VirginiaTech
VIRGINIA POLYTECHNIC INSTITUTE AND STATE UNIVERSITY

Computer Science Seminar Series, 2014

National Capital Region

Hardware-Assisted Isolated Computing Environments

Speaker: Dr. Kun Sun
George Mason University

Friday, March 28, 2014

Abstract

Protecting commodity systems with commercial Operating Systems without significantly degrading performance or usability still remains an open problem. Recent research has shown the need for trustworthy isolated computing environments where the user can segregate different activities to lower risk of cross-contamination after an infection and introspect the state of untrusted computing environments. In this talk, we first introduce a novel BIOS-assisted mechanism to enable secure instantiation and management of isolated computing environments, tailored to separate security-sensitive activities from untrusted ones on x86 architecture. Our system can quickly and securely switch between operating environments without requiring any specialized hardware or OS and application code modifications. Even if the untrusted OS becomes compromised, there is no potential for exfiltration or inference attack against data in the trusted OS. The switching time in our prototype is approximately six seconds. Second, we introduce a hardware-assisted dependability framework that leverages System Management Mode (SMM) to inspect the state of a system. Contrary to Virtual Machine Introspection (VMI), our trusted code base is limited to BIOS and the SMM implementations. It is capable of transparently and quickly examining all layers of running system code including a hypervisor, the OS, and user level applications. We demonstrate several use cases including heap spray, heap overflow, and rootkit detection using real-world attacks on Windows and Linux platforms. Our system is 100 times faster than similar VMI systems.

Biography

Dr. Kun Sun is a Research Professor in Center for Secure Information Systems (CSIS) at George Mason University. He received his Ph.D. in Computer Science from North Carolina State University in 2006. Dr. Sun was a Research Scientist in Intelligent Automation Inc. between 2006 and 2010. In 2010, Dr. Sun joined George Mason University to restart his academic career. His current research focuses on trustworthy computing environment, moving target defense, smart phone security, cloud security, and wireless security.