Self Cleansing Intrusion Tolerance – Next Generation Server Security

Arun Sood
asood@gmu.edu and asood@scitlabs.com
George Mason University, Fairfax, VA and SCIT Labs Inc, Clifton, VA

The complexity of modern information services, and the sophistication, pace, and variety of attack techniques requires a new thinking about the computer security problem. In spite of large investments in computer security, attackers continue to evade the most advanced intrusion prevention and detection systems. The problem stems in large part from the constant innovation and evolution of attack techniques, and rapid development of exploits based on recently discovered software vulnerabilities. We conclude – *intrusions are inevitable*. The sophisticated cyber attacks lend importance to the concept of *intrusion tolerance*: a critical system must fend off or at least limit, the damage caused by unknown and/or undetected attacks.

The current intrusion prevention (firewalls) or detection approaches require prior knowledge of all the attack modalities and software vulnerabilities. These approaches are good at fighting yesterday's wars, but what about the serious current and future threats? What about the malware installed on servers? What about inadvertent configuration errors by system administrators? Our response to these formidable challenges is Self Cleansing Intrusion Tolerance (SCIT). SCIT represents a paradigm shift as compared to firewalls and IDSs. SCIT servers are focused on limiting the losses that can occur because of an intrusion. To achieve this goal we limit the exposure time of the server to the internet. In the SCIT approach we have achieved sub-minute exposure time for servers without service interruption. We emphasize that SCIT is not a replacement technology but instead complements and adds to existing approaches.

Today's servers are on-line for extended periods – often several months at a time. In general, servers are brought off-line only for patch application or upgrades. Thus, attackers have ample time to explore, experiment and understand the server configuration. In this sense, the servers are sitting ducks and easy targets. SCIT technology, intends to make the task of the attackers more difficult by limiting the exposure time of the servers. SCIT facilitates the use of different forms of diversity to constantly change the system configuration, change what the attacker sees, and this, in turn, makes the attacker's task more difficult.

Our underlying assumption is that all software has vulnerabilities. Further, the more complex the software, the greater the likelihood of vulnerabilities and constant patching of the software has now become a costly operation. There are many on-going efforts to develop methodologies that will lead to less vulnerable software products. In the meantime, for servers exposed to the internet, like those servers in the DMZ, SCIT provides an additional layer of defense.

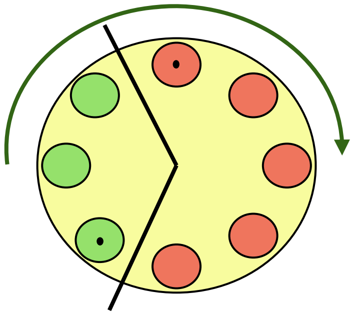
SCIT technical publications are available at http://cs.gmu.edu/~asood/scit. A Google search shows that in the last three months there have been many news reports about SCIT. This includes articles in Network World, Computer World, Dark Reading, etc and some blogs. Pointers to a few articles are included at the above website. This shows the increasing interest in intrusion tolerance as a viable strategy.

Our research has been supported by the US Army, NIST through the Critical Infrastructure Protection Program, SUN Microsystems, with on-going support from Lockheed Martin, and Commonwealth of Virginia CTRF fund (Northrop Grumman is a partner). CTRF funds supports commercialization of developed technology at Virginia universities.

"First there was intrusion detection, then intrusion prevention, and now, intrusion *tolerance*. A professor and researcher at George Mason University is readying the commercial rollout of a new, patent-pendir technology that basically assumes an attacl infection on a server is inevitable, so it inst minimizes the impact of an intrusion."
Dark Reading, 15 May 2008
"Software makes virtual servers a moving target. Innovation seeks to pull servers off before attackers can do their work."
Network World, 19 June 2008

How SCIT Technology Works
Using virtualization technology, SCIT rotates pristine virtual servers and applications every sixty seconds or less.

In the graphic below, five online virtual servers (shown in red) are processing transactions while three offline servers are being cleaned and restored to a pristine state. Every minute a pristine "green" server is swapped out with a "red" server and the SCIT process begins again.



SCIT servers will be tested at Northrop Grumman TRIAD Labs in 2008 Q4 and 2009 Q1.

Dr. Arun Sood is Professor of Computer Science, Director of Laboratory of Interdisciplinary Computer Science, and Co-Director of International Cyber Center at George Mason University, Fairfax, Virginia. He was formerly department chair. He is CEO of a SCIT Labs Inc - start up that is licensing SCIT technology from the university. He has published more than 150 papers, and two edited books. He has been awarded 1 patent, and has applied for 4 patents based on SCIT. His research has been supported by the government and private sector. List of publications and a detailed resume is available at http://cs.gmu.edu/~asood. He was awarded BTech (1966) from Indian Institute of Technology, Delhi, and MS (1967) and PhD (1971) by Carnegie Mellon University. All degrees in Electrical Engineering.