Guarding Against Internet Intruders

To hackers, the Internet is an open road into the computer systems of universities and research centers. But security measures pose painful choices

As you read this, a band of knowledgeable, determined hackers are attacking the computers at the National Library of Medicine (NLM). If they succeed in penetrating the computer system's defenses, the attackers could tamper with anything from MEDLINE, the huge medical bibliographic database, to GenBank, the database that collects DNA sequences deciphered by geneticists around the world. Such tampering could have disastrous effects on the work of thousands of scientists. Yet NLM didn't make any special preparations. "We're not supposed to do anything extraordinary," says NLM computer specialist Jules Aronson rather cheerily. "Then they see how far they can get."

Aronson isn't panicking because "they" are actually benign intruders—members of a "tiger team" from the Computer Security Technology Center at Lawrence Livermore National Laboratory whose job is to probe for weaknesses in computer systems. The attack, explains Aronson, will test the barriers that NLM has erected to protect the integrity of its precious databases, which are heavily used by the outside world. That world includes scientists who routinely communicate with NLM's computers over the Internet—and perhaps a handful of hackers bent on serious mischief.

The security exercise at NLM shows how worried scientific organizations have become about their vulnerability to hackers roaming the Internet. The danger is mounting as the net becomes ever more tightly interwoven with scientific life. Large scientific databases are queried and updated every day via the Internet. Most university computer systems are open to all comers over the Internet. And scientists themselves are putting more and more of their data and reputations on the line—literally—as they use the Internet to collaborate, send out papers, and exchange data. Although most e-mail accounts, databases, and local networks are officially "secure"—inaccessible without a password—hackers have many methods of attack, from exploiting software weaknesses to stealing passwords.

But systems administrators nervous about the security threat are just as nervous about imposing security restrictions that might be anathema to the culture of free exchange on the Internet. "We need to define that balance between security and user needs," says Marcus Ranum, a senior scientist at Trusted Information Systems (TIS), a computer security consulting firm. For example, many industrial and government research labs and data centers, including NLM, are erecting "fire walls": the high-tech equivalent of a castle moat, where everyone and everything that crosses is checked before being allowed inside. But most universities have balked at that measure, which they consider extreme. Instead, while experimenting with less intrusive measures like stepped-up monitoring to detect intruders before they do serious damage, these universities have chosen to wait—and hope that they won't be next.

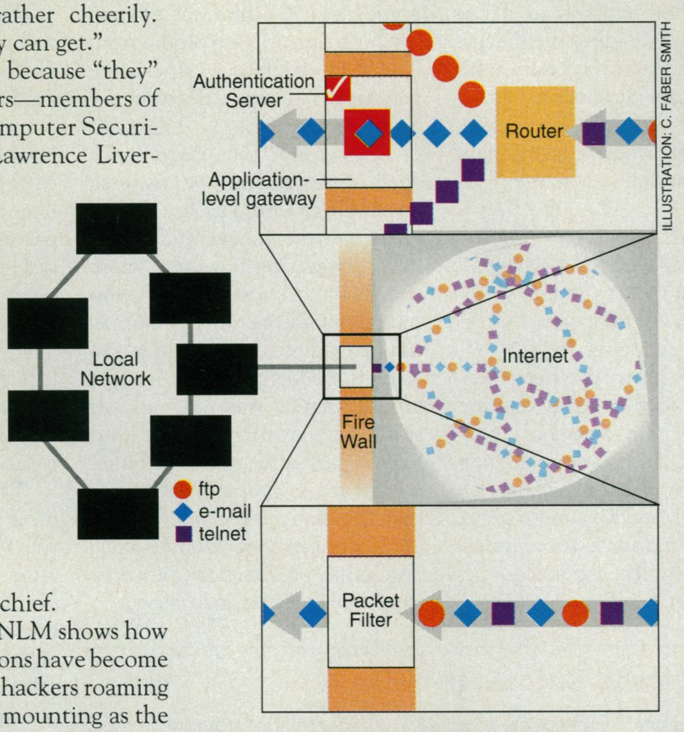

ILLUSTRATION: C. FABER SMITH

Checkpoints in a firewall. One scheme relies on a packet filter *(above)*, which blocks all Internet messages seeking "risky" services such as ftp and telnet. Another, based on application-level gateways *(top)*, allows all services but checks each message individually.

