AP/M. XERIDAT

Who's been looking at your data?

You thought that all those e-mails, data and grant proposals on your computer were for your eyes only? Think again, says Declan Butler. Someone could be snooping on your every keystroke.

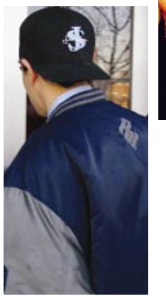
For a few days in February 2000, some of the Internet's biggest sites were toppling like pins in a bowling alley. Yahoo!, Amazon, eBay, CNN.com and others were all hit by 'distributed denial-of-service attacks' launched from computers including machines at Stanford University and the University of California, Santa Barbara. The commercial sites' servers were so busy dealing with electronic junk fired at them by the academic computers that no one could gain access. It was literally child's play: the universities' computers had been hijacked by a 15-year-old Canadian known as Mafiaboy.

This breach of academic computer security was far from an isolated event. Twice in as many weeks last year, hackers broke into computers at Indiana University, accessing names, social-security numbers and addresses of thousands of students, and using the university's servers to store music and other files, and to run chat rooms. Embarrassingly, the security hole through which the intruders gained access was one that the university's computer support service had circulated warnings about only months previously. And late last month came the revelation that officials at Princeton University in New Jersey were under FBI investigation for gaining repeated unauthorized access to the online admissions system at its rival Yale University in New Haven, Connecticut.

These incidents are just the tip of the iceberg — most aren't reported because institutions don't want negative publicity. Universities and research labs are home to some of the world's most sophisticated computer systems. But the standards of computer security that prevail across large parts of academia would give a security professional sleepless nights, says Michael McRobbie, Indiana University's vice-president for information technology (IT). Computer-security offices are often "nonexistent, organizationally buried or understaffed", he says. As a result, anarchy often reigns, with staff plugging machines in and out of networks without anyone knowing, and inadequate checks on whether the people accessing data are who they say they are. Often, there are no central records of what sensitive data are being stored, and where.

Under attack

If you still find the topic a crushing bore, here is at least one reason to sit up and pay attention — the number of attacks is mushrooming. In the early 1990s, says one official at the Massachusetts Institute of Technology (MIT), a major research university might expect two or three computer-security incidents per year. Today, the number of breaches runs in the thousands. "These events, once an amusing technical curiosity, have become a significant organizational concern," says the MIT source.



CANADIAN PRESS/AP (INSET); C. KARLSEN/GETTY NEWS

Two faces of hacking: the annual DefCon gathering (above) highlights security flaws, whereas Mafiaboy (left) exploited them to malicious ends.

In part, this is because you no longer have to be a technical wizard to break into a computer network — automated software, free for download from hacker sites, can do the job for you. 'Distributed port scans', for example, randomly crawl the Internet and probe the entry ports into networks, see what software is running, look for vulnerabilities and automatically break in. On average, each of Indiana University's 55,000 Internet-connected computers is probed at least once a day, says Mark Bruhn, the university's IT policy officer.

When computer-savvy researchers find

AP

On guard: university computer systems need almost constant monitoring to prevent hacker activity.

that a breach has occurred, correcting the problem is no trivial matter. "I find security considerations to be a significant drag on scientific productivity," says Mark Gerstein, a bioinformatician at Yale University. "The few incidents we've had here where computers were cracked wasted a vast amount of time." Even if data remain intact, hacked computers often need to be reinstalled to ensure that the intruders have not left a secret 'back door', giving them future access.

Spies in the wires

Many of the breaches are the work of teenage hackers who want to impress their peers, but others have a more sinister edge. It is perhaps unlikely that your fiercest academic rival is surreptitiously hacking into your unpublished data, but anyone involved in a commercially sensitive project would be foolish to discount the threat of cyber-espionage. Already, some biotech firms are wary of using public databases for fear that competitors will capture their search terms and gain insights into their work. And in May this year, police in Japan arrested three staff at NEC Toshiba Space Systems in Yokohama on charges of hacking computers at the National Space Development Agency to steal designs of a satellite antenna from rival company Mitsubishi Electric.

The most serious threat of all may come from cyber-terrorists. Security experts are seriously worried that rogue states or terrorist groups could launch Mafiaboy-style denial-of-service and other attacks, but on a much larger scale, targeting infrastructures such as electricity grids and communication systems, and disabling vast swathes of the world's computers.

