<<计算机网络安全的理论与实践>>

图书基本信息

书名：<<计算机网络安全的理论与实践>>

13位ISBN编号：9787040241624

10位ISBN编号：7040241625

出版时间：2008-9

出版时间：高等教育出版社

作者：王杰

页数：384

前言

People today are increasingly relying on public computer networks to conduct busi-ness 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 prac-tices 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 secu-rity 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 discov-ered 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, soft-ware, and system configurations. It develops firewalls, anti-malicious-software soft-ware, 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.

内容概要

Computer Network Security Theory and Practice introduces to the reader a complete and concise view of network security. It provides in-depth theoretical coverage of recent advancements and practical solutions to network security threats. This book can be used for a one-semester network security course for graduate and upper-level undergraduate students, as well as a reference for IT professionals.

作者简介

作者：(美国)王杰 (Jie Wang)

<<计算机网络安全的理论与实践>>

书籍目录

1 Network Security Overview 1.1 Mission and Definitions 1.2 Common Attacks and Defense Mechanisms 1.2.1 Eavesdropping 1.2.2 Cryptanalysis 1.2.3 Password Pilfering 1.2.4 Identity Spoofing 1.2.5 Buffer-Overflow Exploitations 1.2.6 Repudiation 1.2.7 Intrusion 1.2.8 Traffic Analysis 1.2.9 Denial of Service Attacks 1.2.10 Malicious Software 1.3 Attacker Profiles 1.3.1 Hackers 1.3.2 Script Kiddies 1.3.3 Cyber Spies 1.3.4 Vicious Employees 1.3.5 Cyber Terrorists 1.3.6 Hypothetical Attackers 1.4 Basic Security Model 1.5 Security Resources 1.6 Closing Remarks 1.7 Exercises2 Data Eneryption Algorithms 2.1 Data Encryption Algorithm Design Criteria 2.1.1 ASCII Code 2.1.2 XOR Encryption 2.1.3 Criteria of Data Encryptions 2.1.4 Implementation Criteria 2.2 Data Encryption Standard 2.2.1 Feistel's Cipher Scheme 2.2.2 DES Subkeys 2.2.3 DES Substitution Boxes 2.2.4 DES Encryption 2.2.5 DES Decryption and Correctness Proof 2.2.6 DES Security Strength 2.3 Multiple DES 2.3.1 Triple-DES with Two Keys 2.3.2 2DES and 3DES/3 2.3.3 Meet-in-the-Middle Attacks on 2DES 2.4 Advanced Encryption Standard 2.4.1 AES Basic Structures 2.4.2 AES S-Boxes 2.4.3 AES-128 RoundKeys 2.4.4 Add Round Keys 2.4.5 Substitute-Bytes 2.4.6 Shift-Rows 2.4.7 Mix-Columns 2.4.8 AES-128 Encryption 2.4.9 AES-128 Decryption and Correctness Proof 2.4.10 Galois Fields 2.4.11 Construction of the AES S-Box and Its Inverse .. 2.4.12 AES Security Strength 2.5 Standard Block-Cipher Modes of Operations 2.5.1 Electronic-Codebook Mode 2.5.2 Cipher-Block-Chaining Mode 2.5.3 Cipher-Feedback Mode 2.5.4 Output-Feedback Mode 2.5.5 Counter Mode 2.6 Stream Ciphers 2.6.1 RC4 Stream Cipher 2.6.2 RC4 Security Weaknesses 2.7 Key Generations 2.7.1 ANSIX9.17 PRNG 2.7.2 BBS Pseudorandom Bit Generator 2.8 Closing Remarks 2.9 Exercises3 Public-Key Cryptography and Key Management 3.1 Concepts of Public-Key Cryptography 3.2 Elementary Concepts and Theorems in Number Theory . 3.2.1 Modular Arithmetic and Congruence Relations .. 3.2.2 Modular Inverse 3.2.3 Primitive Roots 3.2.4 Fast Modular Exponentiation 3.2.5 Finding Large Prime Numbers 3.2.6 The Chinese Remainder Theorem 3.2.7 Finite Continued Fractions 3.3 Diffie-Hellman Key Exchange4 Data Authentication5 Network Security Protocols in Practice6 Wireless Network Security7 Network Perimeter Security8 The Art of Anti Malicious Software9 The Art of Intrusion DetectionReferencesIndex

章节摘录

插图：

编辑推荐

《Computer Network Security:Theory And Practice》由高等教育出版社出版。

<<计算机网络安全的理论与实践>>

版权说明