Overall statistics on hacking incidents or attempts are impossible to come by, but some universities estimate that they get from 10 to 30 "doorknob-rattling" attempts a week. When hackers do succeed in breaking in, the opportunities for mischief range from altering critical scientific data to tarnishing someone's reputation by sending false e-mail in his or her name. Grady Blount, an earth scientist at Texas A&M University in Corpus Christi, has personal experience of the kind of damage that can result.

In late October, hackers used a password-cracking program to log on to Blount's account and sent out racist e-mail in his name to thousands of people. When Blount arrived at his office one Monday morning, he found about 90 e-mail messages waiting for him instead of the usual three or four. "They were ranging from death threats to 'I'll make sure you never publish again,' " says Blount.

The threats caused Blount to move his classes to undisclosed locations around campus. His collaborations with the National Aeronautics and Space Administration were jeopardized because the agency viewed him as a possible security risk. He had to change his e-mail address and pull his contact information from the university's on-line directory. In Blount's own words, he is now "submerged." He adds: "It was purely random, but that doesn't seem to matter. I don't know what the ultimate fallout is going to be."

Ad hoc security

As Blount learned to his dismay, the Internet—a loose confederation of networks rather than a single network—was designed for ease of communication, not security. As a result, many security measures are cumbersome add-ons. "I'd have to describe the security services available on the Internet today as ad hoc," says Dan Nessett, a computer scientist at Sun Microsystems and a member of the Internet Society's Privacy and Security Research Group. Take one-time passwords, a strategy for countering the password-stealing that is the most common method hackers use to break into computers.

Ordinary passwords travel over the network each time a user logs on, making them vulnerable to password-sniffing programs. A one-time password is discarded after a single use, so even if it is captured, it's of no value. When the user tries to log on, the computer issues a challenge consisting of a string of numbers and/or letters. The user then chooses a response—the one-time password—from a pre-printed list or computes it based on a secret key, rather like a PIN number. In one

Learning to Live With a Fire Wall

On Tuesday, 25 August 1992, the supercomputer center at Texas A&M University in College Station realized it had been hacked. The intrusion had gone on for 4 months before it was noticed; by then the hackers were so cocky they were using one of the university machines as a bulletin board to discuss their attacks. Computer break-ins aren't unusual at universities these days, as links with the Internet expose their computer systems to intruders (see main text). But Texas A&M's response was exceptional: Within 10 days, programmers had thrown up a fire wall around the university's computing network.

The fire wall—a means of screening all attempts by the outside world to reach university computers—has been in place ever since, making the Texas A&M campus one of the few to opt for security over keeping the door to the Internet wide open. And although the university community objected at first, fearing that the fire wall would hamper communication with colleagues elsewhere and interfere with remote log-ins, concerns have subsided thanks to the programmers' efforts to make the barrier as unobtrusive as possible. Says biology professor Jim Golden, "The fire wall is not something we're constantly battling with."

When Texas A&M systems analyst Doug Schales and his colleagues first put up the fire wall, he recalls, "I thought they were going to hang us." The barrier consisted of a "packet-filtering" program that allowed the outside world to send e-mail to all computers at Texas A&M but blocked other incoming services such as telnet and ftp, which are considered more dangerous because they allow outsiders to log on to university computers. As a result, faculty who wanted to log in from home found they couldn't.

But that problem was fixed very quickly; for example, the computing center can now provide temporary access to workstations inside the fire wall within minutes after receiving a request. Meanwhile, the fire wall itself has been modified to make it transparent for outbound Internet services. Faculty and students can browse with Mosaic, log in to outside computers, and transfer files.

Scientists at Texas A&M now say the fire wall presents a minor inconvenience at most. Chemist A. T. Watson says he has adapted without much trouble. "I spent a year in Norway and was accessing my computers over here," he recalls. "I had to set up something special [beforehand]," and the computers he wanted to use weren't always directly accessible from outside. But he concludes, "If that's the cost of business, it's not too bad."

And the computer security experts at Texas A&M can argue that the cost is worth it. Since that scary summer of '92, the university has suffered only a few minor break-ins, usually because someone's password was compromised. "We're able to show that the packet filter is blocking attempts," Schales says. "And people are pretty happy, especially since we can answer their needs."

–E.G.

arrangement, each authorized user is equipped with an authentication device, a small handheld keypad that looks like a calculator. The user enters the challenge and the key into the keypad, which computes a one-time password.

