Review of the book

"Towards Hardware-Intrinsic Security: Foundations and Practice" by Ahmad-Reza Sadeghi and David Naccache (Eds.) Springer, 2010

ISBN: 978-3-642-14451-6

S. V. Nagaraj
RMK Engineering College

2012-08-11

1 Summary of the review

Nowadays, the security of hardware is as important as the security of software. This review concerns a book that offers the latest perspectives on hardware-intrinsic security. The book is composed of six parts that focus on topics such as Physically Unclonable Functions (PUFs); hardware-based cryptography; hardware attacks; hardware-based policy enforcement; hardware security in contactless tokens; and hardware-based security architectures and applications.

2 Summary of the book

The book has six parts.

Part I is on Physically Unclonable Functions (PUFs). This part has four chapters. A PUF is a function that produces a response that reckons on an intrinsic random physical feature of a device.

The first chapter (Physically Unclonable Functions: A Study on the State of the Art and Future Research Directions) attempts to cover the complete field of PUF constructions. It is a survey of the state of the art. It uncovers interesting open problems that provide directions for future research.

The second chapter (Hardware Intrinsic Security from Physically Unclonable Functions) looks at the new approach available today to prevent cloning of semiconductor products. PUFs can be employed to produce intrinsic fingerprints for devices. When used with unique activation codes, these fingerprints can produce the secret key which does not have to be stored in the hardware.This provides better security than is currently available.

The third chapter (From Statistics to Circuits: Foundations for Future Physically Unclonable Functions) looks at open challenges in the design and implementation of reliable and efficient PUFs. This requires circuit-level optimization; architecture-level optimization; and statistical analysis.

The fourth chapter (Strong PUFs: Models, Constructions, and Security Proofs) looks at the formal foundations and applications of strong PUFs.

Part II is on Hardware-Based Cryptography. This part has two chapters that discuss hardware-based cryptography. They both analyze leakage attacks on hardware cryptographic modules, revealing the fact that it is possible to elicit reasonable information from the device by yielding an abstraction that models a side channel (such as power consumption or electromagnetic radiation).

The first chapter (Leakage Resilient Cryptography in Practice) investigates the relation between theoretical models and practical engineering processes concerning side-channel attacks. The chapter studies leakage resilient pseudo-random number generators.

The second chapter (Memory Leakage-Resilient Encryption Based on Physically Unclonable Functions) proposes a leakage-resilient encryption scheme that utilizes PUFs.

Part III discusses Hardware Attacks. This part has two chapters. There is a chapter about Trojan horses in hardware. The idea behind hardware Trojans is similar to that of software Trojans. Some extra logic is added to a circuit to induce an undesirable behavior. The manufacturer of the circuit can thus gain access to guarded parts of the memory or make the system work in modes without proper authentication. The chapter demonstrates techniques for warding off this problem.

The first chapter (Hardware Trojan Horses) presents recent knowledge about techniques for detecting hardware Trojan horses as well as design methodologies for bettering Trojan detection methods.

The second chapter (Extracting Unknown Keys from Unknown Algorithms Encrypting Unknown Fixed Messages and Returning No Results) presents experiments that indicate the risk involved in distributing engineering samples of improperly protected tamper-resistant devices.

Part IV is on Hardware-Based Policy Enforcement. This part has two chapters that look at the problem of policy enforcement based on hardware. This part studies problems such as licensed content distribution, the use of hardware fingerprints to obviate copies, and other intellectual property infringements.

The first chapter (License Distribution Protocols from Optical Media Fingerprints) shows how to generate unique fingerprints for any CD. The technique may be used for any pressed and burned CD and extended in theory at the least to other optical storage devices.

The second chapter (Anti-Counterfeiting: Mixing the Physical and the Digital World) studies desiderata for anti-counterfeiting technologies, techniques for digitizing the physical world, applications, and a review of existing methodologies.

Part V is on Hardware Security in Contactless Tokens. This part has three chapters. A contactless token is a commonly used device for making payments and enforcing access control. Contactless tokens are likely to be used widely in the future. The security of such devices is vital, and substantial research is currently afoot in this area.

The first chapter (Anti-Counterfeiting, Untraceability and Other Security Challenges for RFID Systems: Public-Key-Based Protocols and Hardware) covers the security and privacy requirements for RFID systems.

The second chapter (Contactless Security Token Enhanced Security by Using New Hardware Features in Cryptographic-Based Security Mechanisms) imagines the integration of new hardware components into contactless smart cards. These include components such as a flexible display, a real-time clock, and a battery to power the clock in order to form a novel security token.

The third chapter (Enhancing RFID Security and Privacy by Physically Unclonable Functions) demonstrates that PUFs are a very interesting and promising approach for improving the security and privacy of existing RFID systems.

Part VI focuses on Hardware-Based Security Architectures and Applications. This part has five chapters focusing on architectures and applications. The chapters are a collection of techniques employed to real-life problems, such as trusted satellite navigation and reliable remote health care.

The first chapter (Authentication of Processor Hardware Leveraging Performance Limits in Detailed

Simulations and Emulations) presents a new challenge-response scheme for checking the authenticity of a processor based on the performance gap between authentic hardware and simulations or emulations.

The second chapter (Signal Authentication in Trusted Satellite Navigation Receivers) discusses measures that receivers could employ for assessing the authenticity of signals from global navigation satellite systems.

The third chapter (On the Limits of the Hypervisor- and Virtual Monitor-Based Isolation) presents an attack on compartmentalized systems by assuming that a bug or backdoor is present in RAM modules.

The fourth chapter (Efficient Secure Two-Party Computation with Untrusted Hardware Tokens) discusses the usability of a token-assisted protocol for efficient and secure two-party computation.

The fifth chapter (Towards Reliable Remote Healthcare Applications Using Combined Fuzzy Extraction) emphasizes the need for providing solutions that can guarantee that a measurement represents a patient and that it originates from a particular device. This chapter describes a solution that provides very strong safety guarantees using PUFs.

3 What is the book like (style)?

This book offers a useful perspective on hardware-intrinsic security. This is a relatively new field that deals with secure secret key storage. Permanent secret key storage is not required if secret keys are developed using the intrinsic properties of the silicon. In addition, the key exists in the device for a minimum amount of time. This book includes contributions by numerous experts from across the globe in that field. Despite the contributions by various authors, the book maintains homogeneity. Every chapter includes references for further study. This book is suitable for those interested in teaching or researching hardware-intrinsic security. The organizational structure of the book is to be praised.

The book does not have an index. This prevents easy cross-referencing. Some chapters of the book are heavy on obscure mathematical notation which is hard to follow. The book employs small fonts in some places and therefore readability becomes strenuous. However, the book offers a very good perspective on current research in the field of hardware-intrinsic security.

4 Would you recommend this book?

This book offers a worthwhile introduction to research issues related to hardware-intrinsic security. Students, researchers and practitioners will find this book interesting and beneficial. I recommend this book for those interested in various aspects of hardware security and hardware-intrinsic security.

The reviewer is a Professor at the CSE Dept., RMK Engg. College, Kavaraipettai, Tamil Nadu, India