Viruses and worms: What to do?

Galen Gruman, Soft News Editor

Programs written to cause damage and multiply in computer systems and networks are not new. In fact, some — such as the Pakistani Brain, Scores, and nVir — have plagued several networks and software producers in the US and Europe for several years. Japan experienced its first virus attack on a network last September (see the box on p. 96).

But, because of the publicity about the Nov. 2 Internet worm attack that shut down 6,000 computers and about subsequent, unrelated attacks on Milnet, the public is now aware that computers and their data are not necessarily secure.

Reaction. Since the Internet attack made front-page news, many agencies — private and public — have condemned such attacks and considered ways to prevent them:

- Professional societies have condemned those who introduce worms and viruses. (The box on p. 94 defines these terms.) Several, including the Computer Society, have suggested penalties such as professional censure and criminal prosecution and have recommended that ethics be part of the college computing curriculum. The Computer Society's Committee on Public Policy was drafting a policy statement with such recommendations as this issue went to press.
- Congress is considering a bill, HR 55, sponsored by Rep. Wally Herger of California, that would add people "interfering with the operations of computers through the use of programs containing hidden commands that can cause harm" to the list of criminal violations covered by Section 1030 of Title 18 of the US Code. It also lets victim sue for civil damages. (The box on p. 95 covers how current law applies to such actions.) One congressman, Peter Stark of California, cosponsored the bill after his office's Macintosh became infected with a virus.

The proposed law would be tougher than the existing 1986 Virus Abuse Act, said Doug Riggs, Herger's legislative assistant. Under the 1986 law, "if there is no specific damage, there is no way to prosecute," he said. Some states — notably Michigan, Texas, and Washington — have effective laws to deal with attacks on computers, Riggs said. California is working on one of its own and Minnesota is overhauling its law, he said. But most states have no comprehensive laws on computer crime. "We would like to see HR 55 enacted so we have some national uniformity," Riggs said.

- The Defense Dept. set up a Computer Emergency Response Team at the Software Engineering Institute in Pittsburgh. Once put together from experts across the country, the team of about 100 people will advise users of infected computers on research networks. The intent is to "avoid scrambling at the last minute" in another attack, said SEI's Susan Dunke. The many operating systems, mail systems, and hardware platforms in use makes the task difficult, she said. A long-term goal is to look at security methods, not just react to crises, Dunke said.
- However, no major changes are expected to the ARPAnet or Milnet networks because of the Internet worm attack, said Defense Dept. spokesmen. ARPAnet "was not designed for security," said spokeswoman Jan Bodanyi. "It was designed for the research community and is thus as open as you can get," she said. Milnet was likewise vulnerable, said spokeswoman Susan Hansen. The networks' very openness is vital to encourage and accelerate research, they said. "You have to take a risk," Hansen said.

Everyone interviewed for this report about protecting networks stressed the need to balance the risk of virus attack against the benefits of open, easy communication. "I'd be most dismayed if such attacks continued and forced a more restrictive policy," said Eric Auperle, principal investigator at Merit, the Ann Arbor, Mich., consortium that manages the National Science Foundation-supported NSFnet, which serves as a high-speed, broadband backbone link for regional networks. (As only a transporter of data, NSFnet was unaffected by the Internet worm.) "The academic institution's lifeblood is the free flow of information," said David Wasley, manager of data communications and network services at the University of California at Berkeley.

Furthermore, the costs of stringent protection could be prohibitive, the Defense Dept.'s Hansen said. Such high costs are justifiable for networks carrying classified information, and these networks do have stringent protection mechanisms, she said. The Defense Dept. plans to replace ARPAnet with a new network called the Defense Research Internet. DRInet will "balance the special [openness] needs of the research community, cost, and security," Bodanyi said.

- The National Science Foundation's 1990 budget request includes funds to support research and development on network security, said Jeffrey Nohrs, an NSF spokesman.

Overreaction? With the focus on computers' vulnerability, some worry that the public will lose trust in their data.

Kenneth King, president of the Educom consortium that owns the Bitnet research network, wrote in the *Chronicle of Higher Education* and *Educom Bulletin* that an overreaction to such attacks could discourage research organizations from using networks and government agencies from sufficiently funding the development and operation of networks.

