Low-cost strategy developed for curbing computer worms

January 13 2009

Thanks to an ingenious new strategy devised by researchers at University of California, Davis and Intel Corporation, computer network administrators might soon be able to mount effective, low-cost defenses against self-propagating infectious programs known as worms.

Many computers are already equipped with software that can detect when another computer is attempting to attack it. Yet the software usually cannot identify newly-minted worms that do not share features with earlier marauders. When network managers detect suspicious activity, they face a major dilemma, said Senthil Cheetancheri, who led efforts to develop the strategy. "The question is, 'Should I shut down the network and risk losing business for a couple of hours for what could be a false alarm, or should I keep it running and risk getting infected?'"

Cheetancheri, a graduate student in the Computer Security Laboratory at UC Davis when he did the work, has shown that the conundrum can be overcome by enabling computers to share information about anomalous activity. As signals come in from other machines in the network, each computer compiles the data to continually calculate the probability that a worm attack is underway. "One suspicious activity in a network with 100 computers can't tell you much," he said. "But when you see half a dozen activities and counting, you know that something's happening."

The second part of the strategy is an algorithm that weighs the cost of a computer being disconnected from the network against the cost of it being infected by a worm. Results of this ongoing process depend on the

calculated probability of an attack, and vary from computer to computer depending on what the machine is used for. The algorithm triggers a toggle to disconnect the computer whenever the cost of infection outweighs the benefit of staying online, and vice versa.

The computer used by a person working with online sales, for example, might be disconnected only when the threat of an attack is virtually certain; the benefit she provides by continuing to work during false alarms far outweighs the cost of infection. On the other hand, a computer used by a copy writer who can complete various tasks offline might disconnect whenever the probability of an attack rises above even a very low level.

The study is published in "Recent Advances in Intrusion Detection, 2008," the proceedings of a symposium that was held in Cambridge, Mass., in September, 2008.

Source: University of California - Davis