Jie Wang

Computer Network Security

Theory and Practice

高等教育出版社
HIGHER EDUCATION PRESS

AUTHOR:

Prof. Jie Wang
Department of Computer Science
University of Massachusetts
Lowell, MA 01854, USA
E-mail: wang.uml@gmail.com

图书在版编目（CIP）数据

计算机网络安全的理论与实践＝Computer Network Security Theory and Practice：英文／（美）王杰编著.—北京：高等教育出版社，2008.9
ISBN 978-7-04-024162-4

Ⅰ.计… Ⅱ.王… Ⅲ.计算机网络－安全技术－英文
Ⅳ.TP393.08

中国版本图书馆CIP数据核字（2008）第144941号

策划编辑	刘　英	**责任编辑**	刘　英	**封面设计**	张　楠
责任绘图	尹　莉	**责任校对**	张　颖	**责任印制**	陈伟光

出版发行	高等教育出版社	**购书热线**	010-58581118
社　　址	北京市西城区德外大街4号	**免费咨询**	800-810-0598
邮政编码	100120	**网　　址**	http://www.hep.edu.cn
总　　机	010-58581000		http://www.hep.com.cn
		网上订购	http://www.landraco.com
经　　销	蓝色畅想图书发行有限公司		http://www.landraco.com.cn
印　　刷	涿州市星河印刷有限公司	**畅想教育**	http://www.widedu.com
开　　本	787×1092　1/16	**版　　次**	2008年9月第1版
印　　张	25.25	**印　　次**	2008年9月第1次印刷
字　　数	430 000	**定　　价**	48.00元

本书如有缺页、倒页、脱页等质量问题，请到所购图书销售部门联系调换。

物料号 24162-00

Sales only inside the mainland of China
仅限中国大陆地区销售

Preface

People today are increasingly relying on public computer networks to conduct business and take care of household needs. However, public networks may be insecure because data stored in networked computers or transmitted through networks can be stolen, modified, or fabricated by malicious users. Thus, it is important to know what security measures are available and how to use them. Network security practices are designed to prevent these potential problems. Network security, originated from meeting the needs of providing data confidentiality over public networks, has grown into a major academic discipline in both computer science and computer engineering, and also an important sector in the information industry.

The goal of network security is to give people the liberty of enjoying computer networks without fear of compromising their rights and interests. Network security accomplishes this goal by providing confidentiality, integrity, non-repudiation, and availability of useful data that are transmitted in open networks or stored in networked computers.

Network security will remain an active research area for several reasons. First, security measures that are effective today may no longer be effective tomorrow because of advancements and breakthroughs in computing theory, algorithms, and computer technologies. Second, after the known security problems are solved, other security loopholes which were previously unknown may at some point be discovered and exploited by attackers. Third, when new applications are developed or new technologies are invented, new security problems may also be created with them. Thus, network security is meant to be a long lasting scuffle between the offenders and the defenders.

Research and development in network security have mainly followed two lines. One line studies computer cryptography and uses it to devise security protocols. The other line examines loopholes and side effects of existing network protocols, software, and system configurations. It develops firewalls, anti-malicious-software software, intrusion detection systems, and other countermeasures. Interweaving these two lines together provides the basic building blocks for constructing deep layered defense systems against network security attacks.

This book is intended to provide a balanced treatment of network security along these two lines, with adequate materials and sufficient depth for teaching a one-semester introductory course on network security for graduate and upper-level undergraduate students. It is intended to inspire students to think about network security and prepare them for taking advanced network security courses. This book may also be used as a reference for IT professionals.

This book is structured into nine chapters.

Chapter 1 presents an overview of network security. It discusses network security goals, describes common network attacks, characterizes attackers, and defines a basic network security model.

Chapter 2 presents standard symmetric-key encryption algorithms, including DES, AES, and RC4. It discusses their strength and weaknesses. It also describes common block-cipher modes of operations and presents key generation algorithms.

Chapter 3 presents standard public-key encryption algorithms and key-exchange algorithms, including Diffie-Hellman key exchange, RSA public-key cryptosystem, and elliptic-curve cryptography. It also discusses how to transmit and manage keys.

Chapter 4 presents secure hash functions and message authentication code algorithms for the purpose of authenticating data, including the SHA-512 secure hash function, the WHIRLPOOL hash algorithm, cryptographic checksums, and the standard hash message authentication codes. It also presents the block-cipher offset-codebook mode of operations for producing ciphertext and message authentication code. It then discusses birthday attacks on secure hash functions, and describes the digital signature standard. Finally, this chapter introduces a dual signature scheme used for electronic transactions and a blind signature scheme used for producing electronic cash.

