Preface

This book is based on the author's 18 years of teaching and research experience. It covers the fundamental principles in computer and Internet security, including software security, hardware security, network security, web security, and cryptography. Its goal is to help readers understand how various attacks work, what their fundamental causes are, how to defend against them, and how various defense mechanisms work. Equipped with the knowledge from this book, readers will be able to evaluate the risks faced by computer and network systems, detect common vulnerabilities in software, use proper methods to protect their systems and networks, design and implement software systems and applications that are secure against attacks, and more importantly, apply the learned security principles to solve real-world problems. The book can be used as a textbook for undergraduate and graduate courses.

The author strongly believes in "learning by doing", so the book takes a hands-on approach. For each security principle, the book uses a series of hands-on activities to help explain the principle; readers can *"touch"*, *play with*, and *experiment with* the principle, instead of just reading about it. For instance, if a security principle involves an attack, the book guides readers to actually launch the attack (in a contained environment). In some cases, if a principle involves a security mechanism, such as firewall or Virtual Private Network (VPN), the book guides readers to implement a mini-version of such a mechanism (e.g., mini-firewall or mini-VPN). Readers can learn better from such hands-on activities.

All the hands-on activities are conducted in a virtual machine image provided by the author. They can be downloaded from this URL: `https://seedsecuritylabs.org`. Everything needed for the activities have already been set up; readers just need to download the VM (free), launch it using `VirtualBox`, and they can immediately work on the activities covered in the book. This book is based on the `Ubuntu16.04` VM image. The author will regularly upgrade the VM image in every few years.

Most of the activities in the book are based on the author's SEED labs, which are widely used by instructors all over the world. These labs are the results of 17 years' research, development, and testing efforts conducted by the author and his students in a project called SEED, which has been funded by the National Science Foundation since 2002.

The author believes in depth. For any topic covered in his lectures, the author wants to cover it thoroughly, as deep as needed. He is not interested in teaching students only the concepts; he likes to help students gain a deep understanding. The same philosophy is reflected in this book. For example, one can teach students how DNS attacks work in 30 minutes, but this book spends 50 pages on DNS, covering the great details of the DNS protocol and a variety of attacks on DNS. Many of these details took the author himself months of effort to figure out. Another example is the buffer overflow attack, which can be taught in 15 minutes, but this book uses two chapters (67 pages) to talk about it, covering all the required background knowledge, the details of the attack, the challenges of the attack, countermeasures, how to defeat some countermeasures, and some advanced attack techniques.

The author believes in fundamentals. Security is a very broad topic; every time when a new technology XYZ comes up, there will likely be a new security topic called “XYZ security”. While teaching these new security topics seems to be more fashionable, the author strongly believes in teaching fundamentals. Underlying these XYZ-security topics lies the similar security fundamentals. Readers who have mastered the fundamentals can quickly adapt their knowledge to work on new security topics, but those who just learned XYZ-security will have a hard time to work on ABC-security.

To help readers master fundamentals, the book often brings together several seemly-different things (attacks or defense mechanisms), trying to help readers see their fundamental similarities and differences. Moreover, when analyzing security problems of a particular mechanism, the book takes a systematic approach based on security principles, grounding reasoning on solid fundamentals.

New to This Edition

Since the first edition of this book was published, the author wrote seven new chapters; he also added a significant amount of new contents to several existing chapters. Moreover, he has updated the operating system version in his SEED virtual machine; that results in small changes in many places. The followings summarize the significant changes made in this edition.

- **Meltdown and Spectre attacks:** Two chapters on hardware security are added. They cover the recently discovered attacks on CPUs, including the Meltdown attack (Chapter 13) and the Spectre attack (Chapter 14).

- **Bitcoin and blockchain:** One chapter on Bitcoin and blockchain is added (Chapter 26). Bitcoin is a form of cryptocurrency, and it involves several important cryptography concepts, including public key cryptography, elliptic curve cryptography, digital signature, one-way hash function, Merkle tree, and hash chain. Through Bitcoin, readers can learn how these crypto concepts are used to solve real-world problems. Bitcoin is an application of blockchain, so the chapter also covers the blockchain technology.

- **Cryptography:** Three chapters on cryptography are added: Secret-Key Encryption (Chapter 21), One-way Hash Function (Chapter 22), and Public-Key Cryptography (Chapter 23). These are three building blocks on cryptography. Combined with the two existing crypto chapters from the first edition (PKI and TLS) and the Bitcoin (cryptocurrency) chapter, the book now provides a good coverage on the basics of cryptography, which are sufficient for the crypto part of most security courses.

- **Reverse shell:** One chapter on reverse shell is added. The reverse shell technique is a widely used attack technique, and it is used in several chapters of this book. Many students have a hard time understanding how it works, so the author decides to use a separate chapter for the reverse shell technique.

- **New VM (16.04):** The first edition uses the Ubuntu 12.04 VM as its experiment environment. After it was published, all the SEED labs were ported to the Ubuntu 16.04 VM. This new edition is now based on Ubuntu 16.04, so it is consistent with the SEED labs. All the code in this edition has been tested on the provided Ubuntu 16.04 VM.

- Buffer-Overflow (Chapter 4): Added attack strategies in more realistic scenarios.

- Return-to-libc (Chapter 5): Added extensive coverage on Return-Oriented Programming.

