Review of the book

"Computer Network Security"

by Jie Wang

Springer, 2009

ISBN: 978-3-540-79697-8

Mario Strefler
ENS, France

2010-07-15

Abstract

The book gives an extensive overview of network security and the necessary cryptography. It covers standards and protocols in great detail, and can serve as a handy reference for people interested in this area. Due to the many exercises, it can also serve as one of the textbooks of an introductory course on network security.

1 What the book is about

The book is intended as a textbook for a one-semester introductory course on network security, but also as a reference for IT professionals. It is divided into nine chapters, each containing also a set of exercises.

The first chapter gives an overview of network security topics. After a few definitions, it presents common attacks and defense mechanisms. It gives a colorful mix of what the author considers to be the most common attacks, chosen from the whole spectrum of cryptography and computer and network security. Then the author introduces attacker types such as "script kiddies" and "cyber spies", and rounds the chapter off with a basic security model that combines cryptosystems, firewalls, anti-virus programs, and intrusion detection systems into one picture.

The second chapter is called "data encryption algorithms", and deals with symmetric ciphers. The author gives an extensive and detailed description of the DES and AES algorithms. The treatment of block cipher modes of operation, the RC4 stream cipher, and key generation is comparatively short. At the end of the chapter, he also presents some simple attacks.

The third chapter is titled "public-key cryptography and key management", and describes mainly public-key encryption schemes and key exchange protocols. It starts with an overview of basic concepts, contains an introduction to some techniques in number theory that are fundamental for public-key crypto. The rest of the chapter describes RSA, and the ElGamal cryptosystem and Diffie-Hellman key exchange both in multiplicative groups and over elliptic curves. The chapter is rounded off with a short description of a certificate infrastructure.

The fourth chapter is about data authentication. It covers the cryptographic hash functions SHA-512 and Whirlpool, checksums, the HMAC authentication, the offset codebook mode of operation for block ciphers, and the digital signature standard DSS. It closes with some more advanced material describing dual signatures and blind signatures.

The fifth chapter gives a detailed description of network security protocols at the IP, TCP, and application layer. The author describes the X.509 standard for public key infrastructure, IPsec, SSL, PGP and S/MIME, the Kerberos authentication protocol, and SSH.

The sixth chapter is dedicated to WLAN security. After a short introduction to the 802.11 protocol family, the author describes the WEP, WPA, and WPA2 protocol standards in great detail, and mentions security flaws and attacks. He also covers the algorithms used in Bluetooth security. The chapter finishes with security aspects of wireless mesh networks.

The seventh chapter is titled "network perimeter security", and describes circuit and application gateways, packet filters, stateful and stateless filtering, and firewall configuration and policies. It describes several network security topologies such as single- and dual-homed bastion hosts, screened subnets, and demilitarized zones (DMZ), network address translation (NAT). and security for small office and home office (SOHO) networks.

The eighth chapter is about anti-malware programs. The author describes several forms of computer viruses, worms, trojan horses, and countermeasures, including a list of dangerous email attachment file types, and a list of anti-virus software. He also goes into peer-to-peer security, web security including ActiveX, Cookies, and AJAX, and DDoS attacks.

The ninth chapter is on intrusion detection. It starts with an introduction into basic concepts, Auditing and IDS architecture and policies, and covers host- and network-based detection, signature detection, statical analysis, honeypots, and forensics.

The appendix lists the 7-bit ASCII code table, SHA-512 constants, and explains the ZIP compression and Base64 encoding. There is even an experiment to crack WEP using a WEP cracker.

2 Summary

The book is a very exhaustive resource covering network security and the necessary cryptography. The author even goes beyond basic material by introducing dual signatures and blind signatures. Invariably, there are also aspects that the book does not cover, such as DNS security or IPv6 security.

3 What the book is like

The book aims to be a complete and self-sufficient introductory textbook into both cryptography and network security. To accomplish its goal, it gives very detailed descriptions standards in all areas it covers. This makes it a good reference book, but somewhat tiresome to read. The author tries to cover all relevant fields, but this has as a side effect that many topics are covered not very deeply, and that the book relies heavily on lists. Although it is intended as an academic textbook, it contains many useful references to real-world organizations and applications. There are many exercises to each chapter, including both theoretical and practical ones, where again some are intended to familiarize the reader with commonly used applications.

4 Would you recommend this book?

I think the book can serve as a reference book for people interested in network security, thanks to the many and detailed protocol descriptions. As a cryptographer, I cannot recommend the first part of the book to students. The first chapters that cover cryptography suffer from several flaws, including confusing use of terminology (the author never distinguishes between signing and encrypting/decrypting) and inaccurate and nonstandard definitions (e. g. "backward intractability" for encryption). Textbooks written by cryptographers exist, and are better suited as introductions to cryptography. The second part

of the book, the last five chapters that cover network security, leave a much better impression, although I cannot compare them to other textbooks due to my lack of knowledge in the field.
The reviewer is a Ph.D. student of cryptography at the Ecole Normale Supérieure, Paris, France.