Code defends against 'stealthy' computer worms

February 1 2010

Self-propagating worms are malicious computer programs, which, after being released, can spread throughout networks without human control, stealing or erasing hard drive data, interfering with pre-installed programs and slowing, even crashing, home and work computers. Now a new code, or algorithm, created by Penn State researchers targets the "stealthiest" of these worms, containing them before an outbreak can occur.

"In 2001 the 'Code Red' worms caused $2 billion dollars worth of damage worldwide," said Yoon-Ho Choi, a postdoctoral fellow in information sciences and technology, Penn State. "Our algorithm can prevent a worm's propagation early in its propagation stage."

Choi and his colleagues' algorithm defends against the spread of local scanning worms that search for hosts in "local" spaces within networks or sub-networks. This strategy allows them access to hosts that are clustered, which means once they infect one host, the rest can be can be infected quickly. There are many types of scanning worms, but Choi calls these worms the stealthiest because they are the most efficient and can evade even the best worm defenses.

A worm outbreak can begin with the infection of a single computer. After infection, a worm begins to probe a set of random, local or enterprise IP addresses, searching for more vulnerable hosts. When one is found the worm sends out a probe, or packet, to infect it.

"A local scanning worm can purposely scan a local or enterprise network only," said Choi. "As the size of the susceptible population increases, the worm's virulence increases."

The researchers' algorithm works by estimating the size of the susceptible host population. It then monitors the occurrence of infections within it and sets a threshold value just equal to or below the average number of scans necessary to infect a host by an infected host.

If the scanning worm's number of scans carrying a specific destination port number exceeds the threshold, the algorithm quarantines the worm. The algorithm then breaks down the network into many small networks, or cells, which in some cases might be only one computer. A worm can spread within the cells, but not between the cells. This way the algorithm can isolate an infected host or small cluster of infected hosts housing the worm.

"By applying the containment thresholds from our proposed algorithm, outbreaks can be blocked early," said Choi.

To test the effectiveness of their algorithm the researchers ran a series of computer simulations and emulations using different scanning strategies of local scanning worms. Results showed that their algorithm was an efficient estimator of worm virulence and could determine the size of the susceptible host population after only a few infections.

"Our evaluation showed that the algorithm is reliable in the very early propagation stage and is better than the state-of-the-art defense," said Choi.

Choi, working with Lunquan Li, assistant professor, Institute of Microelectronics, Chinese Academy of Sciences, Beijing, and his Penn State colleagues, Peng Liu, associate professor, information sciences and

technology, and George Kesidis, professor, electrical engineering and computer science and engineering, published their work in the February issue of *Computers and Security*.

According to Choi, local scanning worms are constantly evolving. They are becoming more complicated and increasingly efficient. As a result, worm outbreaks pose a real threat to networked systems. Because many networked home and office computers are susceptible to local scanning worms this algorithm may be an effective defense against damaging worm outbreaks.

Provided by Pennsylvania State University