BINGHAMTON UNIVERSITY
STATE UNIVERSITY OF NEW YORK | Computer Science

THE DEPARTMENT OF COMPUTER SCIENCE & THE COMPUTER SCIENCE GRADUATE STUDENT ORGANIZATION (GSOCS) PRESENT

INVITED SPEAKER SERIES

Dr. G. Edward Suh
Cornell University

Friday, 12/2 at noon, EB-110 (Engineering Building, Main Campus)

Title: Secure Multi-Core Processors with Comprehensive and Verifiable Information Flow Control

Abstract: As computing devices are increasingly shared by multiple software entities, hardware-level protection for critical software is essential for a strong security guarantee. This talk will show how static information flow analysis and micro-architecture timing-channel protection can be used to build a multi-core system with comprehensive and verifiable information flow assurance, and briefly discuss how such a system can be leveraged in the context of a self-driving car to protect safety-critical functions.

The first part of the talk will introduce a secure hardware design language, named SecVerilog, which enables designers to statically analyze information flow at the hardware level and thus to build systems where information channels are verifiably controlled. SecVerilog is Verilog, extended with security type annotations, and provides rigorous formal assurance that a hardware design enforces timing-sensitive noninterference. Our experiences suggest that SecVerilog can be used to verify security properties of realistic hardware designs with low overhead. For example, we used SecVerilog to build a processor with a verifiable guarantee on timing channel protection as well as to detect implementation bugs in hardware security architecture similar to ARM TrustZone. The second part of the talk will discuss how today's multi-core processors can be re-designed to control micro-architectural timing channels among software entities sharing the same hardware. The timing channel protection enables comprehensive control of information flows that are visible to software attacks. This talk will discuss the sources of timing channels in today’s multi-core processor and show how shared hardware components can be augmented to remove timing channels.

Bio: G. Edward Suh is an Associate Professor in the School of Electrical and Computer Engineering at Cornell University. He received a Ph.D. degree in Electrical Engineering and Computer Science from the Massachusetts Institute of Technology (MIT) in 2005. Following the graduate school, he spent a year at Verayo Inc., leading the development of unclonable RFIDs and secure embedded processors before joining Cornell. His research interests span computer systems in general with particular focus on developing architectural techniques to improve security and efficiency of future computing systems. He is a recipient of an NSF CAREER award, an Air Force Office of Scientific Research (AFOSR) Young Investigator Program award, and an Army Research Office (ARO) Young Investigator Program award. His work on dynamic information flow tracking won the 2014 most influential paper award from the International Conference on Architectural Support for Programming Languages and Operating Systems (ASPLOS).