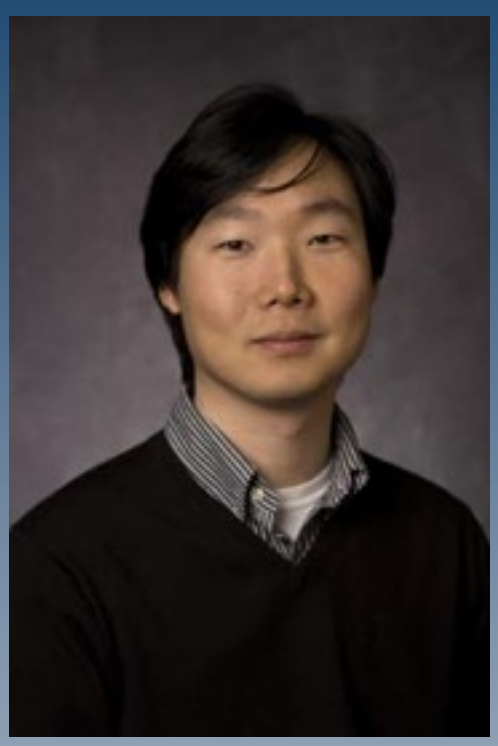
Hardware-Assisted Run-Time Monitoring for Trustworthy Computing Systems

Edward Suh

Cornell University

Thursday, October 27th @ 4PM, 3405 Siebel Center



Abstract

Hardware-enabled security techniques promise to greatly enhance the trustworthiness of future computing systems through their efficiency and tamper resistance. As an example, parallel run-time monitoring in hardware can help ensuring a range of security and correctness properties such as memory safety, information flow restrictions, and others with minimal overheads. In practice, however, fixed-function hardware is often difficult to justify due to their inflexibility and high development costs.

This talk will discuss how selective hardware reconfigurability and heterogeneity can enable a flexible yet efficient platform for instruction-grained run-time monitoring, and show how the monitoring capabilities can be utilized for trust. For monitoring of explicit program properties, our architecture utilizes on-chip reconfigurable fabric (FPGA) along with dedicated logic in order to provide flexibility and efficiency. The reconfigurable fabric can dynamically adapt to a range of monitoring and bookkeeping functions based on application needs without expensive hardware re-design and fabrication. At the same time, the bit-level reconfigurable logic is often more efficient for simple checks than traditional processing cores. In addition to explicit checks, software properties can also be implicitly checked through comparing behaviors of diverse program replicas. In this context, our design introduces a heterogeneous multi-core architecture that can effectively exploit redundancy among replicas. Experimental results suggest that run-time monitoring on these architecture designs can closely match performance and energy efficiency of dedicated hardware mechanisms while providing programmability. Along with the architecture optimizations, the talk will also discuss a set of run-time program monitoring techniques including dynamic information flow tracking, memory safety checks, and an extension to data races for concurrency bug detection, illustrating benefits of fine-grained monitoring.

G. Edward Suh is an Assistant 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 efficiency, security, and correctness of future computing systems. Ongoing research topics include parallel and reconfigurable architecture for security and reliability, embedded cyber-physical systems, flash memory security, and mathematically optimized on-chip network design and management. 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.

Illinois-Intel Parallelism Center (I2PC) Distinguished Speaker Series

i2pc.cs.illinois.edu

http://media.cs.illinois.edu/live/I2PClive.asx

http://i2pc.cs.illinois.edu/chat

I2PC