Review of the book

"COMPUTER SYSTEM SECURITY BASIC CONCEPTS AND SOLVED EXERCISES"

by Gildas Avoine, Pascal Junod and Philippe Oechslin
EPFL Press
2007

ISBN: 978-1-4200-4620-5

Eric Diehl
Security Competence Center, Technicolor

2010-02-09

1. What the book is about

This book is a collection of eight chapters and 106 solved exercises. Each chapter proposes an introduction to a generic problem encountered in computer security systems. After the introduction, the authors propose a set of exercises. Of course, the authors also reveal the succinct corresponding solutions. In a simplified summary, each chapter proposes a lesson, the examination and the corrected results.

The "lessons" are very basic. I would even state too basic. If you are already knowledgeable about the topic, then you will probably learn nothing. If you are not knowledgeable, then you will just get a glimpse of the main issues. Fortunately, the bibliographic references often allow exploring more in details the topic.

The three authors taught at EPFL in the early 2000's. Clearly, the exercises proposed in the book are some of the ones they submitted to their students. There are three types of exercise:

- Control of the acquisition of theoretical knowledge of definitions and concepts; for instance "*Which problems is a user, hidden behind a firewall using dynamic NAT, likely to face when he connects to an external FTP server from his internal network?"*

- Basic exercise to find a "simple" solution; for instance "*if Steve Pirate has a bandwidth of 256Kbps and is able to use 100% of it for his attack, how much of the bandwidth belonging to* `poor.victim.com` *will be used by the attack?"*

- Elaborated complex exercise, most probably part of the final exam; for instance "*Kevin Mitnick's attack"*

The interesting question is: would you be able to solve the exercises by just having read and understood the "lesson"? For the first type of exercise, the answer is yes. For the second type, the answer is maybe. For the more elaborated exercises, the answer is clearly no. The solutions require a deeper knowledge of the security issues and also some other background knowledge (for instance network technology…). In other words, be ready to search for more information outside of the book. Exercise 31 is a clear illustration of that point. This exercise requires explaining the difference between Cross Site Scripting (XSS) and SQL injection. Unfortunately, XSS was not addressed in the book.

The book is a revised translated version of a French initial book published in 2005. Thus, the book neglects (or does not give enough emphasis to) the newest threats such as web services exploits. For instance, there is no emphasis on XSS or Cross Site Reference Forgeries (XSRF). It does not present the latest "hot" trends such as the use of cloud for anti viruses or intrusion detection. A revised version should add several new chapters taking into account the Web 2.0 environment, more detailed application vulnerabilities amongst others.

Sadly, readers who do not understand French will lose the touches of humor of the names used in the exercises. Thus, readers may encounter Salem Enthal, Mehdi Khamenteux, and Sosie Sonsek.

2. What the book is like

Chapter 1: "*Forging E-Mail and Spam"* This section demonstrates that you cannot trust the sender of a mail and explains how it is used to craft spams. Normally after having read this chapter and practiced the exercises, you should be able to analyze the headers of a mail (that modern mailing software hides from us). I would probably not have started with this section, but it has the advantage to be rather simple to understand. Thus it is a good warm-up chapter.

Chapter 2: *"Malwares"* This section presents a rather complete tour of the current taxonomy of malwares. Unfortunately, this taxonomy is not reused later in the section. The most advanced malwares such as rootkits or polymorphic viruses are not described as they would deserve. Hoax is explained on two pages whereas rootkit gets 12 lines! The section explaining the protections against malware is too weak. The exercises are not very interesting. For instance exercise 19 asks what a network administrator has to do to cope with a worm that uses TCP and UDP in the LAN. Exercise 14 needs some revamping. It still uses Windows 95/98 and bootable floppy discs (only old timers like me will remember what a floppy disc is!)

Chapter 3: *"Network and Application Vulnerabilities"* starts with an introduction to TCP/IP. Unfortunately, you will need more than this introduction to solve the exercises. Then, it explores Denial Of Services attacks (DoS), IP spoofing, session hijacking and exploits. DoS are well explained and can be understood by genuine readers. Then, it describes buffer overflow attacks. Once more, the reader needs a good background in computer science to understand the behavior of the stack and some notion of assembly. Some exercises are interesting. Exercise 21 and its solution detail the famous Kevin Mitnick's attack. Exercise 25 is a nice piece. The exercises on the application vulnerabilities are not extremely interesting.

Chapter 4: *"Firewall and Proxies"* is a good general introduction to the topics. It is one of the best chapters of this book. The firewalls are well explained with good description of the basic templates of security network architecture using demilitarized zones. The description of the role of Network Address Translation (NAT) and its consequences in terms of security is clear. Proxies are well described. The exercises of this section require a rather good knowledge of network protocols. After these exercises, you should normally be able to fine tune the filtering of your personal firewall at home.

Chapter 5: *"Cryptography"* this section is deceiving, especially when you know the background of the authors. The introduction could have been more educational. I am not sure that the genuine reader will understand how RSA works. The part on cryptanalysis mainly describes the easy to understand attacks such as brute force, or birthday paradox. It does not introduce more elaborated attacks or is too fast to be useful (3 lines on side channel attacks). The combination of symmetric and asymmetric cryptosystems will be tackled in chapter 7 with the presentation of PGP.

Chapter 6: *"Secure Communications"* first introduces the Virtual Private Network (VPN) concept. When describing VPN, the focus is mainly on the format of the messages and the encapsulated IP packets. The explanation of Internet Key Exchange (IKE) uses (of course) Diffie-Hellman, unfortunately it has not been introduced in the previous section. The description of TLS does not go into the details. The description of SSH is even more limited. It is only with exercise 71 that the man-in-the-middle attack is introduced. The exercises are mainly of the first type.

Chapter 7: "*Security at the User Level"* focuses on user authentication with first a long dissertation on alphanumeric passwords. The description of Kerberos is excellent. The description of PGP is merely an excuse to introduce the key management schemes using asymmetric cryptography to define symmetric session keys. It also provides the usual presentation about the minimal size of keys (which would have been better in chapter 5 according to me). The section should have at least introduced alternative tools such as Radius. Exercise 86 about physical access is a nice piece of work. It was interesting to show that physical security is important in an organization.

Chapter 8: *"Management of Information Security"* cites the major standards such as ISO27001, ISO 17799 or the Common Criteria. It never goes in any details. I am not sure that the reader may have an idea on how costly, fastidious and rigorous those evaluations are. The exercises are at the same level as the section is, i.e. simplistic.

3. Recommendation

This book is difficult to classify. Clearly it is not a lecture book. Although the introduction part of each chapter provides some basic concepts, they are rarely detailed enough to be useful for the reader to become somewhat knowledgeable. The reader, as mentioned in the book's foreground, should have a fair background in computer science and be familiarized with the main network protocols. The reader will have to look for more information elsewhere if he/she wants to succeed the exercises. The exercises offer a rather large overview of the potential questions in an exam. The authors are/were teaching. Therefore, the solutions are clear and can be used to benchmark your knowledge and find where improvement of one's knowledge is still needed.

The book, initially written in 2005, starts to become old. The field of security evolves fast with new technologies, new threats and new attacks. A new edition should add new chapters with new topics and revamp some exercises.

Should you read this book? If you are a student in security computer science, then this book is for you. It is a kind of book of past exams. Would you succeed to solve all the exercises, then you are pretty ready to get graduated. If you are not a student, you may read it for fun or to refresh aging knowledge. If you are looking for an introduction to computer system security, try another book or even better several dedicated books.

The reviewer is the head of Technicolor's security competence center, Rennes, France