

<<网络安全基础>>

图书基本信息

书名：<<网络安全基础>>

13位ISBN编号：9787302229728

10位ISBN编号：7302229724

出版时间：2010-7

出版时间：清华大学

作者：斯托林斯

页数：417

版权说明：本站所提供下载的PDF图书仅提供预览和简介，请支持正版图书。

更多资源请访问：<http://www.tushu007.com>

## 前言

In this age of universal electronic connectivity, of viruses and hackers, of electronic eavesdropping and electronic fraud, there is indeed no time at which security does not matter. Two trends have come together to make the topic of this book of vital interest. First, the explosive growth in computer systems and their interconnections via networks has increased the dependence of both organizations and individuals on the information stored and communicated using these systems. This, in turn, has led to a heightened awareness of the need to protect data and resources from disclosure, to guarantee the authenticity of data and messages, and to protect systems from network-based attacks. Second, the disciplines of cryptography and network security have matured, leading to the development of practical, readily available applications to enforce network security. It is the purpose of this book to provide a practical survey of network security applications and standards. The emphasis is on applications that are widely used on the Internet and for corporate networks, and on standards (especially Internet standards) that have been widely deployed. This book is intended for both an academic and a professional audience. As a textbook, it is intended as a one-semester undergraduate course on network security for computer science, computer engineering, and electrical engineering majors. It covers the material in IAS2 Security Mechanisms, a core area in the Information Technology body of knowledge; and NET4 Security, another core area in the Information Technology body of knowledge. These subject areas are part of the Draft ACM/IEEE Computer Society Computing Curricula 2005.

## <<网络安全基础>>

### 内容概要

本书由著名作者William Stallings编写，以当今网络安全的实际解决方案为基础，既简明扼要，又全面系统地介绍了网络安全的主要内容，包括基本原理、重要技术、主要方法和重要的工业标准等。全书共包含11章。

除第1章引言外，其余各章分为三大部分叙述：第一部分是密码学，重点介绍分组密码、流密码，消息认证码、安全杂凑函数、公钥密码和数字签名等的基本原理、主要方法和重要应用场景等，并简要介绍了几种常用的典型算法，包括DES算法、AES算法、RC4算法和RSA算法等；第二部分是网络安全应用，简要介绍了传输层安全中的SSL / TLS协议、无线局域网安全及WAP协议、电子邮件安全与PGP与SIM，ME协议、IP层安全与IPsec协议等。

