Preface

Cybersecurity has emerged as a dark side of the digital age, and the scale of the world's cybersecurity problems has become daily news. With the convergence of computing and communications, coupled with exponential increase in data volume in Internet, it remains a rising and critical concern. Hardware plays an increasingly important and integral role in cybersecurity, with many emerging system and application vulnerabilities rooted in hardware, including the recently reported Meltdown and Spectre vulnerabilities in various microprocessors in the market. The emergence of new application space in the internet-of-things (IoT) regime is creating new attack surfaces, and new requirements on hardware to support secure and trusted system operations. Additionally, the design, manufacturing, and distribution of integrated circuits (ICs), printed circuit boards (PCBs), as well as other electronic hardware components (passive or active) are becoming more sophisticated and globally distributed, involving a number of untrusted entities. This horizontal—but very complex—supply chain introduces myriad security issues in hardware, including malicious changes, information leakage, side-channel attacks, counterfeiting, reverse engineering, and piracy activities. The shortened time-to-market for system on chips (SoCs), which serve as the backbone for many modern computing systems, further exacerbates the problem by leaving unintentional vulnerabilities in the design that could be exploited by attackers once the chips are in the field.

The topic of hardware security encompasses wide-ranging security and trust issues, which span the entire lifecycle of electronic hardware, and all its abstraction levels (chips, PCBs, systems, and system of systems). With increasing security vulnerabilities and trust issues, the role of hardware as a trust anchor of a computing system is being challenged. Hence, effective and comprehensive hardware security education is crucial at all levels, including undergraduate and graduate students, and professionals involved in design and deployment of computing systems, to safeguard these systems against diverse hardware security/trust issues. We note that there is an increasing demand of well-trained hardware security professionals in the job market. Existing curriculum at colleges and universities, to our knowledge, do not provide adequate insight into the full spectrum of hardware threats and respective protection approaches. They typically fail to provide: (a) a holistic hardware security education that covers security of all abstraction layers; and (b) a hands-on training approach that we believe is crucial in understanding the security vulnerabilities in a complex system, and the corresponding defense mechanisms. To address this important growing need, we embarked on the project of developing the first-ever textbook dedicated to hardware security and trust.

This book aims to provide holistic hardware security training and education to upper-level undergraduate engineering students. Although targeted primarily towards undergraduate students, it can serve as a useful reference for graduate students, security researchers, and practitioners, and also industry professionals, including design engineers, security engineers, system architects, and chief security officers. This book contains material on the background of modern computing systems, followed by description of security issues and protection mechanism. It also contains a set of well-designed experiments that can be performed in any adequately equipped circuit laboratory to learn different aspects of hardware security, which encompasses security vulnerabilities, attacks, and protection mechanisms. To help students understand the components of modern systems before taking a deeper dive into the specific subject area of security, background chapters cover the basics of computing hardware, circuit theory, active and passive electronic components, chip/PCB design, and test flow.

This book includes description of a unique companion material: a hardware platform, referred to as Hardware Hacking (HaHa) platform, that is easy to model a hardware-software system and ethically 'hack' it to learn diverse hardware security issues and countermeasures. All of the hands-on experiments presented in this book can be implemented on this platform, although alternative hardware modules, for example, the Field Programmable Gate Array (FPGA) development boards, can also be used to perform some of the experiments. The comprehensive coverage of hardware security concepts with relevant background material, and a practical learning approach, are the key distinctive features of this text book, which we believe are essential to prepare students for today's challenging hardware security problems.

Unique features of this text book

- It provides a thorough overview of computer hardware, including the fundamentals of computing systems and implications of security risks therein, studies of known attack methodologies, countermeasures, and case studies. Given this foundation, readers are expected to obtain a thorough understanding of key concepts, which facilitate recognizing and countering hardware security threats in actual products and system designs.
- Each major topic in hardware security (security vulnerabilities, attacks, and appropriate protection mechanisms) is explained in detail, combined with a well-designed hands-on experiment on the topic.
- The book includes the description of a custom electronic hardware platform, called HaHa, which is developed by the book's authors to perform the aforementioned laboratory exercises. This hardware module is specifically designed to illustrate various key concepts using a single platform. The experiment descriptions are provided as companion material, which includes step-by-step descriptions of the experimentation process, observations, reporting format, and advanced options.
- Each chapter is also accompanied by a set of exercises divided into three groups with varying difficulty levels. They are meant to provide readers with questions that help them effectively understand the concepts presented in the chapter.

Organization of the book

The authors have organized the topics based on a decade of experience in teaching hardware security to effectively convey the related concepts. Chapter 1 provides an introduction to the topic of hardware security. It presents preliminary and basic concepts on major topics, for example, hardware attack vectors, attack surfaces, adversary model, causes of hardware attacks and effect on business/economic models, hardware supply chain, and relation between security and trust. This chapter also provides a brief history of hardware security, an overview of the scope of the book, and the lab-based approach.