Chapter 5 presents several network security protocols commonly used in practice. It first describes a standard public-key infrastructure for managing public-key certificates. It then presents IPsec, a network-layer security protocol; SSL/TLS, a transport-layer security protocol; and several application-layer security protocols, including PGP and S/MIME for sending secure email messages, Kerberos for authenticating users in local area networks, and SSH for protecting remote logins.

Chapter 6 presents common security protocols for wireless local-area networks at the data-link layer, including WEP for providing wired-equivalent privacy, WPA and IEEE 802.11i/WPA2 for providing wireless protected access, and IEEE 802.1X for authenticating wireless users. It then presents the Bluetooth security protocol for wireless personal-area networks. Finally, it discusses security issues in wireless mesh networks.

Chapter 7 presents firewall technologies and basic structures, including network-layer packet filtering, transport-layer stateful inspections, transport-layer gateways, application-layer proxies, trusted systems and bastion hosts, firewall configurations and screened subnets, and network address translations.

Chapter 8 describes malicious software, such as viruses, worms, and Trojan horses, and introduces countermeasures. It also covers Web security and discusses mechanisms against denial of service attacks.

Chapter 9 presents intrusion detection technologies, including intrusion detection system architecture and common intrusion detection methods. It also discusses event signatures, statistical analysis, and data mining methods. Finally, it introduces honeypot technologies.

To get the most out of this book, readers are assumed to have taken undergraduate courses on discrete mathematics, algorithms, data communications, and network programming; or have equivalent preparations. For convenience, Chapter 3 includes a section reviewing basic concepts and results of number theory used in public-key cryptography. While it does not introduce socket programming, the book contains socket API client-server programming exercises. These exercises are designed for computer science and computer engineering students. Readers who do not wish to do them or simply do not have time to write code may skip them. Doing so would not affect learning the materials presented in the book.

Exercise problems are designed to have three levels of difficulty: regular, difficult (designated with *), and challenging (designated with **). This book contains a number of hands-on drills, presented as exercise problems. Readers are encouraged to try them all.

I have taught network security courses to graduate and senior undergraduate students for over ten years. And I have longed for a concise textbook with a balanced treatment of network security and sufficient depth suitable for teaching a one-semester introductory course for my students. This book is the result of this quest. It was written based on what I learned and experienced from teaching these courses and on student feedbacks accumulated over the years. In particular, I used an early draft of this book to teach a graduate network security course in 2006 and 2008 at University of Massachusetts Lowell, which helped me revise and enhance the materials presented in this book. Powerpoint slides of these lectures can be found at `http://www.cs.uml.edu/~wang/NetSec`.

Due to space limitations, some interesting topics and materials are not presented in this book. After all, one book can only accomplish one book's mission. I only hope that this book can achieve its objective. Of course, only you, the reader, can be the judge of it. I will be grateful if you can please offer your comments, suggestions, and corrections to me at wang@cs.uml.edu.

I have benefited a great deal from numerous discussions over the years with my colleagues and teaching assistants, as well as current and former students. I am full of gratitude to them. I am grateful to Sarah Agha, Samip Banker, Stephen Brinton, Jeff Brown, William Brown, Jason Chan, Guanling Chen, Michael Court, Chunyan Du, Paul Duvall, Adam Elbirt, Zheng Fang, Jami Foran, Swati Gupta, Liwu Hao, Qiang Hou, Bei Huang, Jared Karro, Minghui (Mark) Li, Benyuan Liu, Yan (Jenny) Liu, Wenjing Lou, Jie Lu, David Martin, Paul Nelson, Alexander Pennace, Sandeep Sahu, Blake Skinner, Hengky Susanto, Nathaniel Tuck, Tao Wang, Christopher Woodard, Fang Wu, Jianhui Xie, Jie (Jane) Yang, Zhijun Yu, and Ning Zhong for their help. In particular, I thank Jared Karro for reading the early draft of this book, Stephen Brinton for reading Chapters 1–5 and 7–8, Guanling Chen for reading Chapter 6, and Wenjing Lou for reading Chapters 1–2 and 6. Their comments have helped improve this book in many ways.

I thank Ying Liu at the Higher Education Press for initiating this book project and editing this book.

I owe more than I can express to my wife Helen, my son Jesse, and my daughter Sharon for their understanding that I needed to spend long hours working on this project.

