Special Session 11B: Hot Topic
Hardware Security: Design, Test and Verification Issues

Organizers:
Dr. Swarup Bhunia, Case Western Reserve University, *swarup.bhunia@case.edu*
Dr. Anand Raghunathan, Purdue University, *raghunathan@purdue.edu*

Moderator:
Dr. Swarup Bhunia, Case Western Reserve University, *swarup.bhunia@case.edu*

Presenters:
Pankaj Rohatgi, Cryptography Research, *Side-channel Analysis: Attacks and Countermeasures*
Steve Weingart, ATSEC, *Considering Security Standards While Designing Devices and Systems*
Yiorgos Makris, Yale University, *Hardware Trojans and Trust in ICs*

Abstract

Security is rapidly becoming a critical factor in the IC design and test cycle. To provide higher levels of assurance and trust to designers, manufacturers and end users of integrated circuits (ICs), there is a need to integrate security measures during design, validation, and manufacturing test covering all aspects of security threats in hardware. These threats include secret information leakage, malicious hardware modifications in an untrusted foundry, hardware IP piracy and reverse engineering efforts. This session will have three presentations focusing on the design, validation, and test challenges for attack-resistant secure hardware systems.

The first presentation will provide an introduction to side-channel attacks and associated countermeasures. With the growing usage of cryptography and the deployment of highly sensitive designs in hardware and embedded systems, there is an increasing need to protect design secrets and keys held within these devices from physical and logical attacks. *Side-channel analysis* represents a major, non-invasive and practical threat to such systems, since these attacks can be mounted on a variety of device form factors and are able to extract secret-keys and sensitive information very effectively with only a moderate effort by collecting and analyzing additional sources of information, such as timing, power consumption or electromagnetic (EM) emanations. This presentation will introduce side-channel analysis and techniques such as simple and differential power and EM analysis and describe different classes of countermeasures that can be used to defend against side-channel attacks. Currently, a rigorous approach to designing and testing for side-channel resistance is lacking and developing side-channel resistant solutions is a process of trial and error. Finally, it will describe some of the key requirements and challenges in developing a design and testing methodology and tools for side-channel resistant solutions.

The second presentation will focus on the application of standards to secure device and system design. As the skills of the attackers increase, so must the security and integrity protection of computing systems. This task has been made more difficult as some of the security measures being developed, from tamper resistance to cryptographic algorithms, are not as strong as a developer may claim. This has made it more difficult for a device or system designer to know what to use, or how to use it. In addition, in most cases the end user has no way to judge the efficacy of a given security measure. With these issues in mind, standards have been developed to give designers a point of reference; and users can choose products that have been verified to meet standards. Standards include both security requirements (tamper resistance and response, key management, zeroization and the like), and interoperability requirements (algorithm modes and methods, endianess, etc), to ensure both security and compatibility. However, standards are not perfect. Systems and methods are evolving so rapidly that most standards have to bend and adjust to changing demands. This presentation will discuss the application of standards in terms of requirements on the design, and things to consider during design, to meet standards. Besides, typical side door attacks (attacks that circumvent the security), and the general concept of a security boundary will be discussed.

The third presentation will discuss the problem and review the current state-of-the-art in hardware Trojan detection. The problem of maliciously intended modifications (a.k.a. *hardware Trojans*) in manufactured ICs has recently become of interest not only to academic researchers but also to governmental agencies and industrial entities. Partly because of design outsourcing and migration of fabrication foundries to low-cost areas across the globe, and partly because of increased reliance on external hardware intellectual property (IP) and Electronic Design Automation (EDA) software from various vendors, the integrated circuit supply chain is now considered far more vulnerable to such malicious modifications than ever before. Fears that skillful and resourceful adversaries may be able to compromise some stage of IC design and/or fabrication and insert Trojan hardware are becoming increasingly intense, as rumors about actual occurrence of such cases surface. This presentation will highlight the fundamental concern that hardware Trojan-infested chips may be capable of additional functionality which is unknown to the designer/vendor/customer and which can be exploited by the perpetrator after chip deployment. In addition, it will discuss emerging solutions to detect malicious modifications in ICs and validate hardware trust considering different forms of hardware Trojan attacks.

978-1-4244-6650-4/10/$26.00 ©2010 IEEE