Hardware Security: Preparing Students for the Next Design Frontier

Farinaz Koushanfar
Electrical and Computer Engineering Dept.
Rice University
farinaz@rice.edu

Miodrag Potkonjak
Computer Science Dept.
University of California, Los Angeles
miodrag@cs.ucla.edu

Abstract

Hardware security (HS) has emerged as a premier design and manufacturing objective due to the confluence of economic, social, and technology forces. HS encompasses a wide spectrum of research and development directions ranging from intellectual property (IP) protection, hardware metering, and hardware Trojan horse detection, to design of secure smart cards, voting hardware, detection of explosives and chemical and biologic toxic materials, and protection of physical containers using electronic locks. Development of HS synthesis and evaluation tools have recently received a great deal of attention. However, to the best of our knowledge, no HS courses have been introduced into computer engineering curricula. We summarize the course that was introduced at UCLA and Rice University, present its evaluation, and anticipate future directions to create an even more influential class.

1 Rationale

In the 70's, *area* emerged as the dominant synthesis and design objective for integrated circuit (IC), in the '80s the objective was *speed of execution*, and in the 90's it became *power*. While all these objectives are still very important, security, privacy, and digital right management (DRM) arise as the most important metrics in many modern and emerging applications [7]. The paradigm shift toward DRM, security and privacy is not only due to the common impact of technology push and applications pool, but also it is a consequence of an inherently insecure but dominant *horizontal microelectronic business model* and *design reuse*. The horizontal model is where the design houses, silicon foundries, and system integrators are economically separate entities; hardware IP reuse is to alleviate the design productivity gap.

In preparing students for designing secure hardware, the most challenging is that the intrinsic nature and concepts needed for ensuring security are sharply different from the ones for area, speed, or power optimization. In addition, HS has close interactions with the underlying technologies, system software, and applications. Another significant hurdle is that a high percentage of students do not have a solid background in security.

Our strategic goal is to prepare students for synthesis and evaluation of secure devices and systems. The main technical objectives of the course include understanding of security and DRM mechanisms such as non-destructive observability, IC uniqueness, and methods for hiding information inside the design specifications. A special focus is placed on sound foundation and complete coverage of attacks - defense mechanisms and protocols -, and analysis and complete understanding of the assumptions and models. We also emphasize the importance of preserving transparency of the synthesis process in realizing the HS features.

2 Topics

In the offerings so far, we covered in technical details various subsets of the following topics: (i) smart cards; (ii) manufacturing variability and HW security; (iii) watermarking of designs; (iv) IC fingerprinting; (v) IC metering (vi) HW Trojan horse detection; (vii) IC rapid aging attacks that exploit HCI (hot carrier induced degradation), TDDB (time dependent dielectric [soft/hard] breakdown) and NBTI (negative bias temperature instability) deep-submicron transistor degradation and interconnect electromigration. (viii) obfuscation of the specification of designs and nonreadability of data and computation against power, delay, and radiation attacks; (ix) physically unclonable functions; (x) secure coprocessor, algorithmic HW attacks, and buffer overflow attacks; (xi) HW identification using clock skew and manufacturing variability techniques; (xii) voting HW; (xiii) biometrics techniques and HW; (xiv) jamming and time synchronization attacks in wireless networks; (xv) explosives, chemical, and biologic toxic material detection; and (xvi) security of physical objects such as locks and digital IDs. We briefly elaborate on a sample of the covered topics:

- **Radio frequency identification (RFID).** An RFID tag

2007 IEEE International Conference on Microelectronic Systems Education (MSE'07)
0-7695-2849-X/07 $20.00 © 2007 IEEE

is a device used for an automatic identification [3]. The tags are attached to products or moving objects to identify them based on the locally stored IDs and radio-frequency communication to the remote servers to retrieve the data.

- **Watermarking (WM).** Watermarking is used to securely authenticate the source of an artifact. Digital WM has been applied to the protection of intellectual property (IP) in digital form [8, 5]. WM maybe horizontal or vertical; horizontal marks a specific step of the synthesis or layout process with a unique signature, while vertical marks the at a higher functionality level, and thus, vertically signs all the subsequent synthesis and layout levels.
- **HW metering.** IC *metering* is a set of security protocols that enable the design house to gain post-fabrication control by passive or active control of the number of produced ICs, their properties and use, or by runtime disabling of ICs in case of tamper detection [4].
- **HW Trojan horse detection.** A Trojan horse is a design that disguises itself as the original design, by mimicking the functionality of the original, and adding circuitry or other extra parts before or during the fabrication, to gain access or control to the functional HW or to destroy its functionality [1]. HW Trojan horse detection checks a pertinent IC for presence of malicious or unintentional alterations of design specifications that compromise the correctness of the functionality under specific conditions.
- **Physically Unclonable Functions (PUFs).** The idea of using variability-induced delays for authentication and security has been proposed [2, 6]. PUFs are one-way functions that map a set of challenges to a set of responses, based on an intractably complex physical system. PUFs are unique, since process variations cause significant delay differences among ICs coming from the same mask. Authentication occurs when the IC correctly finds the output of one or more challenge inputs.

3 Class Organization

The target audience were beginning graduate students and advanced undergraduate students. The first week of the semester was used for a broad overview of all covered HW topics, issues, and concepts along with presentations of the basic ideas that may serve as the seeds for class projects. The students were asked to form small teams (at least two and at most three students). A single topic per week was discussed. In the first class, the background material, potential attacks, security mechanisms, protocols, and system and security evaluation were covered. In the second class, two papers on the topic where presented. Usually one was a very significant classical paper and the other was a paper on a recent notable progress or a new direction. The attempt was to have a self-contained class, but it was obvious that the students with a strong background in security and/or cryptography, and/or system design were benefiting significantly more. Typical projects were development of new watermarking and fingerprinting IP protection schemes, use of manufacturing variability for authentication, and security of sensor networks. Grading was emphasizing the project and class presentations, but we also had two midterm exams.

4 Evaluation and Future Directions

We believe that the course was very beneficial to majority of the students: almost all of the groups did remarkable projects, the presentations were well-prepared and delivered. The major problem was that the level of presentations were nonuniform and that a significant percentage of students completely dedicated themselves to their projects in the last three or so weeks at the expense of assignments and presentations. Our main future efforts include better integration with other design classes, further usage of the security and synthesis tools in the programming assignments, and identification of the essential system security principles and paradigms.

References

[1] Defense Science Board (DSB) study on High Performance Microchip Supply. http://www.acq.osd.mil/dsb/reports/2005-02-HPMS_Report_Final.pdf.

[2] B. Gassend et al. *Identification and authentication of integrated circuits*, pages 1077–1098. John Wiley & Sons, 2004.

[3] E. Schuster et al. *Global* RFID*: The Value of the* EPC*global Network for Supply Chain Management*. Springer, 2007.

[4] F. Koushanfar et al. Intellectual property metering. In *Information Hiding Workshop*, pages 81–95, 2001.

[5] F. Koushanfar et al. Behavioral synthesis techniques for intellectual property protection. *ACM Trans. Design Automation of Electronic Sys.*, 10(3):523–545, 2005.

[6] G.E. Suh et al. Design and implementation of the aegis single-chip secure processor using physical random functions. In *ISCA*, pages 25–36, 2005.

[7] S. Ravi et al. Security in embedded systems: Design challenges. *ACM Trans. on Embedded Computing Sys. (TECS)*, 3(3):461–491, 2004.

[8] G. Qu and M. Potkonjak. *Intellectual Property Protection in VLSI Design*. Kluwer, 2003.

0-7695-2849-X/07 $20.00 © 2007 IEEE