

## <<计算机安全原理>>

### 图书基本信息

书名：<<计算机安全原理>>

13位ISBN编号：9787040167757

10位ISBN编号：7040167751

出版时间：2005-6

出版时间：第1版 (2005年6月1日)

作者：康克林 (Conklin, W.A.)

页数：651

字数：950000

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>

## <<计算机安全原理>>

### 内容概要

通过本书，既可以学习到计算机和网络安全的基础知识，又可以为参加 CompTIA 的 Security+ 认证考试做好准备；本书也涵盖了 (ISC)2 SSCP 认证考试的内容——该认证考试侧重于最佳实践、安全专家的角色以及责任。

本书由 IT 安全领域的专家编写，从信息安全的三个层面——技术、实践和意识——较为全面地阐述了通信、基础设施和操作安全的基本原理；还详细介绍了计算机系统和网络如何防御各种攻击。

本书共包含 24 章，分别讲述了以下主题：计算机安全概论与趋势，一般的安全概念，运营/组织安全，人员在安全中的作用，加密，公钥基础结构，标准和协议，物理安全对网络安全的影响，网络基础，基础结构安全，远程访问，无线通信与及时消息，安全基线，攻击和恶意代码，Email，Web 组件，软件开发，灾难恢复、业务连续性与组织策略，风险管理，变更管理，有关计算机的争论，安全与法律。

本书适合作为计算机专业、信息系统与管理专业、电子信息科学专业的本科生教材。

## &lt;&lt;计算机安全原理&gt;&gt;

## 书籍目录

Acknowledgments Foreword Preface Introduction Chapter 1 Introduction and Security Trends The Security Problem Security Incidents Threats to Security Security Trends Avenues of Attack The Steps in an Attack Minimizing Possible Avenues of Attack Types of Attacks Chapter Review Chapter 2 General Security Concepts Basic Security Terminology Security Basics Access Control Authentication Security Models Confidentiality Models Integrity Models Chapter Review Chapter 3 Operational/Organizational Security Security Operations in Your Organization Policies, Procedures, Standards, and Guidelines The Security Perimeter Physical Security Access Controls Physical Barriers Social Engineering Environment Fire Suppression Wireless Electromagnetic Eavesdropping Shielding Location Chapter Chapter 4 The Role of People in Security People--A Security Problem Poor Security Practices Social Engineering People as a Security Tool Security Awareness Chapter Review Chapter 5 Cryptography Algorithms Hashing SHA Message Digest (MD) Hashing Summary Symmetric Encryption DES 3DES AES CAST RC Blowfish IDEA Symmetric Encryption Summary Asymmetric Encryption RSA Diffie-Hellman ElGamal ECC Asymmetric Encryption Summary Usage Confidentiality Integrity Nonrepudiation Authentication Digital Signatures Key Escrow Chapter Review Chapter 6 Public Key Infrastructure The Basics of Public Key Infrastructures Certificate Authorities Registration Authorities Local Registration Authorities Certificate Repositories Trust and Certificate Verification Digital Certificates Certificate Attributes Certificate Extensions Certificate Lifecycles Centralized or Decentralized Infrastructures Hardware Storage Devices Private Key Protection Key Recovery Key Escrow Public Certificate Authorities In-House Certificate Authorities Outsourced Certificate Authorities Tying Different PIs Together Trust Models Certificate Usage Chapter Review Chapter 7 Standards and Protocols PKIX/PKCS PKIX Standards PKCS Why You Need to Know X.509 SSL/TLS ISAKMP CMP XKMS S/MIME IETF/S/MIME v3 Specifications PGP How It Works Where Can You Use PCP? HTFPS IPsec CEP FIPS Common Criteria (CC) WTLS WEP WEP Security Issues ISO 17799 Chapter Review Chapter 8 The Impact of Physical Security on Network Security The Problem Physical Security Safeguards Policies and Procedures Access Controls Authentication Chapter Review Chapter 9 Network Fundamentals Network Architectures Network Topology Network Protocols Packets TCP vs. UDP ICMP Packet Delivery Local Packet Delivery Remote Packet Delivery Subnetting Network Address Translation Chapter Review Chapter 10 Infrastructure Security Devices Workstations Savers Network Interface Cards (NICs) Hubs Bridges Switches Routers Firewalls Wireless Modems RAS Telecom/PBX VPN IDS Network Monitoring/Diagnostic Mobile Devices Media Coax UTP/STP Fiber Unguided Media Security Concerns for Transmission Media Physical Security Removable Media Magnetic Media Optical Media Electronic Media Security Topologies Security Zones VLANs NAT Tunneling Chapter Review Chapter 11 Remote Access The Remote Access Process Identification Authentication Authorization Telnet SSH L2TP and PIP PIP L2TP IEEE 802.11 VPN IPsec IPsec Configurations IPsec Security IEEE 802.1x RADIUS RADIUS Authentication RADIUS Authorization RADIUS Accounting DIAMETER TACACS+ TACACS+ Authentication TAGACS+ Authorization TAGACS+ Accounting Vulnerabilities Connection Summary Chapter Review Chapter 12 Wireless and Instant Messaging Wireless WAP and WTLS 802.11 Instant Messaging Chapter Review Chapter 13 Intrusion Detection Systems History of Intrusion Detection Systems IDS Overview Host-Based Intrusion Detection Systems Advantages of Host-Based IDSs Disadvantages of Host-Based IDSs Active vs. Passive Host-Based IDSs Network-Based Intrusion Detection Systems Advantages of a Network-Based IDS Disadvantages of a Network-Based IDS Active vs. Passive Network-Based IDSs Signatures False Positives and Negatives IDS Models Preventative Intrusion Detection Systems IDS Products and Vendors Honeypots Incident Response Chapter Review Chapter 14 Security Baselines Open, Jew Baselines Password Selection Password Policy/Guidelines Selecting a Password