But one-time passwords can limit new outside users—each one may have to be given a keypad and a code—and can inconvenience existing ones. Says Paul Dourish, a researcher at the Rank Xerox Research Centre in Cambridge, United Kingdom, which relies on one-time passwords: "It's a real pain—it makes logging in much longer." One-time passwords tend to be adopted by industrial labs, which are more security-conscious than universities and have an easier time imposing such measures on their employees.

Less cumbersome for users within an organization, but just as restrictive for outsiders, is another common approach to security: shielding an institution's internal network behind a fire wall. A fire wall allows computer traffic to pass only via certain restricted gateways, consisting of computers and filtering programs. Generally, users inside the fire wall can reach the outside world easily, but outsiders trying to gain access to the organization's network face impediments.

One kind of fire wall relies on so-called packet filters. These systems block packets of information or allow them through depending on what computer they come from or the kind of service they are seeking on the destination computer. A packet filter might, for example, permit any computer outside the fire wall to connect to any computer inside the fire wall to send e-mail, but might only allow outside machines to connect to a few specially secured machines inside the wall for other services such as telnet (for remote log-ins) or ftp (for transferring files). Those services are more risky, as they allow outside users to actually log in to the system.

Another type of fire wall, found at several major corporate research labs including IBM's Thomas J. Watson Research Center, Xerox PARC, and AT&T Bell Laboratories, allows access to more services but monitors each stream of packets closely by funneling it through a separate "application-level" gateway, one for each Internet service such as telnet, ftp, or e-mail. These gateways can log all transactions and control them, for example by requiring one-time passwords or by allowing outside messages through only if they come from certain preapproved machines.

So far, gateways can't reproduce the freedom of open Internet access. When an e-mail gateway is down, for example, e-mail doesn't go through. Says one graduate student who has worked at Bell Labs: "It happens pretty regularly that you don't have e-mail for a day [at Bell Labs], much more often than at a university." Gateways have other drawbacks as well. It may take months to get new Internet services running on them. Bill Cheswick, a security expert at Bell Labs who helped design their fire wall, acknowledges that "every time there's a new Internet application, like Mosaic, we have to figure out how to support it through the fire wall." And fire walls can't guarantee security. In a break-in last Christmas at the San Diego Supercomputer Center, hackers penetrated the fire wall by masquerading as "friendly" computers.

Many government centers make life easier for outside users by setting up their computer resources so that outsiders need not pass through filters and gateways at all. The National Center for Biotechnology Information (NCBI), which runs GenBank, places the computer that acts as the GenBank server to the world outside its fire wall. The archival copy of the database resides on NCBI internal machines, to which the outside world has no access, at least in theory. Similarly, the National Oceanic and Atmospheric Administration (NOAA) puts information ranging from real-time data on solar flares to the last 100 years of weather observations on some 40 computers outside its fire wall. "The dump is done by a physical, hard-wire connection, which is then turned off until the next dump," says Thomas Pyke, NOAA's director for high-performance computing and communication.

But making some resources freely accessible while sealing off others won't work for the National Center for Atmospheric Research (NCAR), because the centerpiece of its system is a Cray supercomputer for use by scientists all over the world. NCAR also runs a Mass Storage System (MSS), which contains over 30 terabytes of atmospheric and oceanographic data. Right now, scientists enjoy open access to these resources: They can send their own data to the MSS, then use the supercomputer to run calculations on the data. The downside of open access was brought home by a recent intrusion that briefly crippled the machine on which the director of the computing division reads his e-mail.

But none of the alternatives to open access looks very attractive, says Greg Woods, an NCAR software engineer. A single gateway, he says, "would be a real bottleneck. ... We will have to have more than one [gateway] machine directly accessible to Internet users." Woods and his colleagues are also considering one-time passwords. But many scientists send in their data in automatic scripts that run in the middle of the night. One-time passwords could make that more difficult because someone might have to be present to respond to the computer's challenge. "We have to be careful not to make it too hard for our users," says Woods. "If it's too hard, people will try to get around it. They'll try—unintentionally—to subvert the security."

Laissez-faire at the universities

These dilemmas are felt even more keenly at universities, long used to keeping their computers open to the easy flow of information. One university's experience with a fire wall has been positive (see box), but many others insist that their students and faculty won't put up with even minor restrictions on their Internet access. System administrators at Columbia University, for example, say the idea of a fire wall has been tossed around, but their users simply wouldn't stand for it.

