendations have found their way into practice. For example, private sector and government officials are paying more attention to security policy, system designers and managers are beginning to implement authentication and access controls, software developers are applying a broader range of security techniques, and emergency response teams are honing their skills. Still, vulnerabilities dramatically outnumber known fixes.

In addition, the government has not funded research that the report says is necessary to ensure security for more advanced and widely distributed computer systems. In fact, the government has actually hindered the progress that could be made through better encryption of messages by enforcing export controls on encryption technology. The absence of a global market weakens the economic incentive for U.S. companies to develop better products.

In general, neither the computer industry, computer users, nor policymakers are acting as if they fully understand the seriousness of the problem.

Defense, defense

Security is improving in some areas, but to achieve an adequate level of protection will require coordinated action. In most conventional systems and networks, a single weak link may be sufficient to compromise the whole. Therefore, progress is necessary on all fronts. Gateways and firewalls are useful stopgaps in isolating systems from bad effects.

The use of encryption could significantly improve electronic-mail security in three fundamental ways. First, messages can be encrypted so that the receiver would have to have a "key" to decipher the message. An additional layer of protection could come from the adoption of single-use encryption keys that would be of little use if stolen. Second, messages can be augmented with integrity seals that would make it easier to detect tampering or with an encoded digital signature that the receiver could verify. Third, system-to-system and user authentication employing cryptography or other techniques can block messages from unauthorized systems and thus make it harder to send counterfeit messages.

Use of encryption is increasing, but the quality of the techniques could be better. Easing export controls on sensible encryption technology to create a larger market would create a powerful incentive for U.S. firms to invest more in the development of encryption.

New incarnations of certain popular computer operating systems such as Unix are correcting earlier security flaws that made it too easy to break into a system or network. Other operating systems such as MS-DOS are still limited in the security they can attain, particularly in distributed environments. Unfortunately, new systems also typically introduce new security shortcomings that will eventually have to be fixed.

Successful implementation of these security measures requires knowledgeable system and network administrators and operators, as well as rigorous enforcement of operating procedures. The slightest deviation from such procedures can result in a breach of security. Too often, system administrators undermine the security features of their own systems through inaction or inadvertent actions. Today, training for administrators and operators is haphazard at best.

Improvement in these areas is a necessary but not sufficient first step. Maitaining security will require constant improvement in all aspects of computing and communications. The impetus for such steady progress should come from market demand, but for now the market is not sending a strong signal. Because so many computer users and system administrators are not sufficiently aware of the vulnerabilities of their systems, they are not demanding more secure systems from vendors. System developers do not generally perceive security as a bottom-line source of profit and find few incentives to produce systems whose operations can be significantly more secure. Even when researchers develop new security technologies, it can take a long time before these advances find their way into products. We need to identify ways to stimulate progress.

Easing export controls on encryption technology to create a larger market would provide a powerful incentive for U.S. firms to invest more in the development of encryption.

Collective action

Action can begin by completing the implementation of the recommendations made in *Computers at Risk*. More effort is needed to pursue relevant research and development on computer systems and networks that can be secure, reliable, highly available, and generally resistant to misuse.

- We need an information campaign to make computer users and system administrators more aware of how vulnerable their systems are to attack so that they will be motivated to employ defensive techniques. This must be a shared responsibility among vendors, customers, universities, and government organizations.
- System developers must recognize that although the market is not demanding more secure systems, buyers are likely to be upset when they discover how vulnerable their systems are. Developers should anticipate the need for more secure and more easily administered systems. They may be able to stimulate demand for more secure systems through advertising, or they can wait to reap the benefits in future sales

when buyers come to appreciate the value of more secure systems.

- System evaluators (government and private) must raise their security standards, which now reflect a lowest-common-denominator approach. The Information Systems Security Association is pursuing the development of a set of information systems security principles, as proposed in *Computers at Risk*.
- President Clinton has recently taken the lead in working with the Departments of State, Defense, and Commerce to relax export controls on many high-technology products. There is some progress in adding modestly secure encryption technology to the list of products whose control may be doing more harm than good. (A new National Research Council review of U.S. encryption policy is just beginning.)
- Legislators must realize that current computer-crime laws are not sufficient to deter break-ins. Federal and state laws are under review.
- Law enforcement agencies need to devote more effort to identifying computer crimes and pursuing those people responsible for them. But we should be realistic about the limitations of legal measures. Violations of computer security are difficult to detect and prosecute. Better laws and more effective enforcement will help, but there is no substitute for better system and network security, better education, and greater awareness.

We know a great deal about what must be done to enhance computer security. Putting it into practice will require an increased sense of urgency among the computer users, system developers and administrators, government officials, and educators followed by a coordinated effort to ensure that all links in the fence are strong.

Recommended Reading

W. R. Cheswick and S. M. Bellovin, *Firewalls and Internet Security*. Reading, Massachusetts: Addison-Wesley, 1994.

D. D. Clark et al., *Computers at Risk: Safe Computing in the Information Age*. Washington, D.C.: Computer Science and Technology Board, National Research Council, National Academy Press, 1990.

P. J. Denning (ed.), *Computers Under Attack: Intruders, Worms, and Viruses*. New York: ACM Press/Addison-Wesley, 1990.

M. Gasser, A. Goldstein, C. Kaufman, B. Lampson, "The Digital Distributed System Security Architecture," *Proceedings of the 12th National Computer Security Conference (Oct. 10-13, 1989)*. Gaithersburg, Md.: National Institute of Standards and Technology. 1990.

K. Hafner and J. Markoff, *Cyberpunks*. New York: Simon & Schuster, 1991.

L. J. Hoffman (ed.), *Rogue Programs: Viruses, Worms, and Trojan Horses*. New York: Van Nostrand Reinhold, 1990.

S. Landau, S. Kent, C. Brooks, S. Charney, D. Denning, W. Diffie, A. Lauck, D. Miller, P. Neumann, and D. Sobel, *Codes, Keys, and Conflicts: Issues in U.S. Crypto Policy*. New York: Association for Computing Machinery, June 1994. A summary of this report by the same authors is available as "Crypto Policy Perspectives" in the *Communications of the ACM* 37, no.8 (August 1994): 115-121.

R. Morris and K. Thompson, "Password Security: A Case History." *Communications of the ACM* 22, no.11 (November 1979): 594-597.

P. G. Neumann and D. B. Parker, "A Summary of Computer Misuse Techniques," *Proceedings of the 12th National Computer Security Conference (Oct. 10-13, 1989)*. Gaithersburg, Md.: National Institute of Standards and Technology, 1990.

Cliff Stoll, *The Cuckoo's Egg: Tracking a Spy Through the Maze of Computer Espionage*. New York: Doubleday, 1989.

K. Thompson, "Reflections on Trusting Trust" (1983 Turing Award Lecture) *Communications of the ACM* 27, no. 8 (August 1984): 761-763.