<<计算机安全原理>>

Components of a Good Password Password Aging Operating System and Network Operating System  
 Hardening Hardening Microsoft Operating Systems Hardening UNIX-or Linux-BaSed Operating Systems  
 Network Hardening Software Updates Device Configuration Ports and Services Traffic Filtering  
 Application Hardening Application Patches Web Servers Mail Servers FIP Servers DNS Servers File  
 and Print Services Active Directory Chapter ReviewChapter 15 Attacks and Malware Attacking Computer  
 Systems and Networks DeniM-of-Service Attacks Backdoors and Trapdoors Sniffing Spoofing  
 Man-in-the-Middle Attacks Replay Attacks TCP/IP Hijacking Attacks on Encryption Password  
 Guessing Software Exploitation Wardialing and WarDriving Social Engineering Malware Auditing  
 Chapter ReviewChapter 16 E-mail Security of E-mail Transmissions Malidous Code Hoax E-mails  
 Unsolicited Commercial E-mail (Spare) Mail Encrypfon Chapter ReviewChapter 17 Web Components  
 Current Web Components and Concerns Protocols Encryption (SSL and TLS) The Web (HTTP and  
 HTIPS) Web Services Directory Services (DAP and LDAP) File Transfer (FIT and SFTP) Vulnerabilities  
 Code-Based Vulnerabilities Buffer Overflows Java and javaScript ActiveX CGI Server-Side Scripts  
 Cookies Signed Applets Browser Plug-Ins Chapter ReviewChapter 18 Software Development The  
 Software EngineeingProcess Process Models ROI and Error Correction Secure Code Techniques Good  
 Practices Requirements Testing Chapter ReviewChapter 19 Disaster Recovery, Business Continuity, and  
 Organizational Policies Disaster Recovery Disaster Recovery Plans/Process Backups Utilities Secure  
 Recovery High Availability and Fault Tolerance Computer Incident Response Teams Test, Exercise, and  
 Rehearse Policies and Procedures Security Policies Privacy Service Level Agreements Human Resources  
 Policies Code of Ethics Incident Response Policies Chapter Review Chapter 20 Risk Management An  
 Overview of Risk Management Macro-Level Example of Risk Management International Banking Key  
 Terms Essential to Understanding Risk Management What Is Risk Management? Business Risks Examples of  
 Business Risks Examples of Technology Risks Risk Management Models General Risk Management Model  
 Software Engineering Institute Model Qualitatively Assessing Risk Quantitatively Assessing Risk  
 Qualitative vs. Quantitative Risk Assesmem Tools Chapter ReviewChapter 21 Change Management  
 Why Change Management? The Key Concept: Segregation of Duties Elements of Change Management  
 Implementing Change Management The Purpose of a Change Control Board Code Integrity The  
 Capability Maturity Model Chapter ReviewChapter 22 Privilege Management User, Group, and Role  
 Management User. Groups Role Single Sign-On Centralized vs. Decentralized Management  
 Centralized Management Decentralized Management The Decentralized, Genralized Model Auditing  
 (Privilege, Usage, and Escalation) Privilege Auditing Usage Auditing Escalation Auditing Handling  
 Access Control (MAC, DAC, and RBAC) Mandatory Access Control (MAC) Discretionary Access Control  
 (DAC) Role-Based Access Control (RBAC) Chapter Review Chapter 23 Computer Forensics Evidence  
 Standards for Evidence Types of Evidence Three Rules Regarding Evidence Collecting Evidence  
 Acquiring Evidence Identifying Evidence Protecting Evidence Transporting Evidence Storing  
 Evidence Conducting the Investigation Chain of Custody Free Space vs. Slack Space Free Space Slack  
 Space What's This Message Digest and Hash? Analysis Chapter ReviewChapter 24 Security and Law  
 Import/Export Encryption Restrictions United States Law Non-U.S. Laws Digital Signature Laws  
 Non-U.S. Laws Digital Rights Management Privacy Laws United States Laws European Laws  
 Computer Trespass Convention on Cybercrime Ethics Chapter Review GlossaryIndex

<<计算机安全原理>>

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>