Researchers develop next-generation computer antivirus system

August 6 2008

(PhysOrg.com) -- Antivirus software on your personal computer could become a thing of the past thanks to a new "cloud computing" approach to malicious software detection developed at the University of Michigan. Cloud computing refers to applications and services provided seamlessly on the Internet.

Traditional antivirus software is installed on millions of individual computers around the world but according to researchers, antivirus software from popular vendors is increasingly ineffective. The researchers observed malware --malicious software--detection rates as low as 35 percent against the most recent threats and an average window of vulnerability exceeding 48 days. That means new threats went undetected for an average of seven weeks. The computer scientists also found severe vulnerabilities in the antivirus engines themselves.

The researchers' new approach, called CloudAV, moves antivirus functionality into the "network cloud" and off personal computers. CloudAV analyzes suspicious files using multiple antivirus and behavioral detection programs simultaneously.

"CloudAV virtualizes and parallelizes detection functionality with multiple antivirus engines, significantly increasing overall protection," said Farnam Jahanian, professor of computer science and engineering in the Department of Electrical Engineering and Computer Science.

Jahanian, along with doctoral candidate Jon Oberheide and postdoctoral fellow Evan Cooke, both in the Department of Electrical Engineering and Computer Science, recently presented a paper on the new approach at the USENIX Security Symposium.

To develop this novel approach, the researchers evaluated 12 traditional antivirus software programs against 7,220 malware samples, including viruses, collected over a year. The vendors tested were: Avast, AVG, BitDefender, ClamAV, CWSandbox, F-Prot, F-Secure, Kaspersky, McAfee, Norman Sandbox, Symantec and Trend Micro.

Traditional antivirus software that resides on a personal computer checks documents and programs as they are accessed. Because of performance constraints and program incompatibilities, only one antivirus detector is typically used at a time.

CloudAV, however, can support a large number of malicious software detectors that act in parallel to analyze a single incoming file. Each detector operates in its own virtual machine, so the technical incompatibilities and security issues are resolved, Oberheide said.

CloudAV is accessible to any computer or mobile device on the network that runs a simple software agent. Each time a computer or device

receives a new document or program, that item is automatically detected and sent to the antivirus cloud for analysis. The CloudAV system the researchers built uses 12 different detectors that act together to tell the inquiring computer whether the item is safe to open.

CloudAV also caches analysis results, speeding up the process compared with traditional antivirus software. This could be useful for workplaces, for example, where multiple employees might access the same document. The new approach also includes what the developers call "retrospective detection," which scans its file access history when a new threat is identified. This allows it to catch previously-missed infections earlier.

The researchers see promising opportunities in applying CloudAV to cell phones and other mobile devices that aren't robust enough to carry powerful antivirus software.

CloudAV Project Summary: www.eecs.umich.edu/fjgroup/cloudav/

Provided by University of Michigan