April 3, 1997

Hunting down intruders

Detection systems help defend home, business computers from hackers / Simson L. Garfinkel

YOU WOULD BE hard-pressed to find a business in Boston that puts locks on its doors but fails to install an alarm system in case those locks are breached.

But that's what's happening on many company Web sites and corporate Internet servers.

When the crooks break in to computer systems during the late hours of the night, they often have free reign until the next morning. Other times they don't make their presence known for weeks as they pilfer files and read confidential documents night after night until they decide to leave a calling card and move on to their next victim.

The problem occurs because "firewalls," the most popular security system on Web sites, are designed to keep people out, and not to detect people who got in.

A firewall stands between a company's internal network and the Internet, blocking all connections other than those that are explicitly authorized. The most restrictive firewalls allow only electronic mail and HTTP, the protocol used by the World Wide Web, to pass. This is theoretically supposed to prevent people from the outside world from breaking into the company's computers.

In practice, firewalls are no perfect defense. Many are installed incorrectly. Sometimes holes are opened in the firewall so that the company's employees can "get their work done." And sometimes there are other ways to get into a company's computer system that don't involve passing through the firewall.

Besides strong locks, businesses need guards or burglar alarms. In the computer world, these are called intrusion detection systems. Just as its name implies, an intrusion detection system scans your computer and watches for a break-in.

When computer hackers break into a system, they frequently alter the computer to make it easier for them to return. Often they will use the compromised computer as a jumping-off point for attacks against the organization, or against other computers on the 'Net.

The simplest intrusion detection systems look for these changes by scanning system programs looking for modifications. One of the best (in fact, one of the only) scanning programs is called Tripwire, available freely over the Internet from Purdue University. Right now, Tripwire runs only on UNIX computers, but a version that runs on Microsoft's Windows NT operating system may be created.

Webstalker, by Haystack Labs, is another kind of intrusion detection system. It monitors a Web server for suspicious activity. It can detect if somebody from the outside world breaks through the firewall or if somebody comes in with an authorized account and then attempts to gain unauthorized privileges.

The program can also detect attacks from insiders – people who are already behind an organization's firewall. For example, Webstalker can detect whether a system operator who is authorized to log into the Web server to make a backup tape decides to make an unauthorized change to a company's home page.

Steve Smaha, Haystack's CEO, says that one of his clients is a large bank that's using Webstalker to monitor a Web server being used to take loan applications. "Their auditors said, 'We have no way of determining if the information on this machine has been changed since the time the person typed it in,' " Smaha recalled. Webstalker monitors the customer data to make sure that it hasn't been touched by an unauthorized process or individual.

If Webstalker does detect a break-in, it can send a message over the network to a special network monitoring station, send out electronic mail, or dial a phone number and ring somebody's pager. Or the program can get nasty, and electronically "kill" the programs on the computer being run by the intruder.

Webstalker runs on Windows NT and on UNIX systems manufactured by Sun Microsystems and IBM. The system costs $4,995; a free, 30-day evaluation program can be downloaded from the company's Web site.

Although right now intrusion detection might seem like an esoteric security technology for big financial Web sites, the technology could make its way to desktop computers. Solid intrusion detection would go a long way toward minimizing the impact of security bugs in programs like Microsoft's Internet Explorer and Netscape Navigator.

Intrusion detection would even help stamp out those pesky computer viruses.

It's unreasonable to think that tomorrow's networked computers will be equipped with invulnerable locks. What the computer industry needs to start building is low-cost alarm systems.

Information about TripWire can be found at the COAST Web site at Purdue University, http://www.cs.purdue.edu/coast/.

Haystack Labs' Web site is at http://www.haystack.com/.

Technology writer Simson L. Garfinkel can be reached at plugged@simson.net.