Pittsburgh, PA
Wednesday
April 24, 2002

News Sports Lifestyle Classifieds About Us

post-gazette.com Health & Science

Take me to... Go

Health & Science
Health
Science
Environment

Home > Health & Science > Science

CMU scientists study castle warfare to improve computer defenses

Monday, April 22, 2002

By Byron Spice, Science Editor, Post-Gazette

A new approach to improving computer security is actually very old -- medieval, in fact.

Think of the battle against computer viruses, worms and other forms of electronic attack as a form of siege warfare and the solution becomes clear: turn the computer into a kind of castle.

That's the approach being taken at Carnegie Mellon University by a group of researchers led by computer scientist Greg Ganger. With the support of a $4.5 million grant from the Department of Defense, they are developing "self-securing devices," computer components such as hard-disk drives and network cards that will be able to defend themselves and, ultimately, each other, from attack.

Most existing computer security strategies, such as the firewalls that defend many company networks and other "intranets," are designed to keep intruders out of the network or the individual computer. But an intruder who somehow makes it through that perimeter defense is home free.

A castle doesn't work like that, Ganger said. Even if an invader managed to make it over or through a castle's walls, he still had to contend with fortified towers and other buildings from which defenders could target him. "There's no single place to attack that can't be seen from two other places."

Like a castle, a computer consists of many parts, not just a central processing unit. It includes disk drives, network cards, graphics cards and other input/output devices. Each incorporates some computer processing power of its own; what Ganger and his colleagues are doing is using some of that computing power on each device so that each component can protect itself, each in its own way.

Take the recent Internet worm dubbed Code Red. Once it had invaded one machine, it was designed to spread to others by sending itself to randomly selected computer addresses. But Ganger said a computer's Internet card, the circuitry that serves as its interface with the Internet, could readily recognize the presence of the Code Red worm if it was designed with some security smarts.

The Internet addresses that humans readily recognize -- usually combinations of words, letters and some minimal punctuation -- are not the ones that computers recognize. The computer must translate the words and letters into a series of numbers. The Code Red worm, however, simply generated random numbers to serve as addresses. This rapid succession of numbers would have been unlike any normal traffic that the Internet card would handle. It would be fairly easy for an Internet card to recognize this weird pattern and shut itself down or notify the computer network administrator.

In similar ways, a hard-disk drive might be able to detect other intruders. Someone who is attacking through an Internet browser, for instance, might try to hide his tracks by changing the system's audit log, and leave himself a "back door" into the system by changing the computer's log-in code. Both these functions would involve the hard disk drive and could be detected, allowing the computer to alert the user or system administrator.

A computer with a video camera input might be programmed to recognize when its user has walked away and to lock up the computer automatically until the user logs in again.

All of this self-protective activity by each component would have been unthinkable just a few years ago, said John Wilkes, a member of the storage management group at Hewlett-Packard Laboratories in Palo Alto, Calif. The amount of computer processing and memory on each component was kept to a minimum to save expense, he explained. Now, processing and storing data have become so cheap that it's possible to economically increase these capacities on each device.

"Disk capacity is so cheap now we're actually looking for new uses of it," Wilkes said.

One advantage of making components self-securing is that each one can closely monitor itself, finding clues about intruders that would go unnoticed by firewall devices, which must handle a large flow of information into a local network from the larger Internet.

"The speed of the network is getting faster," said Don Cameron, a data storage architect at Intel Corp. The increase in network speed is so great it's outstripping the increase in processor speed, which makes it even more difficult for a perimeter defense such as a firewall to keep pace, he added.

Ganger, director of CMU's Parallel Data Lab, which performs research on data storage, said the idea for self-securing devices sprang from an effort to increase the security of disk drives. Ganger and fellow researcher David Nagle realized that similar approaches could be taken for other components, increasing the security of the entire system.

The work has been under way for more than a year now and a prototype self-securing disk drive has been developed. Work on other components is continuing.