An ongoing focus on viruses could mean that "the basic issue of trust will be dissipated from corporate America," said Michael Riemer, chairman of the Software Publishers Association's newly formed special-interest group on viruses.

Problem's extent unknown. "The problem has increased in the last two or three years," congressional aide Riggs said. "We think it is a serious problem," he said. However, there is little data about the frequency of attacks or whether the rate is increasing, he admitted.

Most virus attacks occur on microcomputers, said John McAffee of the Santa Clara, Calif.-based Computer Virus Industry Association, which represents 22 companies. "The Internet infection was an anomaly," he said, "The vast majority of infections are in the PC world. The main threat they pose is in the PC world."

Since May 1988, the association has received more than 430 reports of virus attacks that affected 10 or more computers per incident, McAffee said. However, the actual number is unknown because "when infected, [private companies] do not want any attention paid to them" for fear of losing customers, he said.

The number of cases reported to the Federal Bureau of Investigation from 1985 through 1987 was only 22, said Ken Walton, a deputy assistant director in the criminal-investigative division at the FBI headquarters in Washington, D.C. "Most of these have been hackers [and] kids," he said. However, the FBI's jurisdiction is narrow, Walton said: It is limited to computers connected to a federal agency, to a federally insured bank or depository, or used for interstate commerce.

For those cases that are reported to the FBI, it is difficult to find the perpetrator, and even more difficult to prove intent or damage, Walton said. "There's [often] no crime scene [and] loss of computer time is not a federal violation," he said.

Closing Unix's loopholes. In the November Internet attack, two features in BSD Unix's Sendmail program that are not normally used together — remote debugging and interactive use on a local system — were combined to let the attacker send the worm as a mail message and then get Sendmail to compile the worm code so it could infect the compiling machine. Network nodes using other operating systems were not vulnerable to the worm's attack. "It used all those neat things people put in to make their jobs easier," said Keith Bostic of the University of California at Berkeley's Computer Systems Research Group, which manages BSD Unix. "User convenience is worm convenience," he said.

Berkeley issued a binary fix within days of the attack and a source-code fix in late January. "We found four or five other ways to break it and we think we've fixed all those," Bostic said.

Berkeley is now considering whether to audit the entire BSD Unix operating system for code that people might exploit to introduce a virus or worm. The effort would take two to three man-years, Bostic said, and will be complicated by the lack of modularity and documentation. "Sendmail is proof that a big and single module doesn't work: No single person can understand it," he said. But even with the auditing effort, "how do you handle every possible permutation?" Bostic asked.

One change that the group will make to BSD Unix is to use shadow passwords, which means that the encrypted form of the password is no longer available for decoding, Bostic said.

Because Unix's openness and vulnerability to attacks was long-recognized, the National Security Agency, which manages electronic surveillance and cryptography operations, began an effort in early 1988 — since it was then clear that Unix was becoming popular in government systems — to develop guidelines for Trusted Unix. "Unix has proven to be very portable, but it has proven *not* to be very secure," said Mike Testa, a Trusix participant from Infomation Technology, a Greenbelt, Md., research firm.

The Trusix recommendations are expected to be released by early 1990. The guidelines will be available through the National Institute of Standards and Technology. The Trusix guidelines focus on trust technology, which ensures that "the data you see is the data you were cleared to see," Testa said.

Participants in the Trusix effort are the NSA's National Computer Security Center, AT&T, Sun Microsystems, Harris, Gemini Computer Systems, the Institute for Defense Analyses, and Information Technology. The participants were limited to vendors working on B-level systems, Testa said. To be classified as B-level, computer systems must enforce data protection through mandatory access control and data labeling. The Defense Dept. has directed that all its systems meet at least C2-level requirements by 1990, which would give them discretionary protection.

When the Trusix effort began, there was some question about whether Unix could support B-level security, Testa said. The question was "How far can you stretch Unix so it will still be Unix?" he said, but "it seems fairly clear that [the] B2 [level] is achievable."