- Format String Attack (Chapter 6): Based on the author's own experience, this attack is quite hard for students to understand, so the code injection part is rewritten to make it easier to understand.

- Cross-Site Scripting (Chapter 11): Added coverage on Content Security Policy (CSP), and how to use it to defend against XSS attacks.

- DNS (Chapter 18): Two parts are added: (1) coverage on the technical details of the DNS rebinding attack; (2) detailed experiments on the reply forgery section to show how local DNS servers decide what information in a reply can be cached and what should be discarded.

- Sniffing and Spoofing (Chapter 15): added Scapy code. Writing sniffing and spoofing programs using Python's Scapy library is much easier than using C, and the program is much shorter. For each task in this chapter, a Python version is added. However, the C programs are still kept, because they show us how exactly sniffing and spoofing actually works inside the system. Moreover, there are situations where the performance is critical, and Python's speed cannot satisfy the requirements, so we still need to use C programs or tools that are developed using C or C++.

- Using Scapy code to replace tools. In the first edition, we heavily used tools, such as `Netwox`, for many network attack tasks. We would like students to write such tools. Python's Scapy library provides almost all the functionalities that can be achieved by `Netwox`. In this new edition, the author has replaced the use of `Netwox` with Python Scapy code. He has been using Scapy in his classes for almost a year, and students really prefer Scapy over the existing tools. Teaching students to build their own tools is much better than teaching them to use existing tools. Several chapters now include Scapy code, including Sniffing and Spoofing (Chapter 15), TCP attacks (Chapter 16), and DNS (Chapter 18).

- Adopting Python as the official script language. In some experiments, we need to write code or script for some small tasks, such as constructing attack payload. In the first edition, a variety of programming languages are used, including C code and shell scripts. Starting from this edition, the author has adopted Python as the official script language for these small tasks. Code in several chapters has been rewritten using Python. However, for tasks that focus on coding, the book still uses C.

Split into Two Volumes

After the first edition of this book was published, seven new chapters were written, focusing mostly on cryptography and hardware security. The additions increase the number of pages from 430 to nearly 700. This trend will very likely continue for the next few editions, as there are a few more topics that the author wants to add to the book. Given the depth covered in each chapter, it is hard to imagine that a typical class would cover all the chapters from this book (the author himself uses the content from this book for two different 3-credit security courses, each covering one half of the book).

To make the book more affordable to students, starting from this edition, the author will simultaneously publish three different versions of this book, including two volumes that cover part of the book and one that covers all.

- *Computer & Internet Security: A Hands-on Approach* (ISBN: 978-1-7330039-2-6, hardcover): This book covers all the 26 chapters in the second edition.
- *Computer Security: A Hands-on Approach* (ISBN: 978-1-7330039-0-2): This volume covers the part of the book related to Computer Security (18 chapters in total). It includes the topics on software security, hardware security, web security, and cryptography.
- *Internet Security: A Hands-on Approach* (ISBN: 978-1-7330039-1-9): This volume covers the part of the book related to Internet Security (16 chapters in total). It includes the topics on network security, cryptography, and web security.
- **Notes:** To satisfy the diversified teaching needs from instructors, the author intentionally includes some common chapters in both volumes, including all the three chapters on web security and the first four chapters on cryptography (TLS and Bitcoin, two advanced topics on cryptography, are included only in the *Internet Security* volume).

The History of the SEED labs

"I hear and I forget. I see and I remember. I do and I understand". This famous saying, by Chinese philosophy Confucius (551 BC – 479 BC), has been a motto for many educators, who firmly believe that learning must be grounded in experience. This is particularly true for computer security education. Seventeen years ago, with this motto taken to the heart, and a desire to become an excellent instructor in computer security, the author searched the Web, looking for hands-on projects that he could use for his security classes. He could only find a few, but they came from various places, and were incoherent; their coverage of security topics was quit narrow, even jointly, and the lab environments they used were not easy nor inexpensive to set up.

Determined, he decided to develop his own hands-on exercises (called labs in short), not one lab, but many of them, covering a wide spectrum of security topics; not just for his own use, but for many other instructors who share the same teaching philosophy as he does. All the labs should be based on one unified environment, so students do not need to spend too much time learning a new environment for different labs. Moreover, the lab environment should be easy and inexpensive to set up, so instructors are not hindered even if they have limited time or resources.

With the above goals in mind and an initial grant from NSF ($74,984.00, Award No. 0231122), he started the journey in 2002, naming the project as SEED (standing for SEcurity EDucation). Ten years later, after another NSF grant ($451,682, Award No. 0618680) and the help from over 20 students, he has developed about 30 SEED labs, covering many security topics, including vulnerabilities, attacks, software security, system security, network security, web security, access control, cryptography, mobile security, etc. Most SEED labs have gone through multiple development-trial cycles—development, trial, improvement, and trial again—in actual courses at Syracuse University and many other institutes.

The SEED project has been quite successful. As of now, more than 1000 instructors worldwide told the author that they have used some of the SEED labs; more people simply used the SEED labs without telling (which is perfectly fine), as all the SEED lab materials and the lab environment are available online, free of charge. To help others use the SEED labs, NSF gave the author another grant ($863,385.00, Award No. 1303306), so he can organize two training workshops each year and fund those who come to attend the workshops. Every year, about 70 instructors attended the workshops. In summer 2019, a record number of 110 instructors will come to attend the workshops.