It's against this background that academic leaders are waking up to the need to revamp their security procedures. In a survey last year, security did not figure among the top ten IT issues ranked by the 1,800 member institutions of EDUCAUSE, which promotes the use of IT in US higher education. In the 2002 survey, security rose to number five in the rankings — and number two for medium-to-large organizations.

Institutions that aren't taking the threat seriously may soon find that external pressures force them to do so. Lawyers are pressing for research laboratories and universities to be held liable if they neglect to secure their systems and so allow their computers to be used to launch denial-of-service attacks or give hackers access to confidential data. The likes of Mafiaboy typically have few assets, so the "deep pockets of universities are an attractive target", observes Frank Vinik, risk manager with United Educators Insurance of Chevy Chase, Maryland, the main insurer for the US academic sector.

Alan Paller, director of research at SANS, the System Administration, Networking and Security Institute in Bethesda, Maryland, which brings together more than 156,000 computer professionals, suggests that government research funding should be made conditional on labs meeting minimal security requirements. And Richard Clarke, President George Bush's computer-security adviser, will next month issue a national cyberspace protection plan that is expected to include specific guidelines for government agencies. "Every American relies upon cyberspace and every American has to do something to secure their part of cyberspace," Clarke has said.

But securing academic networks is inherently difficult. A campus will typically have tens of thousands of machines hooked up to the Internet at any one time, and the corporate approach of applying rigid central control and putting everything bar the servers that run public websites behind security firewalls isn't appropriate. "University networks are by design and of necessity open," observes Gregory Jackson, vice-president and chief information officer of the University of Chicago.

What's more, many computers used for research are uniquely configured, for example for data gathering, and often are only fully understood by the scientists running the project. "Often, the system administrator knows not much more about a specific computer than where to turn it on or off," says Gerstein. Individual labs usually cannot afford to hire their own computer-security specialist, resulting in a risky do-it-yourself approach. Stephen Nesbitt, director of operations at NASA's Computer Crimes Division, which has an enviable record in bringing malicious hackers to justice, observes that security will often come second to pressing deadlines to finish a research paper or to complete an experiment.

Despite these disadvantages, the prospects aren't entirely gloomy. Academia boasts some of the world's foremost experts in computer security. And staff at the CERT Coordination Center at Carnegie Mellon University in Pittsburgh, the main clearing-house for information about security threats, are on hand to provide technical assistance and to coordinate responses to attacks.

On the defensive

So what can researchers and their host institutions do to improve the situation? Academic networks are often stuffed with sensitive information such as research data, grant proposals, and medical and student records. The first step is to ring-fence off the most critical parts using firewalls designed to block all but authorized traffic.

Intrusions are inevitable, so both in front of the firewalls and behind them, systems should have encrypted communications — much like those you use when banking online — to protect passwords and data from prying eyes. And every single machine should be protected, or 'patched', against newly identified security flaws, and have its antivirus software up to date.

Gerstein's lab has adopted this layered approach to security. He has separated its network into private and public spaces, created secure 'private' backups of the data on servers running public websites, implemented encryption, and keeps up to date with the latest security patches. "This consumes a serious amount of time and hinders implementation of useful bioinformatics services," Gerstein admits. But given the importance of protecting data, and the hassle of restoring systems after a security breach, he argues that it is time well spent.

The adoption of encryption remains patchy, however. The University of Chicago

has secured half of its key IT services this way and expects to complete the process by autumn. But most universities have been slow to take up the technology.

Nevertheless, a few institutions stand out as models of good practice. MIT's IT staff probe its networks to spot machines that are insecure, and have the power to force those that don't make the grade off the network immediately — a policy that most institutions have been reluctant to implement. As MIT doesn't rely heavily on firewalls, this tough enforcement obliges users to install software patches to protect against new threats.

Protect and survive

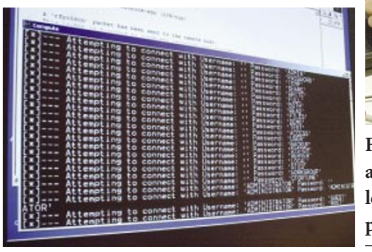
This policy paid off in July last year, when the Code Red virus spread across the world's computer networks. "It was a non-event on the MIT campus," says one university IT official. Code Red exploited a security flaw in Microsoft's IIS web-server software, copying itself to randomly chosen Internet addresses, defacing websites with the message "Hacked by Chinese", and attempting a denial-of-service assault on a White House website. Variants of Code Red infected hundreds of thousands of machines. In disrupting the performance of infected systems and requiring them to be cleaned up, the viruses caused up to US$2 billion of damage. To William Wulf, president of the US National Academy of Engineering, this experience illustrates the "Maginot line syndrome" — a false sense of security that can be engendered by firewalls.

