Vulnerable Computer Systems

May 24, 1996
The Chronicle of Higher Education A19

Colleges find it difficult to bar intruders from their networks

By David L. Wilson

P1.

EVERY DAY, people all over the world try to rummage around inside a computer at Clemson University. Sometimes it's for the thrill of trespassing. Sometimes they want to browse through a stranger's electronic mail. And sometimes they deposit a pirated copy of an expensive computer program and tell their friends to grab a copy off the Clemson equipment.

"Security is the No. 1 problem I worry about," says Mike S. Marshall, the systems programmer at Clemson who is responsible for that computer. He spends a good deal of his time tracking the trespassers, throwing them out, and upgrading his software to plug new holes.

Mr. Marshall is not alone. Thousands of computer-system administrators across the country have found that they must devote more and more of their time and resources to cleaning up the mess left by electronic vandals.

Bruno Wolff III, who works for the information-and-media-technologies division of the University of Wisconsin at Milwaukee, spent the past four months tracking down a single intruder, who now faces criminal charges. Mr. Wolff says he can't put a monetary value on the damage done, but "it cost us several thousands of dollars in staff time."

The incident has spurred the university to improve its computer security.

Last month, Justice Department officials charged a college student in Argentina with breaking into Harvard University computers and using them to enter computer systems operated by the U.S. military.

INCREASING PESSIMISM

College officials are increasingly pessimistic that they will be able to find solutions to security problems without breaking the bank, infringing on academic freedom, or isolating campuses from the Internet.

The difficulty, they say, is that there are more and more computer programs developed by intruders that let even unsophisticated users break into campus systems.

In addition, experts cite the growing decentralization of computing in higher education. Many individual campus computers are under the supervision of administrators who have no special training in security. They don't know where to look for important security announcements, don't know how to compile the computer code needed to repair the software, and don't know how to install a patch over the security leak.

Any lapse is crucial, experts say, because once an intruder has entered one computer, it is easy to compromise others on the same local network.

The problem is not unique to higher education. But unlike businesses, which can simply decide to restrict users' Internet access to a relatively safe set of activities, colleges are loath to tread on academic freedom by building roadblocks between the outside world and campus computers.

"Universities face a particularly daunting challenge, because we require openness," says Jack Suess, associate director of university computing services for the University of Maryland–Baltimore County. "As of this moment, the hackers are actually winning this battle."

In fact, computer "crackers"—malevolent hackers who break into computers to loot, spy, or destroy—say there isn't much distinction in breaking into university computers anymore. One self-described cracker says that while prestige in his circle can be gained by breaching computer defenses, academic computers are too easy to enter. "We use college computers for practice, as a place to store stuff, and as a way of making it harder to trace us." (He communicated with *The Chronicle* via someone else's account at a California university.)

Non-academic computer systems often are protected by "firewalls," devices and techniques designed to keep outside intruders from exploiting flaws in the software on computers behind the firewall. A simple version would consist of a comput-

er that connected a local network to the Internet. This computer would be programmed to reject any unusual activity that might signal an attack on the system behind it.

But firewalls are uncommon in academe. Dean B. Krafft, director of computing facilities at Cornell University's computer-science department, installed one on the department's computers nearly two years ago, but says he took the action reluctantly.

'CLEANING UP AFTER PEOPLE'

"We installed a firewall because we were spending a lot of resources cleaning up after people who broke into our systems. And we decided that we would spend fewer resources, with less risk to our systems, by putting a firewall into place."

Some people were not happy with the firewall, he adds. "It was a bit of a sales job."

On the other hand, for Greg Morrisett, an assistant professor of computer science at Cornell, "being behind the firewall is not a big deal." In general, he says, faculty members have accepted it, although it sometimes requires them to jump through a few more hoops to get things done. "But we're computer scientists, so we can do that ourselves. You can imagine how if this were used for the general population, the number of people calling for help would rise significantly."

Mr. Krafft says the firewall is the latest in a series of increased security measures that he has had to take as crackers develop their own new tools. "When the level of problems gets intolerable, when the techniques get widespread, you raise the bar," he says.

Cornell's centralized computer administration is leaving computer security up to individual departments—one reason that Cornell doesn't have a campuswide firewall. Most other universities also do not, says Mr. Krafft. "It requires somebody putting the financial resources into doing that, and typically that's not going to happen until somebody's gotten a good scare."

'POLITICALLY IMPOSSIBLE'

The computer needed for a firewall might cost $20,000, but the real costs involve keeping the system current. "It can be both an administrative headache and a major expense," he says.

Alva L. Couch, an associate professor of electrical engineering and computer science at Tufts University, is blunter when he talks about the difficulties involved:

Security Problems Plague Colleges' Computer Systems

Continued From Page A19

"It's politically impossible," he says. "It's difficult to justify security measures, even if they're obviously needed, because of the potential cost, and in particular the cost of supporting such a measure."

TRACKING REPORTS

Mr. Couch spends a lot of time tracking reports of security problems and making the recommended repairs as soon as word of them is distributed. But some computers at Tufts, he says, are administered by graduate students or others with little technical expertise and enormous demands on their time, creating a situation in which those machines are quite vulnerable.

"How do I deal with it? Well, it's not my business, to tell you the truth," he says. Mr. Couch has improved security on his part of the network in ways that he declines to talk about in public, and those methods help to protect his machines from other computers on the campus that may have been compromised. He isn't happy about this every-man-for-himself state of affairs but feels that he has little choice.

But at least Mr. Couch can protect his computers.

Usually, one vulnerable machine on a campus network puts every other machine at risk, says Richard D. Pethia, who is the head of the Computer Emergency Response Team Coordination Center, the federally supported program responsible for Internet security. It is based at Carnegie Mellon University.

SHARED RESPONSIBILITY

Everybody needs to be responsible for security these days, Mr. Pethia says. "As we've shifted the technology away from central management and gone to distributed architectures, we've also distributed the management of that technology. And those folks need to understand what their new responsibilities are, given this new world we're all living in."

He also criticizes computer manufacturers, saying that although they have made great strides in developing systems that are faster, smaller, cheaper, and easier to use, "we haven't matched that improvement in ease of use with improvement in ease of management.

"We need an order-of-magnitude improvement in ease of secure administration."

What's more, Mr. Pethia says, people on campuses need to be more conscious of how much outsiders covet their resources. "Very often when we have an incident and we're talking to people on the phone, they can't imagine why some intruder would be on their systems," he says. But even a quick conversation, he says, can identify research information, copyrighted works, or personnel files scattered among campus computers. At some point during such a discussion, he says, "a light turns on." ■

DH19960006E

"Vulnerable Computer Systems"

P2