HyperCheck: A Hardware-Assisted Integrity Monitor

Speaker: Prof. Angelos Stavrou
Department of Computer Science
George Mason University

Friday, March 25, 2011
1:00PM-2:00PM, NVC 325

Abstract

Over the past few years, virtualization has been employed to environments ranging from densely populated cloud computing clusters to home desktop computers. Security researchers embraced virtual machine monitors (VMMs) as a new mechanism to guarantee deep isolation of untrusted software components. Unfortunately, their widespread adoption promoted VMMs as a prime target for attackers. In this talk, I will present HyperCheck, a hardware-assisted tampering detection framework designed to protect the integrity of VMMs and, for some classes of attacks, the underlying operating system (OS). HyperCheck leverages the CPU System Management Mode (SMM), present in x86 systems, to securely generate and transmit the full state of the protected machine to an external server. Using HyperCheck, we were able to ferret-out rootkits that targeted the integrity of both the Xen hypervisor and traditional OSes. Moreover, HyperCheck is robust against attacks that aim to disable or block its operation. Our experimental results show that HyperCheck can produce and communicate a scan of the state of the protected software in less than 40 ms.

Biography

Angelos Stavrou is an Assistant Professor in the Computer Science Department and a member of the Center for Secure Information Systems at George Mason University, Fairfax, Virginia. He received his M.Sc. in Electrical Engineering, M.Phil., and Ph.D. (with distinction) in Computer Science, all from Columbia University. He also holds an M.Sc. in theoretical Computer Science from the University of Athens, and a B.Sc. in Physics with distinction from the University of Patras, Greece. His current research interests include security and reliability for distributed systems, security principles for virtualization, and anonymity with a focus on building and deploying large-scale systems. He is a member of the ACM, the IEEE, and USENIX. Contact him at astavrou@gmu.edu.