VirginiaTech
VIRGINIA POLYTECHNIC INSTITUTE AND STATE UNIVERSITY

Computer Science Seminar Series

National Capital Region

Using ARM Cache Incoherence for Good and Bad

Speaker: Prof. Kun Sun
George Mason University

Wednesday, February 28, 2018
1:00PM- 2:00PM, NVC 325

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. We observe and verify an ARM TrustZone cache incoherence behavior, which results in the cache contents of the two worlds, secure world and normal world, 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 first develop a new cache-based rootkit called CacheKit that hides in the cache of the normal world and is able to evade memory introspection from the secure world. The experimental results show that CacheKit can successfully evade memory introspection from the secure world and has small performance impacts on the rich OS. Second, we develop a cache-assisted secure execution framework, called CaSE, on ARM processors to defend against sophisticated attackers who can launch multi-vector attacks including software attacks and hardware memory disclosure attacks.

Biography

Dr. Kun Sun is an associate professor in the Department of Information Sciences and Technology at George Mason University. He is also the director of Sun Security Laboratory. He received his Ph.D. in Computer Science from North Carolina State University in 2006. Before joining GMU, he was an assistant professor in College of William and Mary. His research focuses on systems and network security. Dr. Sun has more than 15 years working experience in both industry and academia, publishing over 60 conference and journal papers. His current research focuses on trustworthy computing environment, moving target defense, smart phone security, and password management.