New intrusion tolerance software fortifies server secrurity

June 16 2008

In spite of increased focus and large investments in computer security, critical infrastructure systems remain vulnerable to attacks, says Arun Sood, professor of computer science at George Mason University. The increasing sophistication and incessant morphing of cyber-attacks lend importance to the concept of intrusion tolerance: a system must fend off, or at least limit, the damage caused by unknown and/or undetected attacks.

"The problem is that no matter how much investment is made in intrusion prevention and detection, intruders will still manage to break through and trespass on computer servers," says Sood. "By looking at this problem from a different angle, we developed a way to contain the losses that may occur because of an intrusion."

Sood, who is the director of the Laboratory of Interdisciplinary Computer Science at Mason, along with Yin Huang, senior research scientist in the Center for Secure Information Systems at Mason, created the Self Cleansing Intrusion Tolerance (SCIT) technology to provide an additional layer of defense to security architecture with firewalls and intrusion prevention and detection systems. While typical approaches to computer security are reactive and require prior knowledge of all attack modalities and software vulnerabilities, intrusion tolerance is a proactive approach to security.

In the SCIT approach, a server that has been online is assumed to have been compromised. SCIT servers are focused on limiting the losses that

can occur because of an external intrusion, and achieve this goal by limiting the exposure time of the server to the Internet. Exposure time is defined as. the duration of time that a server is continuously connected to the Internet. Through the use of virtualization technology, duplicate servers are created and an online server is periodically cleansed and restored to a known clean state, regardless of whether an intrusion has been detected. These regular cleansings take place in sub-minute intervals.

"This approach of regular cleansings, when coupled with existing intrusion prevention and detection systems, leads to increased overall security," says Sood. "We know that intrusion detection systems can detect sudden increases in data throughput from a server, so to avoid detection, hackers steal data at low rates. SCIT interrupts the flow of data regularly and automatically, and the data ex-filtration process is interrupted every cleansing cycle. Thus, SCIT, in partnership with intrusion detection systems, limits the volume of data that can be stolen."

By reducing exposure time, SCIT provides an additional level of protection while efforts are ongoing to find and fix vulnerabilities and correct configuration errors.

Source: George Mason University