Lowell, Massachusetts *Jie Wang*
June 2008

About the Author

Jie Wang is Professor and Chair of Computer Science at the University of Massachusetts Lowell (UML). He is also Director of the Center for Network and Information Security of UML. His first name "Jie" in Mandarin is pronounced similar to "Jed." He received Ph.D. degree in Computer Science from Boston University in 1990, M.S. degree in Computer Science from Zhongshan University in 1985, and B.S. degree in Computational Mathematics from Zhongshan University in 1982. He has over 18 years of teaching and research experience and is equipped with network security consulting experience in financial industry. His research interests include network security, algorithms and computational optimization, computational complexity theory, and wireless sensor networks. His research has been funded continuously by the National Science Foundation since 1991 and has also been funded by IBM, Intel, and the Natural Science Foundation of China. He has published over 95 journal and conference papers, two books and three edited books. He is active in professional service, including chairing conference program committees and organizing workshops.

Contents

Chapter 1
Network Security Overview

If you know your enemies and know yourself, you will win hundred times in hundred battles. If you know yourself but not your enemies, you will suffer a defeat for every victory won. If you do not know yourself or your enemies, you will always lose.

– Sun Tzu, "The Art of War"

The goal of network security is to give people the freedom to enjoy computer networks without fear of compromising their rights and interests. Network security therefore needs to guard networked computer systems and protect electronic data that is either stored in networked computers or transmitted in the networks. The Internet which is built on the IP communication protocols has become the dominant computer network technology. It interconnects millions of computers and edge networks into one immense network system. The Internet is a public network, where individuals or organizations can easily become subscribers of the Internet service by connecting their own computers and networking devices (e.g. routers and sniffers) to the Internet and paying a small subscription fee.

Since IP is a store-forward switching technology, where data is transmitted using routers controlled by other people, user A can read user B's data that goes through user A's network equipment. Likewise, user A's data transmitted in the Internet may also be read by user B. Hence, any individual or any organization may become an attacker, a target, or both. Even if one does not want to attack other people, it is still possible that one's networked computers may be compromised into becoming an attacking tool. Therefore, to achieve the goal of network security, one must first understand the attackers, what could become their targets, and how these targets might be attacked.

1.1 Mission and Definitions

The tasks of network security are to provide *confidentiality*, *integrity*, *non-repudiation*, and *availability* of useful *data* that are transmitted in public networks or stored in networked computers.

The concept of data has a broad sense in the context of network security. Any object that can be processed or executed by computers is data. Thus, source code, executable code, files in various formats, email messages, digital music, digital graphics, and digital video are each considered data. Data should only be read, written, or modified by legitimate users. That is, unauthorized individuals or organizations are not allowed to have access to data.

Just as CPU, RAM, hard disk, and network bandwidth are resources, data is also a resource. Data is sometimes referred to as *information* or *message*.

Each piece of data has two possible states, namely, the *transmission state* and the *storage state*. Data in the transmission state is simply data in the process of being delivered to a network destination. Data in the storage state is that which is stored in a local computer or in a storage device. Thus, the meanings of data confidentiality and data integrity have the following two aspects:

1. Provide and maintain the confidentiality and integrity of data that is in the transmission state. In this sense, confidentiality means that data during transmission cannot be read by any unauthorized user and integrity means that data during transmission cannot be modified or fabricated by any unauthorized user.
2. Provide and maintain the confidentiality and integrity of data that is in the storage state. Within this state, confidentiality means that data stored in a local device cannot be read by any unauthorized user through a network and integrity means that data stored in a local device cannot be modified or fabricated by any unauthorized user through a network.

Data non-repudiation means that a person who owns the data has no way to convince other people that he or she does not own it.

Data availability means that attackers cannot block legitimate users from using available resources and services of a networked computer. For example, a computer system infected with a virus should be able to detect and disinfect the virus without much delay, and a server hit by denial of service attacks should still be able to provide services to its users.

Unintentional components in protocol specifications, protocol implementations, or other types of software that are exploitable by attackers are often referred to as *loopholes*, *flaws*, or *defects*. They might be an imperfect minor step in a protocol design, an unforeseen side effect of a certain instruction in a program, or a misconfigured setting in a system.

Defense is the guiding principle of network security, but it is a passive defense because before being attacked the victim has no idea who the attackers are and from which computers in the jungle of the Internet the attackers will launch their attacks. After a victim is attacked, even if the attacker's identity and computer system is known, the victim still cannot launch a direct assault at the attacker, for such