Yet security problems at universities can be even more acute than at government institutes because their computer systems are managed so loosely. Thanks to cheap desktop computing power, nearly every departmental research group has its own workstations, ordered directly from the manufacturer and installed and maintained by a graduate student who would rather be doing something else. Most universities have taken a rather laissez-faire attitude toward these security vulnerabilities, but as evidence of the dangers mount, they are taking some first steps. Many are adopting network programs that conceal informative files such as lists of user names and force users to choose passwords that are hard to crack. The Massachusetts Institute of Technology is trying to reduce its system's vulnerability through its use of Kerberos, a program that encrypts information passing through the huge campus network.

For the long term, universities are hoping that the burgeoning research on computer security will soon deliver some better way to balance security with user needs. One line of work is aiming at building a better fire wall, such as the experimental one erected by the distributed systems group of Stanford University's computer science department last year to protect the group's computers. Thanks to some fancy programming, the fire wall appears virtually transparent to authorized users both inside and outside it.

Another avenue of research starts with the assumption that computers and networks cannot be designed without security holes and aims instead to detect break-ins early. For example, researchers at the University of California, Davis, are working on artificial intelligence programs that can recognize anomalies in network use. Ultimately, such programs might be able to respond to suspicious activity by cutting off the suspect user or notifying the system administrator.

In the meantime, universities and other institutions are moving cautiously. As TIS's Ranum puts it: "If you're so scared of the hackers that you destroy the network to protect it, they've won."

–Ellen Germain

Ellen Germain is a science writer in New York City.

RUSSIA

Chechnya War Threatens Science

MOSCOW—Another year of financial chaos is in store for Russian scientists in 1995. Last week, deputies in the Duma, the lower house of Russia's parliament, put themselves on a collision course with Boris Yeltsin's government over this year's science budget. Members of the Duma's subcommittee on science more than doubled the requested amount for science for the year, an increase that would still fall short of the country's 200% inflation rate. But it will be virtually impossible for the government to pay even this amount and still meet other commitments, such as the war in Chechnya, that are draining the public purse.

The government's proposed budget for 1995 was debated in mid-December in the first of three sessions that analyze the proposals in increasing detail. This first revision pegged science to receive 5.4 trillion rubles (about $1.36 billion), which is 2.5% of total government expenditure. Although this is 500 billion rubles more than last years' science spending, it would have been a substantial cut in spending power because inflation totaled 204% in 1994.

Last week, however, in the second Duma budget session, deputies from the science subcommittee proposed hiking science spending to 13 trillion rubles ($3.25 billion). From this pot, the Russian Academy of Sciences, which runs most of the country's fundamental research institutes, would receive $401 million, and the Foundation for Basic Research, a new body that dispenses Western-style peer-reviewed grants, would receive $110 million. The committee also earmarked $70 million to continue work on several key nuclear physics facilities—at Protvino and Dubna near Moscow, Gatchina near St. Petersburg, and Novosibirsk in Siberia—that have been unfinished since the collapse of central funding several years ago.

A prolonged military operation could undo proposed increases in the science budget.

—Alexander Pochinok

The third and final session, in which deputies vote on all the proposed changes, is due to take place in mid-February, after which the budget will become law. But deputies are already pessimistic about the government's ability to stick to the budget. Estimates for the cost of the campaign in Chechnya and for reconstruction run into trillions of rubles. Alexander Pochinok, deputy chair of the Duma budget committee, says that if military operations last much longer, it may sink the whole budget and lead to a "wartime budget" with severely restricted expenditure on science, culture, and education. Anatoly Shabad, the Duma deputy who leads the work on Russia's new science law, has visited Chechnya several times during the conflict and is even more pessimistic: He says it is already practically impossible to pay for the conflict and maintain this budget.

Another drain on the goverment's coffers will be the Duma's populist stance on a minimum wage. A new law that raises minimum salaries to 54,100 rubles ($13.50) per month will double the budget deficit, which currently stands at $18.5 billion. Duma deputies worry that with more budget commitments than it is able to pay for, the finance ministry will withhold money for some programs, as it has done in previous years.

So Russian scientists have another year of belt-tightening to look forward to. Pochinok says the government may have to face the unpleasant task of reducing the number of research institutes it supports. He believes the country should concentrate its resources in key institutes—"the pride of Russia," he calls them, without naming names—as well as awarding grants to specified research programs.

–Andrey Allakhverdov

Andrey Allakhverdov is a science writer in Moscow.