Students Discover Computer Threat

The discovery of a simple but powerful way to break into computer systems poses a problem: who should be told of the threat and how?

About 6 months ago, a group of undergraduate students at the University of California at Berkeley made an alarming discovery. They found an extremely simple way to break into computer systems—a way that, according to Charles Wood, a computer security expert at Stanford Research Institute (SRI), makes passwords obsolete. "In computer science we use the word elegant to mean powerful and simple. The threat these students discovered is very elegant," Wood says. "We believe it to be the most serious computer security problem we have encountered."

What the students discovered is a way for a person who is legitimately logged onto one terminal in a time-sharing computer system to trick the computer into thinking he is another user logged in at a different terminal. He would thereby gain access to all the privileges of the user he impersonates, such as access to the second user's files, the ability to modify or delete information from those files, and the ability to execute the other user's programs. "An otherwise innocuous feature of many computer systems, the ability to determine who is logged in at a particular time, is necessary for this method to succeed," says Wood.

The Berkeley students, realizing the serious implications of their discovery, passed word of the method to other students who told faculty members. They, in turn, told M. Stuart Lynn, the director of computing affairs at the university, who took the problem to the computer experts at SRI.

Wood and SRI systems programmer Scott Kramer tested the method and confirmed that it was a serious threat to the integrity of time-shared systems. The SRI computer experts believe that not only the widely used operating systems of the type in the Berkeley computer but also other very popular systems are vulnerable. The weakness that the method exploits is in the computer terminals, which communicate with the operating systems. And, says Wood, "this particular feature is part of the terminal and is used by manufacturers to sell terminals."

According to Wood, there are a number of ways to prevent this sort of attack, but all involve some expense. One is to add a new circuit to the programmable read-only memory in the computer terminals. Another is to alter the computer network so that it scans all information passing between terminals and deletes certain characters when it sees them. The operating system could also be modified to prevent certain types of terminal-to-terminal communication. Or the users of applications programs, like payroll or accounts receivable, could be prevented from using a particular way of communicating with the computer.

The SRI group pondered what to do. "We always wondered what would happen if someone found a way to compromise large systems of computers. Now someone has and we don't know what to do about it," says Donn Parker of SRI. "We have no formal mechanism to disseminate this information," says Wood. "It also is a sticky legal problem. Are manufacturers liable for having vulnerable terminals? Are they obligated to fix their computers? Are we liable for not notifying everyone who could be affected?"

The SRI computer experts decided to approach the computer manufacturing and trade associations and also the National Security Agency (NSA). Wood spoke to the presidents of the Computer and Communications Industry Association (CCIA) and the Computer and Business Equipment Manufacturers Association (CBEMA). The SRI group also gave out a paper, describing the method in detail, to any person who had a legitimate need to know.

CBEMA made sure its members were aware of the threat, and strongly encouraged them to modify their computer products if necessary. Jack Biddle, the president of CCIA, says that when the SRI group told him of the method, he flew Wood to the next meeting of CCIA chief executives so Wood could tell them of the threat. "I consider it my responsibility to be sure my members are in the leading edge of any new technology. This is one I thought they ought to know about," Biddle remarks. So far, says Wood, he knows of only one manufacturer who has taken any action. That manufacturer is now offering a $60 attachment to the read-only memory of its terminal to deflect the threat.

The National Security Agency assumed a matter-of-fact attitude. Colonel Roger Schell, deputy director of the NSA's new computer security evaluation center, explains, "Our reaction was a little bit different from their's [SRI's] from the standpoint that to us this is just another one of a class of vulnerabilities called Trojan horses." In fact, Schell notes, the particular technique that the SRI group finds so disturbing was discovered independently by the Air Force in the early 1970's.

When the problem was brought to Schell's attention by the SRI group, however, the NSA looked at its own computer users and decided they would not be affected by the vulnerability. All the NSA employees have security clearances and so, presumably, would not maliciously break into each other's terminals. But the NSA did not tell its employees of the threat. "They would be better off not having that kind of information," says Schell.

> The SRI group says, "We believe it to be the most serious computer security problem we have encountered."

"I share their [SRI's] general concern for the lack of security in computer systems," says Schell. "We believe that all computer security problems are serious and this one is as well. But this is just one of numerous sorts of concerns. Trojan horses are insidious sorts of things."

Asked what he would advise a group like SRI to do when a vulnerability is discovered, Schell said that the NSA has discussed such problems at length. "Although we are generally committed to sharing information, we would not share vulnerabilities. We shared our views when approached by SRI but we did not

0036-8075/82/0305-1216$01.00/0

and would not have initiated such open discussions," Schell remarks.

