

<<网络安全基础教程>>

图书基本信息

书名：<<网络安全基础教程>>

13位ISBN编号：9787302077930

10位ISBN编号：7302077932

出版时间：2004-1-1

出版时间：清华大学出版社

作者：William Stallings

页数：409

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>

## <<网络安全基础教程>>

### 内容概要

本书是著名作者William Stallings的力作之一，详细介绍了网络安全的基础知识、应用及标准。全书共分为三部分：（1）密码算法和协议，包括网络应用中的密码算法和协议；（2）网络安全应用，介绍了一些主要的网络安全工具和应用，如Kerberos、x.509v3证书、PGP、S/MIME、IP安全、SSL/TLS、SET以及SNMPv3等；（3）系统安全，介绍了一些系统级的安全问题，如网络入侵与病毒的危害及对策，防火墙和托管系统的应用等。

此外，每章后面都提供了一定的练习和复习题，以便于读者对所学知识的巩固。

第2版新增高级加密标准的讨论，对病毒、蠕虫及非法入侵的论述也进行了扩充。

而且，教师和学习还可以通过访问[www.WilliamStallings.com/NetSec2e.html](http://www.WilliamStallings.com/NetSec2e.html)来获取补充材料。

本书可作为计算机科学、计算机工程、电子工程等相关专业本科生的网络安全课程教材，也是网络安全从业人员的自学用书。

## 书籍目录

CHAPTER 1 INTRODUCTION 1.1 The OSI Security Architecture 1.2 Security Attacks 1.3 Security Services  
1.4 Security mechanisms 1.5 A Model for Network Security 1.6 Internet Standards and the Internet Society 1.7  
Outline of This Book 1.8 Recommended Reading 1.9 Internet and Web ResourcesPART ONE  
CRYPTOGRAPHY CHAPTER 2 SYMMETRIC ENCRYPTION AND MESSAGE CONFIDENTIALITY 2.1  
Symmetric Encryption Principles 2.2 Symmetric Encryption Algorithms 2.3 Cipher Block Modes of Operation  
2.4 Location of Encryption Devices 2.5 Key Distribution 2.6 Recommended Reading and Web Sites 2.7 Key  
Terms,Review Questions,and Problems CHAPTER 3 PUBLIC-KEY CRYPTOGRAPHY AND MESSAGE  
AUTHENTICATION 3.1 Approaches to Message Authentication 3.2 Secure Hash Functions 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 Questions,and  
ProblemsPART TWO NETWORK SECURITY APPLICATIONS CHAPTER 4 AUTHENTICATION  
APPLICATIONS 4.1 Kerberos 4.2 X.509 Authentication Service 4.3 Recommended Reading and Web Sites  
4.4 Key Terms,Review Questions,and Problems Appendix 4A Kerberos Encryption Techniques CHAPTER 5  
ELECTRONIC MAIL SECURITY 5.1 Pretty Good Privacy 5.2 S/MIME 5.3 Recommended Web Sites 5.4  
Key Terms,Review Questions,and Problems Appendix 5A Data Compression Using Zip Appendix 5B  
RADIX-64 Conversion Appendix 5C PGP Random Number Generation CHAPTER 6 IP SECURITY 6.1 IP  
Security Overview 6.2 IP Security Architecture 6.3 Authenticaation 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 Questions,and Problems Appendix 6A Internetworking and Internet Protocols CHAPTER 7  
WEB SECURITY 7.1 Web Security Considerations 7.2 Secure Socket Layer and Transport Layer Security 7.3  
Secure Electronic Transaction 7.4 Recommended Reading and Web Sites 7.5 Key Terms,Review Questions,and  
Problems CHAPTER 8 NETWORK MANAGEMENT SECURITY 8.1 Basic Concepts of SNMP 8.2 SNMPv1  
Community Facility 8.3 SNMPv3 8.4 Recommended Reading and Web Sites 8.5 Key Terms,Review  
Questions,and ProblemsPART THREE SYSTEM SECURITY CHAPTER 9 INTRUDERS 9.1 Intruders 9.2  
Intrusion Detection 9.3 Password Management 9.4 Recommended Reading and Web Sites 9.5 Key  
Terms,Review Questions,and Problems Appendix 9A The Base-Rate Fallacy CHAPTER 10 MALICIOUS  
SOFTWARE 10.1 Viruses and Related Threats 10.2 Virus Countermeasures 10.3 Recommended Reading and  
Web Site 10.4 Key Terms,Review Questions,and ProblemsAPPENDICES APPENDIX A STANDARDS CITED  
IN THIS BOOK A.1 ANSI Standards A.2 Internet RFGs A.3 ITU-T Recommendations A.4 NIST Federal  
Information Processing Standards APPENDIX B SOME ASPECTS OF NUMBER THEORY B.1 Prime and  
Relatively Prime Numbers B.2 Modular ArithmeticGLOSSARYREFERENCESINDEX

<<网络安全基础教程>>

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>