Researchers invent system to control and quarantine worms attacking computer networks

February 8 2007

A new anti-worm technology developed by Penn State researchers can not only identify and contain worms milliseconds after a cyber attack, but can also release the information if the quarantine turns out to be unwarranted.

Because many current security technologies focus on signature or pattern identification for blocking worms, they cannot respond to attacks fast enough, allowing worms to exploit network vulnerabilities, according to the researchers. As a result, several minutes can elapse between when a signature-based system first recognizes that a packet or datagram is a worm and when it creates a new signature to block further spread.

But when signature-based systems shorten the signature-generation time, they often miss those worms capable of mutating automatically.

The researchers' new technology -- Proactive Worm Containment (PWC) -- doesn't rely on signature generation. Instead it targets a packet's rate or frequency of connections and the diversity of connections to other networks -- which allows PWC to react far more quickly than other technologies.

"A lot of worms need to spread quickly in order to do the most damage, so our software looks for anomalies in the rate and diversity of connection requests going out of hosts," said Peng Liu, associate

professor of information sciences and technology at Penn State and lead researcher on the PWC system.

When a host with a high rate is identified, then PWC contains that host so that no packets with the worm code can be sent out.

Liu estimates that only a few dozen infected packets may be sent out to other networks before PWC can quarantine the attack. In contrast, the Slammer worm, which attacked Microsoft SQL Server, on average sent out 4,000 infected packets every second, Liu said.

Because high connection rate transmissions do not always indicate worms, PWC includes two novel techniques that can verify that suspect hosts are clean or not infected. These techniques use vulnerability-window and relaxation analyses to overcome the denial-of-service effect that could be caused by false positives, he added.

"PWC can quickly unblock any mistakenly blocked hosts," Liu said.

The PWC software can be integrated seamlessly with existing signature-based worm filtering systems. The researchers are currently beta testing PWC. Because PWC targets connection rates to identify worms, it may miss slow-spreading worms. But current technologies already can pick those up, Liu said. Worms pose a serious threat to networks, compromising network performance and even leading to denial of services. SQL Slammer, for instance, not only slowed Internet traffic but also disrupted thousands of A.T.M. machines. Additionally, worms can open the door for attackers to machines within infected networks.

A provisional patent has been filed by Penn State on the software, "Proactive Worm Containment (PWC) for Enterprise Networks," invented by Liu; Yoon-Chan Jhi, a doctoral student in the Department of Computer Science and Engineering; and Lunquan Li, an IST doctoral

student.

Source: Penn State