The SRI group, in its attempts to behave responsibly, had hoped to keep the news of the computer network vulnerability confined to manufacturers and users who had a legitimate need to know. But a reporter for a computer trade newsletter, *InfoWorld*, found out about the method and 2 months ago told the SRI group that he planned to publish a report on the discovery. Parker and Wood dissuaded him from publishing specific details, but now it may be too late to stop the method from being widely known.

The *InfoWorld* story appeared on 11 January. Already, computer hacks, communicating on electronic bulletin boards—widely available computerized message centers—are speculating on what the method may be and are passing on to each other weaknesses in various computer systems. Once it is known that a simple method exists that allows one user to masquerade as another in a time-sharing system, it is only a matter of time until someone finds the method.

So here is a situation in which everyone involved made every attempt to find the right thing to do, and in which the end result will most likely be the one that everyone was trying to avoid. "I just want you to ask your readers," Wood said to *Science*, "what should we have done?"—GINA KOLATA

U.S. Considers Ocean Dumping of Radwastes

EPA is revising its regulations on ocean dumping; critics charge this may pave the way for dumping low-level waste

After a pause of almost two decades, the United States could soon resume dumping radioactive materials into the oceans. The Navy has already expressed an interest in getting rid of the radioactive reactors of old nuclear submarines by scuttling the vessels in deep water, and the Department of Energy (DOE) is looking to the seas as a potential repository for thousands of tons of slightly contaminated soil from the cleanup of disused atomic weapons facilities. And the nuclear industry, which is facing mounting political difficulties in dumping low-level wastes onshore, is watching these government plans with interest, for they could ease the way for a resumption of marine disposal of waste material from commercial operations.

These possibilities have begun to stir up opposition from environmentalist groups, and an intense debate over the potential hazards of dumping radwaste into the oceans is expected to develop in the next few months. At the center of the turmoil will be the Environmental Protection Agency (EPA), which is responsible for regulating ocean dumping. EPA is now in the throes of drafting new regulations governing all ocean dumping activities, including marine disposal of radwastes, and it is expected to publish its proposals in the next few weeks.

Although there are currently plans to dump only limited amounts and types of radwaste from government programs, opponents are concerned that if these plans are allowed to go ahead, they may be a prelude to more extensive dumping. In particular, they are worried that any resumption of dumping low-level wastes may eventually lead to the disposal of high-level wastes in or under the sea floor. Moreover, the critics point out, European countries, especially Britain, are already dumping thousands of barrels of low-level wastes each year in the Atlantic, and Japan has plans to begin dumping in the Pacific next year. Instead of adding its radioactive garbage to this growing pile, opponents argue, the United States should be urging restraint on its allies.

In response to these criticisms, advocates of ocean dumping contend that there is no evidence that the radwastes already disposed of in the oceans have resulted in environmental or health hazards. A controversial report, published last year by the General Accounting Office (GAO), supports this contention. It concluded that "Congressional and public concern about this issue has been over-emphasized," and recommended that EPA should get on with drafting regulations governing future ocean dumping.

The United States virtually abandoned dumping low-level wastes in the oceans in the early 1960's, although a few barrels a year were dumped until 1970. It is generally assumed that public concern over safety was responsible for bringing the practice to an end, but economics played an equally important role. Burial sites on land opened up in the early 1960's, and they offered a much cheaper alternative to marine disposal. Recently, however, the cost of onshore burial has increased sharply, and public opposition has surfaced in the two states (South Carolina and Washington) that have commercial burial sites in operation. This explains the renewed interest in dumping low-level wastes into the ocean and the attention being given to EPA's attempts to write new marine disposal regulations. The new rules will determine the conditions, if any, under which ocean dumping can be resumed.

EPA inherited responsibility for marine disposal of radwastes from the Atomic Energy Commission (AEC) in 1970. At that time, a de facto moratorium on dumping radioactive material was in effect. AEC stopped issuing dumping permits in 1960, but it allowed existing permits to be renewed, and the practice gradually petered out when renewal applications stopped coming in.

In 1972, 2 years after the last consignment of radwaste was shipped, Congress passed the Marine Protection, Research, and Sanctuaries Act (generally known as the ocean dumping act) which directed EPA to write new regulations governing all ocean dumping. The act prohibited marine disposal of high-level radioactive wastes but gave EPA authority to set rules for dumping low-level material.

EPA's regulations, which were published in 1977 and are still in force, make it difficult to dump anything into the oceans. In essence, they allow dumping permits to be issued only when no alternative means of disposal exists; they thus virtually preclude weighing the costs and benefits of ocean dumping against those of dumping on land. As for radioactive wastes, the regulations specify that, in addition to satisfying the requirement that no other means of disposal is available, they must be packaged

0036-8075/82/0305-1217$01.00/0