第三部分是系统安全，简要介绍了入侵检测与口令管理、恶意软件与防火墙等。

本书以最新和实用的网络安全知识为主题，采用深入浅出的叙述手法，每章末尾还给出一定的推荐读物和思考练习题。

因此，本书既是高等学校网络安全基础课程的好教材，也是工程技术人员和网络爱好者了解网络安全基本概貌的好读物。

<<网络安全基础>>

作者简介

作者：（美国）斯托林斯（William Stallings）

## 书籍目录

Preface ix About the Author xiv Chapter 1 Introduction 1 1.1 Computer Security Concepts 3 1.2 The OSI Security Architecture 8 1.3 Security Attacks 9 1.4 Security Services 13 1.5 Security Mechanisms 16 1.6 A Model for Network Security 19 1.7 Standards 21 1.8 Outline of This Book 21 1.9 Recommended Reading 22 1.10 Internet and Web Resources 23 1.11 Key Terms, Review Questions, and Problems 25 PART ONE CRYPTOGRAPHY 27 Chapter 2 Symmetric Encryption and Message Confidentiality 27 2.1 Symmetric Encryption Principles 28 2.2 Symmetric Block Encryption Algorithms 34 2.3 Random and Pseudorandom Numbers 42 2.4 Stream Ciphers and RC4 45 2.5 Cipher Block Modes of Operation 50 2.6 Recommended Reading and Web Sites 55 2.7 Key Terms, Review Questions, and Problems 56 Chapter 3 Public-Key Cryptography and Message Authentication 61 3.1 Approaches to Message Authentication 62 3.2 Secure Hash Functions 67 3.3 Message Authentication Codes 73 3.4 Public-Key Cryptography Principles 79 3.5 Public-Key Cryptography Algorithms 83 3.6 Digital Signatures 90 3.7 Recommended Reading and Web Sites 90 3.8 Key Terms, Review Questions, and Problems 91 PART TWO NETWORK SECURITY APPLICATIONS 97 Chapter 4 Key Distribution and User Authentication 97 4.1 Symmetric Key Distribution Using Symmetric Encryption 98 4.2 Kerberos 99 4.3 Key Distribution Using Asymmetric Encryption 114 4.4 X.509 Certificates 116 4.5 Public-Key Infrastructure 124 4.6 Federated Identity Management 126 4.7 Recommended Reading and Web Sites 132 4.8 Key Terms, Review Questions, and Problems 133 Chapter 5 Transport-Level Security 139 5.1 Web Security Considerations 140 5.2 Secure Socket Layer and Transport Layer Security 143 5.3 Transport Layer Security 156 5.4 HTTPS 160 5.5 Secure Shell (SSH) 162 5.6 Recommended Reading and Web Sites 173 5.7 Key Terms, Review Questions, and Problems 173 Chapter 6 Wireless Network Security 175 6.1 IEEE 802.11 Wireless LAN Overview 177 6.2 IEEE 802.11i Wireless LAN Security 183 6.3 Wireless Application Protocol Overview 197 6.4 Wireless Transport Layer Security 204 6.5 WAP End-to-End Security 214 6.6 Recommended Reading and Web Sites 217 6.7 Key Terms, Review Questions, and Problems 218 Chapter 7 Electronic Mail Security 221 7.1 Pretty Good Privacy 222 7.2 S/MIME 241 7.3 DomainKeys Identified Mail 257 7.4 Recommended Reading and Web Sites 264 7.5 Key Terms, Review Questions, and Problems 265 Appendix 7A Radix-64 Conversion 266 Chapter 8 IP Security 269 8.1 IP Security Overview 270 8.2 IP Security Policy 276 8.3 Encapsulating Security Payload 281 8.4 Combining Security Associations 288 8.5 Internet Key Exchange 292 8.6 Cryptographic Suites 301 8.7 Recommended Reading and Web Sites 302 8.8 Key Terms, Review Questions, and Problems 303 PART THREE~ SYSTEM SECURITY 305 Chapter 9 Intruders 305 9.1 Intruders 307 9.2 Intrusion Detection 312 9.3 Password Management 323 9.4 Recommended Reading and Web sites 333 9.5 Key Terms, Review Questions, and Problems 334 Appendix 9A The Base-Rate Fallacy 337 Chapter 10 Malicious Soft-ware 340 10.1 Types of Malicious Software 341 10.2 Viruses 346 10.3 Virus Countermeasures 351 10.4 Worms 356 10.5 Distributed Denial of Service Attacks 365 10.6 Recommended Reading and Web Sites 370 10.7 Key Terms, Review Questions, and Problems 371 Chapter 11 Firewalls 374 11.1 The Need for Firewalls 375 11.2 Firewall Characteristics 376 11.3 Types of Firewalls 378 11.4 Firewall Basing 385 11.5 Firewall Location and Configurations 388 11.6 Recommended Reading and Web Site 393 11.7 Key Terms, Review Questions, and Problems 394 APPENDICES 398 Appendix A Some Aspects of Number Theory 398 A.1 Prime and Relatively Prime Numbers 399 A.2 Modular Arithmetic 401 Appendix B Projects for Teaching Network Security 403 B.1 Research Projects 404 B.2 Hacking Project 405 B.3 Programming Projects 405 B.4 Laboratory Exercises 406 B.5 Practical Security Assessments 406 B.6 Writing Assignments 406 B.7 Reading/Report Assignments 407 Index 408 ONLINE CHAPTERS Chapter 12 Network Management Security 12.1 Basic Concepts of SNMP 12.2 SNMPv1 Community Facility 12.3 SNMPv3 12.4 Recommended Reading and Web Sites 12.5 Key Terms, Review Questions, and Problems Chapter 13 Legal and Ethical Aspects 13.1 Cybercrime and Computer Crime 13.2 Intellectual Property 13.3 Privacy 13.4 Ethical Issues 13.5 Recommended Reading and Web Sites 13.6 Key Terms, Review Questions, and Problems

ONLINE APPENDICES Appendix C Standards and Standards-Setting Organizations C.1 The Importance of Standards C.2 Internet Standards and the Internet Society C.3 National Institute of Standards and Technology Appendix D TCP/IP and OSI D.1 Protocols and Protocol Architectures D.2 The TCP/IP Protocol Architecture D.3 The Role of an Internet Protocol D.4 IPv4 D.5 IPv6 D.6 The OSI Protocol Architecture Appendix E Pseudorandom Number Generation E.1 PRNG Requirements E.2 PRNG Using a Block Cipher E.3 PRNG Using a Hash Function or Message Authentication Code Appendix F Kerberos Encryption Techniques E.1 Password-to-Key Transformation E.2 Propagating Cipher Block Chaining Mode Appendix G Data Compression Using ZIP G.1 Compression Algorithm G.2 Decompression Algorithm Appendix H PGP Random Number Generation H.1 True Random Numbers H.2 Pseudorandom Numbers Appendix I The International Reference Alphabet Glossary References

## 章节摘录

插图：3DES has two attractions that assure its widespread use over the next few years. First, with its 168-bit key length, it overcomes the vulnerability to brute-force attack of DEA. Second, the underlying encryption algorithm in 3DES is the same as in DEA. This algorithm has been subjected to more scrutiny than any other encryption algorithm over a longer period of time, and no effective cryptanalytic attack based on the algorithm rather than brute force has been found. Accordingly, there is a high level of confidence that 3DES is very resistant to cryptanalysis. If security were the only consideration, then 3DES would be an appropriate choice for a standardized encryption algorithm for decades to come. The principal drawback of 3DES is that the algorithm is relatively sluggish in software. The original DEA was designed for mid-1970s hardware implementation and does not produce efficient software code. 3DES, which has three times as many rounds as DEA, is correspondingly slower. A secondary drawback is that both DEA and 3DES use a 64-bit block size. For reasons of both efficiency and security, a larger block size is desirable. Because of these drawbacks, 3DES is not a reasonable candidate for long-term use. As a replacement, NIST in 1997 issued a call for proposals for a new Advanced Encryption Standard (AES), which should have a security strength equal to or better than 3DES and significantly improved efficiency. In addition to these general requirements, NIST specified that AES must be a symmetric block cipher with a block length of 128 bits and support for key lengths of 128, 192, and 256 bits. Evaluation criteria included security, computational efficiency, memory requirements, hardware and software suitability, and flexibility.

编辑推荐

《网络安全基础:应用与标准(第4版)(影印版)》：大学计算机教育国外著名教材系列



版权说明

本站所提供下载的PDF图书仅提供预览和简介，请支持正版图书。

更多资源请访问:<http://www.tushu007.com>