Trusted Hardware

Radu Sion
Stony Brook Trusted Hardware Laboratory
sion@cs.stonybrook.edu

Summary. Increasingly, modern networked storage and computation services are fundamentally vulnerable to faulty behavior and malicious compromise. In online, un-trusted environments, security, privacy and correctness assurances become essential functionality requirements. However, achieving such assurances *efficiently* is extremely challenging. Scalability requirements often do not allow for centralized points of trust, while distributed alternatives are rarely practical due to large computation and communication overheads.

The advent of *general-purpose* trustworthy hardware offering tamper-resistance and reactivity, allows for fundamentally new paradigms of trust. Trust chains spanning untrusted and possibly hostile environments can now be built by deploying such secure tamper-proof hardware at the service processing components' site. The trusted hardware will run certified logic on behalf of service clients; close data-proximity coupled with tamper-resistant guarantees allow an optimal balance and partly de-coupling of the efficiency-security trade-off. Long speculated about , technology has now matured sufficiently to enable such applications. Computing can now be both efficient and secure.

In this tutorial we explore secure tamper-proof hardware deployed in the design and implementation of trusted, efficient, and scalable computing. Specifically, we discuss known *vulnerabilities and attacks*, adversarial and deployment *models* and provide an *hands-on programming* session for hardware ranging from simple TPM microcontrollers and smart-cards, on-disk encryption mechanisms such as Seagate's Full Disk Encryption (FDE) units , to full-fledged FIPS 140-2 Level 4 certified IBM 4758 and the newer IBM 4764 PCI-X cryptographic coprocessors.

An important part of the tutorial will lie in conveying the insights of how practical limitations of trusted hardware devices pose a set of significant challenges in achieving sound assurances in practical applications in financial (trading systems, online banking, ATMs), commercial, governmental and defense applications. Specifically, heat dissipation concerns under tamper-resistant requirements limit the maximum allowable spatial gate-density. As a result, e.g., general-purpose secure co-processors (SCPUs) are often significantly constrained in both computation ability and memory capacity, being up to one order of magnitude slower that host CPUs. We will explore how to achieve efficiency in this setting.

Speaker. *Radu Sion* is an assistant professor of Computer Sciences in Stony Brook University, heading the Network Security and Applied Cryptography Laboratory. His research focuses on data security and information assurance mechanisms. He has been applying practical cryptography and strong assurance mechanisms to achieve practical data privacy solutions, develop efficient regulatory compliant systems, cellular DRM solutions and conditional micro-payment schemes. Sion also directs the Stony Brook Trusted Hardware Laboratory, a central expertise and research knowledge repository on secure hardware. Collaborators and funding partners include Motorola Labs, Xerox/Parc, IBM Research, the IBM Cryptography Group, the Center of Excellence in Wireless and Information Technology CEWIT, the Stony Brook Office for the Vice-President for Research and the National Science Foundation. Sion serves on the organizing committee and steering boards of conferences such as CCS, NDSS, FC, USENIX Security, SIGMOD, ICDE, ICDCS, a.o.