MIT has also created a cross-institute team comprised of information-security staff, students, faculty members and representatives of its big independent labs, such as the Laboratory for Computer Science, the Artificial Intelligence Laboratory, the Media Lab, the Research Laboratory of Electronics and the Whitehead Institute for Biomedical Research. "This broad-based approach recognizes that the information-technology experts cannot handle security alone," says Vinik.

Broad-based also means thinking beyond the campus perimeter. Even if lab computers are secure, networks may be vulnerable as a result of researchers working from home, or at conferences, on computers that have been compromised so that an intruder can capture every keystroke. This risk was famously demonstrated in October 2000 by a hacker who managed to access Microsoft's most heavily guarded asset — the source code of its Windows operating system — through an employee logging on to the company's secure system from an unprotected home computer that had been compromised.

Mark Gerstein: lab time is being wasted.

Mention Microsoft to any security expert, and they will point out that the company's big-selling, interconnected products are the most common point of illicit entry into a system. "The biggest and most widespread security threats have come from two or three Microsoft products, primarily Outlook and the Microsoft IIS web server, but also Internet Explorer," says John Franks, a mathematician and computer-security expert at Northwestern University in Evanston, Illinois.



Franks, for one, favours the use of products such as the Linux operating system, in which the source code is open for anyone to scrutinize, increasing the chance that security vulnerabilities will be spotted and made public. Red Hat, the major Linux distributor, has configured its software so that, when a new security patch is released, it can be automatically installed on Internet-connected machines running the operating system.

Microsoft is also now making security a higher priority. In response to customer concerns about the vulnerability of its products, the company has decided to send 9,000 of its élite programmers on courses in writing secure software.

Language barriers

While software vendors try to get their houses in order, what is a sharper focus on computer security likely to mean for the scientist at the bench? In the first instance, unfortunately, it will drain time from research. "Even knowledgeable individuals can find the minutiae of security to be daunting," says one IT official at MIT.

If academic computer networks are to be successfully secured, security experts and scientists may have to take time to find a common language through which to discuss the issues at hand — the jargon of the security professional can be impenetrable to the uninitiated. Observes the IT official from MIT: "More than once, in response to a carefully crafted and technically complete security advisory, we have received feedback along the lines of: 'I'm a professor of chemical engineering, and not stupid, but I've no idea what you are talking about or how to fix the problem you suggest I have'."

The constant development of software products, and of the tools for hacking into them, means that securing academic computer networks will be an ongoing endeavour. But a new commitment to provide funding for research should help to tip the balance in favour of those trying to protect your data. In February, the US House of Representatives approved the Cyber Security Research and Development Act. Now being considered by the Senate, this would commit some $880 million over five years to create a research programme into computer security to be led by the National Science Foundation and the National Institute of Standards and Technology.

AP

Fighting back: students at a military college learn how to spot a password attack (left).

New approaches are likely to recognize that security must be more automated. The idea is to anticipate unknown forms of attack by blocking unusual activity on the network, or reporting it to system administrators. Some researchers, for instance, are developing programs that mimic the function of the immune system to react to both known and unknown threats (see *Nature* **415,** 468–470; 2002).

In the long run, improving security will mean redesigning systems with security uppermost in mind, says Nesbitt. Changes in the way research is done may help to drive this process. In future, many scientists will organize themselves in large international collaborations using 'Grid' networks, which aim to provide supercomputing power on tap by distributing tasks and data over tens of thousands of machines at institutions worldwide.

Grid computing takes security beyond the boundaries of individual institutions, as each must be able to trust the security provisions of others. For example, researchers will need to be able to 'sign in' and then, depending on their level of authorization, access different levels of resources at multiple institutions around the globe, without further authentification. "Succeeding will require rethinking infrastructure, procedures and trust relationships," says Ian Foster, a leader in Grid development at the Argonne National Laboratory near Chicago.

Whether or not you need to use Grid computing, the threat posed by malicious hackers is real, and growing. If you're still in the habit of deleting security advisories from your IT department as soon as they arrive in your e-mail, you may be playing Russian roulette with your data. And if your IT people haven't yet raised security issues with you, perhaps it's time to give them a call. ■

Declan Butler is *Nature*'s European correspondent.