Seminar Talk

Kun Sun, PhD

Assistant Professor,
Department of Computer Science,
College of William and Mary

Friday, April 8, 2016
3:00 p.m. KH 224

Title: CacheKit: Evading Memory Introspection Using Cache Incoherence

Abstract:
With the growing importance of networked embedded devices in the upcoming Internet of Things, new attacks targeting embedded OSes are emerging. ARM processors, which power over 60% of embedded devices, introduce a hardware security extension called TrustZone to protect secure applications in an isolated secure world that cannot be manipulated by a compromised OS in the normal world. Leveraging TrustZone technology, a number of memory integrity checking schemes have been proposed in the secure world to introspect malicious memory modification of the normal world. In this paper, we first discover and verify an ARM TrustZone cache incoherence behaviour, which results in the cache contents of the two worlds, secure and non-secure, potentially being different even when they are mapped to the same physical address. Furthermore, code in one TrustZone world cannot access the cache content in the other world. Based on this observation, we develop a new rootkit called CacheKit that hides in the cache of the normal world and is able to evade memory introspection from the secure world. We implement a CacheKit prototype on Cortex-A8 processors after solving a number of challenges. The experimental results show that CacheKit can successfully evade memory introspection from the secure world and has small performance impacts on the rich OS. We discuss potential countermeasures to detect this type of rootkit attack.

Bio:
Dr. Kun Sun is an assistant professor in the Department of Computer Science at College of William and Mary. He received his Ph.D. in Computer Science from North Carolina State University in 2006. His research focuses on systems and network security. Dr. Sun has more than 10 years working experience in both industry and academia. Before joining W&M, he was a Research Professor in George Mason University. Before that, he was a Senior Research Scientist in Intelligent Automation Inc. at Rockville Maryland. He was a Member of the Technical Staff at Bell Labs, Lucent Technology in 2000. His current research focuses on trustworthy computing environment, moving target defense, smart phone security, and password management.