Hardware Enhanced Security

Ruby Lee
Princeton University
Princeton, NJ
rblee@princeton.edu

Simha Sethumadhavan
Columbia University
New York NY
simha@cs.columbia.edu

G. Edward Suh
Cornell University
Ithaca, NY
suh@csl.cornell.edu

ABSTRACT
Building a secure computing system requires careful coordination among all layers in the system from hardware to software. Even if secure by itself, a higher layer protection mechanism may be bypassed if lower layer software or hardware is vulnerable. Additionally, hardware complements software through its efficiency, tamper resistance, etc. There have been significant efforts recently in hardware communities that aim to leverage hardware strengths to secure software layers, and also to secure hardware itself. This tutorial presents some of these hardware-enhanced security techniques to the security community.

Categories and Subject Descriptors
C.0 [**General**]: System Architectures; K.6.5 [**Management of Computing and Information Systems**]: Security and Protection

General Terms
Security, Design

Keywords
Hardware security, Hardware Trojan, Side channel attacks, Secure processors, PUF, Secure cloud computing.

1. INTRODUCTION
Current security research is largely oriented to top-down design where the most exposed layers of the system, the network/application layers, are first studied assuming that the lower layers are secure, even when they are not. The lower layers are studied only when new threats appear at those layers. Security has thus become, as the cliché goes, an arms race to the bottom. There are many examples in the literature of lower-layer attacks including those that target anti-virus scanners, libraries, OS, hypervisors, and even code stored in non-volatile ROM. For every software mitigation strategy, vulnerabilities at the same level or in the software layer below can be used to attack and weaken the mitigation strategy.

A longer-term solution to this problem is to push security mechanisms down to the hardware, which is one component of the system that is typically immutable. The increasing number of on-chip transistors and multicore chips provide an opportunity to explore hardware-enhanced security systems. In addition to immutability and nonbypassability offered by hardware, there are four further additional advantages to implementing hardware security mechanisms. First, hardware-supported security mechanisms are much more energy-efficient than software-supported mechanisms. Given current energy- and power-efficiency trends, hardware support may be essential for security techniques to gain traction in the real world. Second, hardware offers unmatched visibility into program execution, creating opportunities for novel ways to improve systems security. Third, small hardware modifications, amounting to few lines of code, offer significant protections to trillions of lines of software. Further, because of nature of hardware construction of security features it is much more feasible to provide useful measures of security for hardware-hardened schemes.

In this context, there have been significant efforts recently that aim to secure hardware itself and also leverage strengths of hardware in securing software layers. For example, to build a more secure hardware foundation, researchers have investigated ways to protect against backdoors built into hardware (hardware Trojans) and timing channels through shared hardware resources such as caches. To complement limitations of software layers, researchers have also proposed to leverage hardware architecture to provide protection against physical tampering, reduce the trusted software base and its attack surface. Similarly, at a lower level, noise and variations in hardware have been studied as sources for true random numbers and device-specific secrets. This tutorial will provide a peek into the emerging area of hardware-hardened security systems.

2. AGENDA
We will discuss hardware trends and provide a very brief outline of research in hardware security support. We will discuss how hardware can support more secure software environments and cloud computing systems. We will also cover state-of-the-art research techniques for more secure hardware construction, including backdoor-free hardware, leak-free hardware and useful hardware primitives such as PUFs. We will close with a discussion on how hardware and security researchers can engage better. The tutorial will cover some of the following topics:

- Hardware trends, overview of hardware security support
- Secure processor and multicore architectures
- Secure cloud computing
- Hardware backdoors and Trojans
- Hardware mitigation of cache side channels
- Physical Security Functions - PUFs, RNGs, etc.

3. Intended Audience
The tutorial will be targeted towards security researchers and practitioners with some basic understanding of computer architecture.

CCS'12, October 16–18, 2012, Raleigh, North Carolina, USA.
ACM 978-1-4503-1651-4/12/10.