Designing Secure Heterogeneous Multicore Systems from Untrusted Hardware and Software Components

Michel A. Kinsy
Boston University, Boston MA

2:30 pm, April 12, 2018
RSCH 163

Abstract:

The emergence of general-purpose system-on-chip (SoC) architectures has given rise to a number of significant security challenges. The current trend in SoC design is system-level integration of heterogeneous technologies consisting of a large number of processing elements such as programmable RISC cores, memories, DSPs, and accelerator function units/ASIC. These processing elements may come from different providers, and application executable code may have varying levels of trust. Some of the pressing architecture design questions are: (1) how to implement multi-level user-defined security; (2) how to optimally and securely share resources and data among processing elements; (3) how to use reconfiguration for the purpose of obfuscation to attackers.

In this talk, I will present two design cases of secure multicore architecture: (1) *Hermes*, an architectural framework for integrating multiple processing elements (which may include secure and non-secure cores) into the same chip design, while (i) maintaining individual tenant security, (ii) preventing data leakage and corruption, and (iii) promoting collaboration among the tenants. The *Hermes* architecture is based on a programmable secure router interface and a trust-aware routing algorithm; (2) *Sphinx*, a hardware-software co-design architecture for binary code and runtime obfuscation. The Sphinx architecture uses binary code diversification and self-reconfigurable processing elements to maintain application functionality while obfuscating the binary code and architecture states to attackers. This approach dramatically reduces an attacker's ability to exploit information gained from one deployment to attack another deployment.

Bio:

Michel A. Kinsy is an Assistant Professor in the Department of Electrical and Computer Engineering at Boston University (BU), where he directs the Adaptive and Secure Computing Systems (ASCS) Laboratory. He focuses his research on computer architecture, interconnection networks, hardware-level security and cyber-physical systems. He is an MIT Presidential Fellow, DFT'17 Best Paper Award Finalist, FPL'11 Tools and Open-Source Community Service Award Recipient. Dr. Kinsy earned the PhD in Electrical Engineering and Computer Science in 2013 from the Massachusetts Institute of Technology. His doctoral work in algorithms to emulate and control large-scale power systems at the microsecond resolution inspired further research by the MIT spin-off Typhoon HIL, Inc. Before joining the BU faculty, Dr. Kinsy was an assistant professor in the Department of Computer and Information Systems at the University of Oregon, where he directed the Computer Architecture and Embedded Systems (CAES) Laboratory. From 2013 to 2014, he was a Member of Technical Staff at MIT Lincoln Laboratory and a core-lead member of the Advanced Computer Architecture Concepts sub-group tasked with exploring future secure computing architectures in critical DoD systems. He holds an M.S. in Electrical Engineering and Computer Science from MIT, a B.S.E. in Computer Systems Engineering and a B.S. in Computer Science from Arizona State University.