Ants vs. worms: New computer security mimics nature

Wake Forest University computer science professor Errin Fulp works with graduate students Brian Williams (center) and Wes Featherstun (far right), who worked this summer at Pacific Northwest National Laboratory developing a new type of computer network security software modeled after ants. Credit: Ken Bennett/Wake Forest University

In the never-ending battle to protect computer networks from intruders, security experts are deploying a new defense modeled after one of nature's hardiest creatures -- the ant.

Unlike traditional security devices, which are static, these "digital ants" wander through computer networks looking for threats, such as "computer worms" — self-replicating programs designed to steal information or facilitate unauthorized use of machines. When a digital ant detects a threat, it doesn't take long for an army of ants to converge at that location, drawing the attention of human operators who step in to investigate.

The concept, called "swarm intelligence," promises to transform cyber security because it adapts readily to changing threats.

"In nature, we know that ants defend against threats very successfully," explains Professor of Computer Science Errin Fulp, an expert in security and computer networks. "They can ramp up their defense rapidly, and then resume routine behavior quickly after an intruder has been stopped. We were trying to achieve that same framework in a computer system."

Current security devices are designed to defend against all known threats at all times, but the bad guys who write malware — software created for malicious purposes — keep introducing slight variations to evade computer defenses.

As new variations are discovered and updates issued, security programs gobble more resources, antivirus scans take longer and machines run slower — a familiar problem for most computer users.

Glenn Fink, a research scientist at Pacific Northwest National Laboratory (PNNL) in Richland, Wash., came up with the idea of copying ant behavior. PNNL, one of 10 Department of Energy laboratories, conducts cutting-edge research in cyber security.

Fink was familiar with Fulp's expertise developing faster scans using parallel processing — dividing computer data into batches like lines of shoppers going through grocery store checkouts, where each lane is focused on certain threats. He invited Fulp and Wake Forest graduate students Wes Featherstun and Brian Williams to join a project there this summer that tested digital ants on a network of 64 computers.

Swarm intelligence, the approach developed by PNNL and Wake Forest, divides up the process of searching for specific threats.

"Our idea is to deploy 3,000 different types of digital ants, each looking for evidence of a threat," Fulp says.

"As they move about the network, they leave digital trails modeled after the scent trails ants in nature use to guide other ants. Each time a digital ant identifies some evidence, it is programmed to leave behind a stronger scent. Stronger scent trails attract more ants, producing the swarm that marks a potential computer infection."

In the study this summer, Fulp introduced a worm into the network, and the digital ants successfully found it. PNNL has extended the project this semester, and Featherstun and Williams plan to incorporate the research into their master's theses.

Fulp says the new security approach is best suited for large networks that share many identical machines, such as those found in governments, large corporations and universities.

Computer users need not worry that a swarm of digital ants will decide to take up residence in their machine by mistake. Digital ants cannot survive without software "sentinels" located at each machine, which in turn report to network "sergeants" monitored by humans, who supervise the colony and maintain ultimate control.

Source: Wake Forest University (news : web)