Other technical changes. Whatever the operating system used, "we need automatic load shedding," said Mike Roberts, Educom's vice president for networking. "We need to kill a runaway Ethernet

Electronic infections defined

Many common computing terms are based on allusions to everyday things — mice, hosts, memory, scroll bars, and almost everything associated with object-oriented programming come to mind. The terms for breaking-and-entering techniques are no different. Here are some definitions of terms that data-security questions have made popular:

- Back door. *See the second definition of "Trojan horse."*
- Bomb. An event-triggered routine in a program that causes the program to crash.
- Hacker. Someone who almost religiously seeks every opportunity to decompose a program or system. The term has negative connotations because of the hackers who enter other people's systems without permission and often intentionally cause damage. While the underlying motive is the same as any scientist or engineer has — to see how things work and test their limits — a hacker often disregards the effects of his actions on others. The term's original connotation — someone, perhaps a social misfit, who is obsessive about programming and learning how systems worked but who in the process becomes a master of the art — is rapidly falling into disuse.
- Trojan horse. This has two meanings.

1. It is a seemingly benign program (often downloaded from a bulletin board or copied from a disk that is widely circulated) that includes a bomb, virus, or worm routine.
2. It is a back door into an operating system or other systems-level component that someone can take advantage of to sneak into an operating system's internals or account information. An example is a program that mimics the actions of the system login program on an idle terminal. When an unsuspecting user logs in from that terminal, the program captures the account information and password and then feigns a login failure and exits to the real login program, giving its creator access to other accounts.

- Trap door. *See the second definition of "Trojan horse."*
- Virus. A program or program fragment inserted into another program. It is activated by its host program, replicates itself, and seeks new hosts to infect. Computer viruses spread the same way biological viruses do: by contact. A virus routine infects data or programs each time a user runs an infected program or interprets infected data in a way that the virus can take advantage of to replicate itself. Because a virus is usually embedded in a legitimate program or data, the system considers it to be a legitimate entity and thus gives it whatever privileges the infected host has — just as a virus slips through the body's defenses by incorporating itself in the body's cells.
- Worm. A self-contained, self-propagating program that works its way through a system, often intentionally causing damage. Unlike a virus, it needs no host program to activate it. Like a virus, it may replicate and enter other systems. The name apparently comes from "tapeworm," which science-fiction writer John Brunner used in his 1975 book *The Shockwave Rider* to describe programs that sapped a host computer's resources and spread themselves to other machines.

The definitions of a virus and a worm in both the technical literature and casual conversation are often contradictory. The main difference is that a worm is self-contained while a virus is not. So what was the cause of the now-infamous Internet shutdown of Nov. 2-3: a virus or a worm? It entered the system as a mail message, tricked the responding mail system into compiling the message (which was actually an uncompiled program), and then, once compiled, dialed out from the newly invaded host to get the rest of itself copied into the new host. Because it was self-contained, it is properly a worm. If it had integrated itself into the mail system software, it would have been a virus.

—Galen Gruman, Mike Lutz, and Paul Oman

[link]," he said, to stop the traffic that spreads the virus or worm. Without automatic load shedding, too much demand in one area can knock out communication throughout the network, Roberts said. For example, the electrical brownouts in New York in the early 1970s were caused by an inability of the power utilities to automatically shed load, he said.

Furthermore, "networks should offer an easily accessible node-to-node encryption," Roberts said. A future version of BSD Unix will require MIT's Kerberos encryption for sensitive data like passwords when transferred by Ethernet links, which are easily tapped because Ethernet is a broadcast system, Berkeley's Bostic said. Users will have an option to encrypt everything, he said, "but the overhead is tremendous."

Safe computing. "The whole virus issue is just exploiting the whole security and management problem on PCs," said the virus SIG's Riemer. "You're inviting trouble the more you connect," he said, but the move toward connectivity means that staying unconnected is increasingly unacceptable. "There are thousands and thousands of nodes on the Internet. We're connecting as fast as we can, and that will continue," Berkeley's Bostic said. "But we're also continually improving the security," he said.

The long-term solution to virus attacks is better management, Riemer said. "You can take certain precautions to limit your risk," Riemer said, just as is in diseases: "Not everyone in the US is going to stop having sex because of a fear of AIDS."

The following safe-computing practices are based on interviews with network managers, representatives of industry associations, and reports from the Congressional Research Service, Computer Virus Industry Association, Foundationware, and MIS Training Institute.

