

<<网络安全基础应用与标准>>

图书基本信息

书名：<<网络安全基础应用与标准>>

13位ISBN编号：9787302154518

10位ISBN编号：7302154511

出版时间：2007-8

出版时间：清华大学出版社

作者：斯托林斯

页数：413

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>

## <<网络安全基础应用与标准>>

### 内容概要

本书由著名作者William Stallings编写，完全从实用的角度出发，用较小的篇幅对当前网络安全解决方案中使用的主要算法、重要协议和系统管理方法等内容做了全面而详细的介绍。

全书共分为三部分：(1)密码算法和协议，包括网络安全应用中最常用的密码算法和协议；(2)网络安全应用，介绍了网络安全解决方案中使用的各种安全协议，如Kerberos、PGP、S/MIME、IPSec、SSL/TLS和SET等；(3)系统安全，介绍了一些系统级的安全问题，如网络入侵、恶意软件和防火墙等。

每章后面都提供了一定数量的推荐读物、网址、思考题和习题等。

全书最后还提供了一定数量的项目作业。

为方便使用本教材的教师搞好教学，出版社还提供了较为完整的配套服务。

与本书的前两版相比，第3版除在语言和叙述方面做进一步加工提高外，主要增加的内容包括RC4算法、公钥基础设施(PKI)、分布式拒绝服务攻击(DDoS)和信息技术安全评估通用准则等。

本书既可作为我国高校相关课程的教材使用，又是满足普通网络安全爱好者学习和了解网络安全基本知识的一本难得好书。

<<网络安全基础应用与标准>>

作者简介

作者：(美国)斯托林斯

<<网络安全基础应用与标准>>

书籍目录

Preface  
 Chapter 1 Introduction  
 1.1 Security Trends  
 1.2 The OSI Security Architecture  
 1.3 Security Attacks  
 1.4 Security Services  
 1.5 Security Mechanisms  
 1.6 A Model for Internetwork Security  
 1.7 Internet Standards the Internet Society  
 1.8 Outline of This Book  
 1.9 Recommended Reading  
 1.10 Internet and Web Resources  
 1.11 Key Terms , Review Question , and Problems  
 PART ONE CRYPTOGRAPHY  
 Chapter 2 Symmetric Encryption and Message Confidentiality  
 2.1 Symmetric Encryption Principles  
 2.2 Symmetric Block Encryption Algorithms  
 2.3 Stream Cipher and RC2  
 2.4 Cipher Block Modes of Operation  
 2.5 Location of Encryption Devices  
 2.6 Key Distribution  
 2.7 Recommended Reading and Web Sites  
 2.8 Key Terms , Review Question , and Problems  
 Chapter 3 Public-Key Cryptography and Message Authentication  
 3.1 Approaches to Message Authentication  
 3.2 Secure Hash Function and HMAC  
 3.3 Public Key Cryptography Principles  
 3.4 Public-Key Cryptography Algorithms  
 3.5 Digital Signatures  
 3.6 Key Management  
 3.7 Recommended Reading and Web Sites  
 3.8 Key Terms , Review Question , and Problems  
 PART TWO NETWORK SECURITY APPLICATIONS  
 Chapter 4 Authentication Applications  
 4.1 Kerberos  
 4.2 X.509 Directory Authentication Service  
 4.3 Public Key Infrastructure  
 4.4 Recommended Reading and Web Sites  
 4.4 Key Terms , Review Question , and Problems  
 Appendix 4A: Kerberos Encryption Techniques  
 Chapter 5 Electronic Mail Security  
 5.1 Pretty Good Privacy ( PGP )  
 5.2 S/MIME  
 5.3 Recommended Web Sites  
 5.4 Key Terms , Review Question , and Problems  
 Appendix 5A: Data Compression Using ZIP  
 Appendix 5B: Radix-64 Conveyance  
 Appendix 5C: PGP Random Number Generation  
 Chapter 6 IP Security  
 6.1 IP Security Overview  
 6.2 IP Security Architecture  
 6.3 Authentication Header  
 6.4 Encapsulating Security Payload  
 6.5 Combining Security Associations  
 6.6 Key Management  
 6.7 Recommended Reading and Web Sites  
 6.8 Key Terms , Review Question , and Problems  
 Appendix 6A: Internetworking and Internet Protocols  
 Chapter 7 Web Security  
 7.1 Web Security Requirements  
 7.2 Secure Sockets Layer ( SSL ) and Transport Layer Security ( TLS )  
 7.3 Secure Electronic Transaction ( SET )  
 7.4 Recommended Reading and Web Sites  
 7.5 Key Terms , Review Question , and Problems  
 Chapter 8 Network Management Security  
 8.1 Basic Concepts of SNMP  
 8.2 SNMPv1 Community Facility  
 8.3 SNMPv2  
 8.4 Recommended Reading and Web Sites  
 8.5 Key Terms , Review Question , and Problems  
 PART THREE SYSTEM SECURITY  
 Chapter 9 Intrusion  
 9.1 Intrusion  
 9.2 Intrusion Detection  
 9.3 Password Management  
 9.4 Recommended Reading and Web Sites  
 9.5 Key Terms , Review Question , and Problems  
 Appendix 9A: The Base-Rate Fallacy  
 Chapter 10 Malicious Software  
 10.1 Viruses and Related Threats  
 10.2 Virus Countermeasures  
 10.3 Distributed Denial of Service Attacks  
 10.4 Recommended Reading and Web Sites  
 10.5 Key Terms , Review Question , and Problems  
 Chapter 11 Firewalls  
 11.1 Firewall Design Principles  
 11.2 Trusted Systems  
 11.3 Common Criteria for Information Technology Security Evaluation  
 11.4 Recommended Reading and Web Sites  
 11.5 Key Terms , Review Question , and Problems  
 APPENDICES  
 Appendix A Some Aspects of Number Theory  
 A.1 Prime and Relatively Prime Numbers  
 A.2 Modular Arithmetic  
 Appendix B Projects for Teaching Network Security  
 B.1 Research Projects  
 B.2 Programming Projects  
 B.3 Laboratory Exercises  
 B.4 Writing Assignments  
 B.5 Reading/Report Assignments  
 Glossary  
 References  
 Index

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>