Protecting Computers After the Barbarians are Inside the Gate

ANGELOS KEROMYTIS

Associate Professor of Computer Science

SYSTEMS

"The barbarians are no longer at the gates," Associate Professor Angelos Keromytis said about computer security. "They are inside the doors and there are not enough guards to repel them."

Most security systems are designed to keep bad guys out, and can do little once they are inside, Keromytis explained. "We start with the proposition that attackers will compromise your system, despite your best efforts to keep them out. The only solution is to make systems that are self-healing and self-protecting," he said.

Keromytis' approach is to teach computers to act like the best human experts, if they had all the time in the world to react to an attack. "We want the computer to recognize an attack, see what happens, and come up with a way to modify the system so that it blocks the attack," he said.

Most attackers take advantage of the fact that nearly all computers on a network run the same software. If an attacker finds a vulnerability in one computer, it can attack all the computers. Keromytis turns this into an asset. His software monitors each system, noting when attacks fail or succeed and looking for unusual behavior.

When the alarm sounds, his security system isolates the infected computer. Then it analyzes recent events to find the trigger – an e-mail virus, a malicious download, a tainted document – that set it off. The system automatically attempts to write software code to fix the problem, testing different approaches until it finds one that works. It then rolls back the computer to a time before the attack and inserts the fix. The entire process takes only fractions of a second.

The newly inoculated computer also passes information about the threat around the network. Each computer then builds its own fix. This build-your-own approach prevents hackers from somehow attaching viruses to fake fixes.

"What we're trying to do is build systems where the individual computers and servers collaborate to prevent attacks, fix attacks that succeed, and then send information to other parts of the network about the vulnerability so they can fix it too."

Keromytis is currently testing the software and plans to scale up to larger systems soon. He is also looking at ways to find viruses that wait weeks or months until erupting.

The barbarians may have gotten through the gates, but in the future they will find the doors barred by a new generation of persistent guards.

B.S., Crete, Heraclion, 1996; M.S., Pennsylvania, 1997; Ph.D., 2001