Review of the book

"Elements of Computer Security"

by David Salomon

Springer, 2010

ISBN: 978-0-85729-005-2

Yeşem Kurt Peker
Randolph College

15 June 2011

1 Summary of the review

The book is an excellent resource on the essential topic of computer and network security and privacy in online communications for anyone who uses computers and the Internet for computation, communication, or leisurely purposes. It provides a very good understanding of the vulnerabilities of computer hardware and software and how some attacks/threats exploit these vulnerabilities to infect computers, violate one's privacy, or interrupt communications as well as tools to counter the attacks and threats.

2 Summary of the book

In the Introduction the author prepares the framework and provides motivation for the subsequent chapters. He also provides a list of resources ("good" websites and books) which he believes offer reliable information and user education. He classifies computer security and problems into three large classes: Physical Security, Rogue Software, and Network Security.

Chapter 1 discusses topics that have to do with the physical security including side-channel attacks; physical threats such as power issues, security of facilities, backups; laptop security; recovery planning and privacy protection.

Chapters 2-4 are devoted to explaining the principles behind rogue software or malware. Chapter 2 discusses viruses in depth. It explains different types of viruses according to their infection mechanisms, the harm they can inflict on a computer, and the platform or the operating system they can infect. Various examples of viruses are provided with details of how they work. Chapter 3 discusses worms in detail. It examines the mechanisms used by known worms and considers ways to write more efficient worms. As for viruses, the author provides details on various known worms such as Code Red, the Internet worm, and iPhone worms. Chapter 4 discusses Trojan Horses in detail along with examples. It goes into details of how a Trojan is installed and how to rig a compiler to leave no trace when a Trojan is installed.

The history and main features of several computer viruses and worms are described in Chapter 5. The examples chosen are significant in terms of their overall impact and their mechanisms of infection. The author does a good job tying them with his explanations in Chapters 2 and 3. Chapter 6 is on the important topic of preventing rogue software and defending against it. It starts by explaining the vulnerabilities and continues on to discuss methods for prevention and defense such as anti-virus software, backups, file permissions, and more.
Chapters 7 through 10 are on network security. Chapter 7 starts with what network vulnerability means and definitions of a threat, a passive attack and an active attack. The subsequent sections discuss various threats and attacks that actually occurred on the Internet such as port scanning, spoofs, spams, denial of service attacks, and others. These sections also include discussions of ways to avoid the threats and attacks. There is also a section that discusses the basics of firewalls.
Chapter 8 concentrates on authentication. It discusses local and remote authentication techniques including signatures, biometric techniques, and passwords. Special emphasis is given to choosing passwords and keeping them secure.
Chapter 9 discusses spyware; what they are, how they operate, their implications in social aspects of life and how hard it is to deal with them. It talks about what kind of data spyware can collect and how they can remotely report to interested parties. The author also includes sections on adware and researchware where he clarifies what is meant by these words and provides examples.
Chapter 10 discusses identity theft and ways to reduce the risk of identity theft to a minimum. It explains how the attackers use Internet cookies and phishing to lure people into providing personal information and warns against homograph threats which is, in very crude terms, using legitimate looking names for fake websites.
Finally, chapter 11 addresses general privacy concerns. It touches on topics such as online privacy, children's safety, digital forensics, and trust.
The book also includes three interesting appendices. Appendix A discusses the word "hacker", its definition and use throughout the years; Appendix B introduces "l33t", a notational system widely used by hackers. And finally Appendix C traces the history of viruses and other rogue software stressing "firsts" from 1940s to early 2010s.
The author also maintains a website located at `http://www.davidsalomon.name/UTICScompSec/UTICSCompSec.html` where he provides an errata list and auxiliary material including , answers to exercises in the book, some references and a document that discusses the principles and concepts behind some encryption algorithms used by modern cryptography. This document may not be accessible to all readers of the book as the principles require some mathematical background.

3 What is the book like (style)?

The book is well-written with clear explanations of the principles behind security threats and attacks, and measures to counter them. Each section includes clear definitions for the terms used in that section and draws attention to different uses of the word when appropriate which makes it easy to follow the

subsequent discussions. These terms are ones that are commonly encountered such as malware, virus, worm, spyware, adware, phishing, snoofing, and many others.
The book does not assume any mathematical or advanced computer science background. Although some familiarity with the inner workings of computers and programming would benefit the reader in chapters 2 through 5 and part of chapter 7, for the most part, the book is very informative and accessible to almost all computer and Internet users. It includes various examples for each kind of security concern along with a discussion of their historic significance.
It does not provide the reader with recipes on how to secure one's computer or communication but leaves them with a very good understanding of how the threats and attacks work and tools available for preventing and defending against them.

4 Would you recommend this book?

I would recommend the book to any computer user who wants to become more informed about the various threats and attacks out there to their privacy and the functionality of their computers. Even though chapters 2 to 5 and part of chapter 7 require some familiarity with the inner workings of a computer and programming, the rest of the book is accessible to anyone who uses computers and the Internet daily for communication and other purposes. The book could also be used for an introductory or informatory course on computer security.

The reviewer is a professor of mathematics at Randolph College, Lynchburg, VA.