SCIT Reduces Zero Day and APT Induced Losses

(Slaying Cyber Security Myths)

Arun Sood
Professor Computer Science and Co-Director International Cyber Center,
George Mason University, Fairfax, VA 22030
and
Founder, SCIT Labs, Clifton, VA
{asood@gmu.edu , asood@scitlabs.com}

Cyber risk is a product of threats, vulnerabilities and consequences. Driving any one of these to zero, will achieve zero risk. Most of us do not have a James Bond 007 license and thus cannot eliminate threats. For some time the general belief has been that all vulnerabilities can be eliminated, thus driving cyber risk to zero. Are there any CISOs who are telling their CEOs that all vulnerabilities are eliminated? Detection is a much more difficult problem than most expected. In our work, we believe that intrusions are inevitable and focus on reducing the consequences of a successful intrusion.

If we rely exclusively on the current reactive systems, then the virtualized servers, or the cloud, are going to be no more secure than the existing systems. In fact, multi tenancy, additional software, sharing of the memory resources, sharing of the internal data paths like the internal buses, all point to the possibilities of additional vulnerabilities, with shared resources providing a path for spreading the impact of an initial foot hold intrusion. However, this is only part of the story - the virtualized and clustered computer environments provide the system designer new opportunities to improve system security.

In this talk we present Self Cleansing Intrusion Tolerance (SCIT) a patented novel approach for reducing cost of intrusions. This Moving Target Defense (MTD) strategy leads to higher level of cyber defense. We show through experimental results and simulations that using SCIT results in much lower data ex-filtration losses even for zero day and APT attacks. Another interesting result of our work is that combining reactive and proactive systems provides significant advantage as compared to either separately.

The SCIT strategy effectively converts static servers into dynamic systems. In this way, we can facilitate a new series of strategies to effectively protect physical systems and virtualized environments including the cloud.

Arun K. Sood
Professor Computer Science & Director International Cyber Center, George Mason University
and Founder, SCIT Labs Inc
{ asood@gmu.edu, asood@scitlabs.com }

Dr. Arun Sood is Professor of Computer Science in the Department of Computer Science, and Director of the International Cyber Center at George Mason University, Fairfax, VA. His research interests are in security architectures; image and multimedia computing; performance modeling and evaluation; simulation, modeling, and optimization.

He and his team of faculty and students have developed a new approach to server security, called Self Cleansing Intrusion Tolerance (SCIT). We convert static servers into dynamic servers and reduce the exposure of the servers, while maintaining uninterrupted service. This research has been supported by US Army, NIST through the Critical Infrastructure Program, SUN, Lockheed Martin, Commonwealth of Virgina CTRF (in partnership with Northrop Grumman). SCIT technology was winner of the Global Security Challenge (GSC) sponsored Securities Technologies for Tomorrow Challenge.

Dr Sood is Founder and CEO of SCIT Labs, a university start up, which is commercializing SCIT technology. He received B.Tech degree from the Indian Institute of Technology (IIT), Delhi, and the M.S. and Ph.D. degrees in Electrical Engineering from Carnegie Mellon University. His research has resulted in more than 180 publications, 2 edited books, 8 patents and 1 pending patent applications. His resume including publications list is available at http://cs.gmu.edu/~asood.