- Determine the risk/benefit ratio of open communication. Vital systems should have higher protection than nonvital ones. "You need to come up with an optimal trade-off for secrecy, functionality, and integrity," said Fred Cohen, a long-time virus researcher, at a Dec. 5 workshop on viruses for DP managers. "It's a lot like a lock on your door: It won't prevent someone with an assault rifle from coming in and killing you," said Berkeley's Bostic. "But you don't hire a Marine to sit in your living room" as a guard, either, he said. "In university research, you can annoy someone [by introducing a worm and causing data loss] but the value of data is not that high" compared to that in a banking military network, said Wasley, Berkeley's network-services manager.
- Never boot from any floppy disk other than the original, write-protected disk. If you have a hard disk, never boot from a floppy.
- Write-protect all program disks.
- Back up data. But be aware, Cohen said, that for some viruses "backups tend to be a safe harbor — a backup will have a good copy of the virus. They protect users from our attempt to remove them. Even if you clean up a system, you're not necessarily preventing its return."
- Disallow passwords like "Mom" and "Password." Encourage mixed-case passwords, but don't make them so complex the user must write them down — "that's the worst thing possible," Wasley said.
- Validate the source of all software and data received before using it. Introduce new software — especially software obtained through easily modified routes such as shareware and bulletin boards — to an isolated machine for testing. (Bulletin boards are a frequently cited source of infected software, but Cohen said they are actually not a major source.)
- Keep source code isolated from other code or data. Restrict access to that source code. Consider environments that restrict the directories from which programs may execute, since this reduces the chance of a virus being run even it does get copied to your system. Good change control over source, executable, and data files through a trusted channel "is the state of the art in virology now," Cohen said.
- Limit sharing. Cohen recommends basing information flow on partially ordered sets, which let the information go only where it needs to go. It also helps pinpoint the sources of viruses, he said.
- Limit the interpretation of data. Flexible interpretation means someone can exploit the interpreter by manipulating the data it uses.
- Limit functionality. "If we didn't have general-purpose functionality, we could limit people's ability to get infected," Cohen said. But PCs and networked systems work against this approach, he said.

Role of ethics education. Teaching ethics to computer-science students as a way to combat viruses is a frequent suggestion. However, "you can't make bad people good," said Deborah Johnson, a professor at the Science and Technology Studies Dept. at Rensselaer Polytechnic Institute in Troy, N.Y. "Everybody who plants viruses knows what they're doing is bad or that no one will like it," she said. "Would taking a course in ethics change their behavior? Probably not," Johnson said. And, she added, "I can't do much with people who want to be unaware."

An ethics class is not meant to indoctrinate students to follow preferred patterns of behavior, said Michael McFarland, a professor at Boston College. It is a "misconception" that ethics are merely a set of rules, he said. "In a course, you can give students a methodology for thinking about these problems," he said.

The focus of such classes is on the social implications of computing, such as privacy and ownership issues, not just narrow issues like viruses. Johnson estimated that 20 to 30 colleges offer such courses.

For Johnson, the larger issues are that "we glorify the successful criminal of any kind" and the attitude that "your intelligence puts you in this elite class with special privileges," she said. The solution is to "encourage people to see [computing] work as part of a profession" and to show them "with their special knowledge comes special responsibility," she said.

Japanese face first virus attacks

While computer viruses are not new to US or Europe, they are new to Japan. Japan's first reported virus attack occurred in September. It spread through NEC Corp.'s 50,000-member national PC-VAN network and through a small local network, said Hideki Ikuta, assistant general manager of NEC's Information-Services Engineering Dept. The virus infected only NEC PC/9800 computers running MS-DOS — the most popular type of PC in Japan, he said.

The virus monitored logins to PC-VAN and stored passwords on the bulletin board for retrieval by the yet unknown person who introduced the virus, Ikuta said.

NEC issued a report about the virus that urged users to follow safe computing practices, recommended development of a vaccine for it, and recommended enhanced network security features such as disallowing consecutive illegal sign-ons and a safeguard procedure during password modification.

The Japanese Ministry of Posts and Telecommunications and the Ministry of International Trade and Industry have also set up task forces to investigate viruses. The MITI group's preliminary report is due this month, said Hideo Nakanishi, director of the Information-Technology Promotion Agency's Software Technology Center, the MITI division that handled the virus investigation. The task force will be expanded and given several hundred thousand dollars in funding as of April, he said. The expanded committee will investigate technical and legal issues, he said.