Computer scientists set on winning the computer virus 'cold war'

May 24 2007

First came the virus. Then came the antivirus software. Ever since, virus programmers have been escalating their technology, trying to stay one step ahead of the computer security engineers and vice versa.

"Essentially, this is an arms race," says Somesh Jha, an associate professor of computer science at the University of Wisconsin-Madison. Jha and graduate student Mihai Christodorescu have taken the next step in that proliferation.

In collaboration with computer scientists at the University of California-Berkeley and Carnegie Mellon University, the two UW-Madison researchers have developed new software called the Static Analyzer for Executables (SAFE).

SAFE targets viruses, spyware and other malicious programs - called malware - based on their behavior. Commercial virus scanners, such as McAfee and Symantec, search programs for specific patterns, or signatures. They read through programs like a computer might search a document for a specific word. SAFE would not only pick up that one word, but would spot all of its synonyms as well.

SAFE examines the behavior of a program without running it. Then it compares the behavior with a list of suspicious behaviors, such as reading an address book and sending e-mails. The programs that perform suspicious behaviors are considered malware.

The traditional signature-based method leaves an opening for virus programmers to disguise the virus and render the commercial scanners useless. Each disguised variant has a unique signature that must be distributed. Right now, most virus scanners recommend downloading updates weekly, but more frequent updates may become necessary, he says.

"I don't think the approaches currently being used by commercial companies are going to be sustainable," Jha says.

SAFE requires updates only when viruses exhibit new behavior. It is proactive, rather than reactive.

"This is the next generation in malware detection," Jha adds.

Jha and Christodorescu began working on SAFE when they tested variations of four viruses on Norton and McAfee antivirus scanners and found that only the original variation of each virus was caught. SAFE caught all variations.

SAFE's advantages are not limited to convenience and sustainability. Programmers are beginning to write viruses that change every time they get sent to another computer. These transformations are written directly into the code, and can create infinite variations of the virus.

"[Attackers] are already becoming very sophisticated. They are using on-the-fly evasion techniques," Jha says. "As they use more sophisticated things to hide their malware, your detection has to become better and better."

Source: University of Wisconsin-Madison