

The University of Texas at Austin

McCombs MBA Alumni Network

MBA : MMA Network : News and Publications : business@texas : Front Line



You're on the Front Line

by Pam Losefsky

To the average office worker, logging on to the computer to begin the business of the day couldn't be more routine or raise less concern. But to the computer services personnel whose job is to maintain the security and integrity of the computer networks the rest of us take for granted, danger lurks behind every keystroke.



A quick cyber trip to the CERT web site, a center of Internet security expertise at the Software Engineering Institute (Carnegie Mellon University), is all it takes to enter the paranoid world of the computer security officer. Advisories posted at the site warn of "recent activity against secure shell daemons," the W32/Goner worm, and "multiple vulnerabilities in WU/FTPD." Articles discuss attack scenarios, the frequency of scans and probes committed by hostile elements, and how best to protect your system from external threats.

But this is not hollow combat jargon: the war against hackers has been escalating at an alarming rate. According to CERT, the number of hacking incidents reported jumped from a mere six in 1988 to more than 34,700 just through the third quarter of 2001 (one incident could involve thousands of Internet sites). What's more, McAfee, a leading security application service provider, maintains a directory of 50,000 known viruses.

While the FBI and other government agencies publish statistics, the actual rate of cyber crime is difficult to determine. Many computer users will not even know that they have been attacked. What's more, attack reports tend to be underreported, says Larry Leibrock, Associate Dean for Technology at the McCombs School and an appointee on both the Texas Infrastructure Protection Advisory Committee and the Board of the Texas Department of Information Resources. "There are incentives for business not to report; and in many third-world countries, there is no reporting at all."

Why has the Internet become such a battleground, and what is being done to win the war?

Hackers run the gamut from 'script kiddies'-security slang for ego-driven people with minimal skills who thrill at the game of breaking into secure areas rather than causing significant damage-to serious criminals who seek to steal information for financial gain or to cause severe disruptions in commerce. And they have used efficiencies enabled by the Internet itself to more effectively zero in on their targets.

"Script kiddies often pull tools from the Internet and use them for malicious activities; you might equate this form of criminal mischief to a group of high schoolers stealing a car to take a joy ride or spray-painting a fence with graffiti," says Leibrock, who has testified on hacking before a committee of the U.S. Senate. "But hackers are just one class of high-tech criminal. Traditional crimes are also committed using computers; for instance a stalker might use the Internet to obtain information on his or her victim."

Quick Reference

Protect Yourself

- Get and install an antivirus program, if you are uncomfortable updating your system yourself, consider a centrally managed service.
- If you use Outlook, make sure you are running the version with the latest security patch (Outlook XP), which prevents executables from running on your computer.
- Don't ever click on or run anything that you're not absolutely sure of.
- Buy a hardware firewall. This can cost up to a couple hundred dollars, but is well worth it. (Firewalls prevent incoming requests that probe the Internet for computers that are vulnerable.)
- If you purchase goods over the Internet, use only one credit card and check your statement closely every month; report any unauthorized charges.
- Be careful about disclosing too much personal information on Web sites, use common sense in your communications.

The United States is probably the most at-risk country, says Chris Davis, MBA 01 and a wireless security architect with Texas Instruments in Dallas. "We have more users and more commerce that depends on the Internet than anyone else, both B2B and B2C. Our dependencies make us vulnerable, and so does our complacency."

Without a doubt, most people don't take the time to update their systems and virus protection. But even if you are one of the few who do, there is no guarantee of your computer's security. "The general standard is that a freshly installed computer with Windows 2000 will be hacked within eight hours," Davis says, citing statistics that were current about six months ago. "And if that computer is on a college campus, it's a much shorter time frame."

Part of the reason our systems are so insecure is that manufacturers knowingly release new products with flaws. "Operating systems are produced on schedules," explains Davis. "And there is a strong, justifiable business case for these companies to get the systems out there on time."

Within security circles a debate rages about whether companies should fully disclose known flaws or black box them. "If the code is black-boxed, that prevents hackers from getting it and exploiting the flaws for malicious intent," Davis says. "But if the code were disclosed, it would be easier for security companies to work on remedies." What is happening now,

· Safeguard data on all digital devices, not just on computers, but Palm Pilots and cell phones. Tips from Larry Leibrock, McCombs School Associate Dean for Technology, and Chris Davis, MBA 01

Davis indicates, is that usually within a week or so of a new product release, security companies will find flaws and contact the manufacturer, putting pressure on the computer company to fix the problem under threat of widely releasing the information.

To make matters worse, security officers are faced with information overload.

"Within an environment like the McCombs School of Business that has about 10,000 clients, every day probably 15 to 20 bugs are reported," Davis says. "And an officer will probably get 50 to 100 messages a day to sort through, determine the viability of, and act on." This makes his or her job very difficult.

"No matter how hard we try, it is impossible to produce a 100% secure solution because of the people part of the equation," says Davis, who is in the business of developing security features for mobile phones. "People are never going to act in predictable ways." With this in mind, the trend in computer security is to move to managed services. "Services like McAfee are centrally managed, automatically updating, and hands-free. They can take a lot of the human element out of computer security," he says.

The most important thing we need to do as a country is to educate computer users, believes Davis. "Since September 11, people have become more aware of security mechanisms and measures, and that extends to computer security as well." Leibrock agrees, "Clearly, there's been renewed interest in the protection of our critical information infrastructures. It is very important for everyone to think of globally connected information systems not only as a powerful tool for economic development, but as a weapon when in the wrong hands."

[BACK TO TOP](#)