The remainder of the book is organized in four parts:

1. Part 1: Background on Electronic Hardware
2. Part 2: Hardware Attacks: Analysis, Examples, and Threat Models
3. Part 3: Countermeasures Against Hardware Attacks
4. Part 4: Emerging Trends in Hardware Attacks and Protections

Part 1: Background on Electronic Hardware: Part 1 includes three chapters. Chapter 2 provides a background on digital logic, circuit theory, embedded systems, ICs, application specific integrated circuits (ASICs), FPGAs, PCBs, firmware, hardware-firmware-software interaction, and the role of hardware in system security. Chapter 3 gives an overview of SoC design and test. It describes intellectual property (IP)-based SoC lifecycle, the SoC design process, the verification/test steps, and design-for-test, and design-for-debug infrastructures. The final chapter in this part, Chapter 4, provides an introduction to design and test for PCBs. In particular, this chapter describes PCB lifecycle, PCB design process, and PCB testing methods.

Part 2: Hardware Attacks: Analysis, Examples, and Threat Models: This part of the book covers attacks and vulnerabilities in hardware throughout its lifecycle, and in today's supply chain. Chapter 5 focuses on hardware Trojan attacks in ICs and hardware IPs. It presents different types of Trojans: triggers and payloads, and different threat vectors in the design and fabrication process. Chapter 6 provides a detailed insight into today's electronics supply chain security and integrity issues. Chapter 7 presents security issues in the hardware IP lifecycle, with emphasis on challenges related to hardware IP piracy and IP reverse engineering. This chapter also presents issues related to FPGA IP security issues, as FPGA market and IP supply chain continues to grow. Chapter 8 presents the topic of side-channel attacks (SCA). It covers all forms of side-channel attacks, namely, power side-channel attacks, timing attacks, electromagnetic (EM) side-channel attacks, and fault-injection attacks. Chapter 9 introduces test infrastructure-oriented attacks with focus on scan and JTAG. Different forms of information leakage attacks using on-chip test/debug infrastructure are covered in this chapter. Chapter 10 focuses on physical attacks and microprobing. Chip-level reverse engineering and microprobing attacks at chip level for information leakage, and tampering are also discussed in detail in this chapter. Finally, Chapter 11 presents various attacks on PCB, with emphasis on physical attacks. The physical attacks include snooping of PCB traces for information leakage, PCB reverse-engineering and cloning, and malicious field modification or modchip-type attacks.

Part 3: Countermeasures Against Hardware Attacks: This part of the book focuses on countermeasures against hardware attacks. In particular, countermeasures fundamental to hardware security assurance and building the hardware root of trust are presented. Chapter 12 focuses on design and evaluation of hardware security primitives and their roles in functional security and protection against supply chain issues. It covers common primitives, such as, physical unclonable functions (PUFs) and true random number generators (TRNGs). Chapter 13 presents design-for-security (DFS) and security/trust validation for integrated circuits, security built into a design at different levels, and targeted to prevent different hardware attacks. Chapter 14 discusses hardware obfuscation. It presents a number of obfuscation techniques, including state-space obfuscation, logic locking and camouflaging, and discusses their role in protecting against IP piracy, reverse engineering, and malicious modification. Chapter 15 describes PCB integrity validation and authentication. It presents PCB-level authentication solutions using intrinsic signature of PCBs, and protection of PCB against field attacks.

Part 4: Emerging Trends in Hardware Attacks and Protections: The final chapter in this book (Chapter 16) describes system-level attacks and countermeasures, possibilities of exploiting hardware security vulnerabilities by system/application software, and SoC security architecture for secure systems. Assets in a SoC are major targets of software attacks. Hence, developing secure SoC architecture for protecting these assets is essential. This chapter describes architecture-level solutions for protecting on-chip assets from diverse attacks that rely on access-control or information flow violations, or other vulnerabilities.

We hope that the target readership enjoys the content of this book and greatly benefits from it. We believe that the content of this book will remain highly relevant for many years to come, as the topic of hardware security, as it relates to the broader field of cybersecurity, is consistently growing in scope and relevance.

Companion material

This book has a companion material (available at https://hwsecuritybook.org/) that provides detailed description of the hands-on experiments that use the custom HaHa platform. This modular, flexible, and simple hardware platform is expected to be very effective for hardware security education and training. It is designed to enable students to build a computing system of selected capability by adding various components (for example, sensors or communication units) in a LEGO-like fashion, and connect multiple units wirelessly to create a networked system. It then allows students to implement diverse security attacks ranging from hardware Trojans, side-channel attacks, tampering, reverse engineering, and snooping. We hope the hands-on experiments will serve as an invaluable resource for the students, helping them to thoroughly understand key concepts and stimulating their interest to explore new vulnerabilities, or protection mechanisms.

Book website

Supporting materials and the lab modules for this book are available at the book's own website: www.hwsecuritybook.org. The website will include the following: slides for each chapter, sample homework assignments, sample exams and tests, lab modules for HaHa board, sample projects, videos of a selected number of lab modules, simulation tools, Verilog/VHDL designs, and more. This website will be a hub for any educational materials available to help further students and instructors' understanding of the concepts in hardware and systems security. We will also work with instructors, who teach this course to facilitate widespread sharing of the materials among members of the hardware security community.

For instructors

The "www.hwsecuritybook.org" webpage includes additional materials for instructors only. This part of the site is password protected. If you plan to use it, please contact the webmaster, allow a week to obtain a login username and password via the procedure published on the web. The instructor area will contain original slides, notes supporting each slide, complete set of exams, homework assignments, quizzes, and more. The website also includes answer to selected exercises and exams.

Swarup Bhunia and Mark Tehranipoor