Design and Verification of Security-aware Processors

Ruby B. Lee

Abstract: Today, supporting security in computers is not an option but a necessity. Using hardware in processors to enable more secure software and systems is very promising. However, security is new to processor designers and tools for verifying the security provided are sorely lacking. To illustrate what needs to be verified, I will discuss proposed hardware-software security architectures. These include new features that can be added to existing processor architectures and microarchitectures to facilitate confidentiality and integrity protection for secret or sensitive data and programs. For example, the Bastion security architecture's goal is to show that trusted software modules can be protected within an untrusted software stack – in particular, the commodity Operating System is untrusted, or can be compromised by attackers. Carefully designed trusted software modules can provide very flexible security functionality, are smaller and easier to verify, and are themselves protected by the processor and hypervisor -- thus leading to a "general-purpose" security architecture.

How can we verify the security properties that are provided in the design? Ideally the same simulation platform can enable both security and performance verification. However, this has not been possible since security verification needs full system simulations (including hypervisor, operating system, networking and applications), while performance evaluation needs cycle-accurate simulation of the processor with the new hardware features. Also, existing formal verification techniques do not scale, and current verification tools typically apply to only software or only hardware, but not both. Furthermore, security benchmarks and attack suites are needed. We discuss the huge need for a security verification tool-chain that can help hone the design for security-aware processors, to enable their deployment, and thus help to improve cyber security.

Biography: Ruby B. Lee is the Forrest G. Hamrick Professor of Engineering at Princeton University. Her current research is in security-aware computer architecture, secure cloud computing, trustworthy hardware, secure multicore chips, smartphone security and security verification. Prior to Princeton, Lee served as chief architect at Hewlett-Packard for processor architecture, multimedia architecture, and then security architecture. She was a founding architect of HP's PA-RISC architecture and instrumental in the initial design of several generations of PA-RISC processors for HP's business and technical computer product lines. She also has experience helping the widespread adoption of multimedia in commodity products, by pioneering data-parallelism support for multimedia in microprocessors and supporting the first realtime software video in low-end products. She was co-leader of the Intel-HP Itanium multimedia architecture team. She created the first security roadmap for enterprise and e-commerce security for HP before going to Princeton. Lee is an ACM Fellow and IEEE Fellow, and holds over 120 U.S. and international patents. Known for her hardware security expertise, Lee is often asked

to serve on national committees for improving cyber security research, such as being a co-leader of the U.S. National Cyber Leap Year Summit and co-authoring the National Academies' study mandated by Congress for improving cyber security research.