



全国工程硕士专业学位教育指导委员会推荐教材

计算机网络安全

——协议、技术与应用

黄河 编著 李伟琴 审核

<http://www.tup.com.cn>



清华大学出版社

- 软件质量保证、测试与评价
- 软件需求工程
- 软件工程过程
- 计算机网络安全——协议、技术与应用
- 信息系统分析与设计

ISBN 978-7-302-18057-9



9 787302 180579 >

定价：49.00元

内 容 简 介

本书以 TCP/IP 网络安全协议为核心,全面、系统地论述计算机网络安全协议、技术与应用等问题。全书共分为三个部分:网络安全基础部分,包括网络安全概述、密码学基础、数字认证技术和公钥基础设施等;网络安全协议部分,分层描述计算机网络各层的安全协议及其应用,包括网络层的 IPSec,传输层的 SSL/TLS,应用层的 S/MIME、PGP、SSH、DNSSEC、TSIG、SNMPv3 等;网络安全技术与应用部分,详细讲解防火墙、VPN、访问控制、入侵检测、系统审计等较为成熟的网络安全技术,同时还介绍了移动 IP 安全、无线网络安全、Web Service 安全等网络安全新技术。

本书可作为通信、计算机等相关专业的大学本科生和研究生教材,也可作为从事计算机网络与信息安全工作的工程技术人员和广大爱好者的参考书。

本书封面贴有清华大学出版社防伪标签,无标签者不得销售。

版权所有,侵权必究。侵权举报电话:010-62782989 13701121933

图书在版编目(CIP)数据

计算机网络安全——协议、技术与应用/黄河编著. —北京:清华大学出版社,2008.9
(全国工程硕士专业学位教育指导委员会推荐教材)

ISBN 978-7-302-18057-9

I. 计… II. 黄… III. 计算机网络—安全技术—研究生—教材 IV. TP393.08

中国版本图书馆 CIP 数据核字(2008)第 098217 号

责任编辑:丁 岭 赵晓宁

责任校对:梁 毅

责任印制:李红英

出版发行:清华大学出版社

地 址:北京清华大学学研大厦 A 座

<http://www.tup.com.cn>

邮 编:100084

社 总 机:010-62770175

邮 购:010-62786544

投稿与读者服务:010-62776969, c-service@tup.tsinghua.edu.cn

质 量 反 馈:010-62772015, zhiliang@tup.tsinghua.edu.cn

印 装 者:北京鑫海金澳胶印有限公司

经 销:全国新华书店

开 本:185×230 印 张:25.5 字 数:551 千字

版 次:2008 年 9 月第 1 版 印 次:2008 年 9 月第 1 次印刷

印 数:1~3000

定 价:49.00 元

本书如存在文字不清、漏印、缺页、倒页、脱页等印装质量问题,请与清华大学出版社出版部联系调换。联系电话:(010)62770177 转 3103 产品编号:023457-01

目 录

| | |
|-------------------------|-----|
| 本章实验 | 79 |
| 思考题 | 79 |
| 第4章 公钥基础设施 | 79 |
| 4.1 PKI概述 | 80 |
| 4.2 PKI技术发展及应用现状 | 82 |
| 4.3 PKI体系结构 | 83 |
| 4.4 X.509证书 | 87 |
| 第一部分 网络安全基础 | |
| 第1章 网络安全概述 | /3 |
| 1.1 网络安全的概念及目标 | 3 |
| 1.2 网络安全现状 | 5 |
| 1.3 ISO/OSI 网络安全体系 | 8 |
| 1.3.1 安全策略 | 8 |
| 1.3.2 安全服务 | 11 |
| 1.3.3 安全机制 | 12 |
| 1.3.4 安全管理 | 14 |
| 1.4 典型网络安全模型 | 15 |
| 1.4.1 动态自适应网络模型 | 15 |
| 1.4.2 APPDRR 模型 | 16 |
| 1.4.3 分层的网络安全解决方案 | 17 |
| 1.5 网络安全评估规范 | 20 |
| 1.5.1 可信计算机系统评估准则 | 21 |
| 1.5.2 通用准则 | 23 |
| 1.5.3 信息安全保障技术框架 | 24 |
| 1.5.4 计算机信息系统安全保护等级划分准则 | 27 |
| 本章实验 | 28 |
| 思考题 | 28 |
| 第2章 密码学基础 | /29 |
| 2.1 密码学概述 | 29 |
| 2.1.1 密码算法和密钥 | 30 |

Contents

| | | |
|-----------------------|----------------------|----|
| 2.1.2 | 密码算法分类 | 30 |
| 2.1.3 | 密码分析与计算复杂性 | 32 |
| 2.2 | 对称密钥算法 | 33 |
| 2.2.1 | DES | 33 |
| 2.2.2 | 3DES | 34 |
| 2.2.3 | 其他对称密钥算法 | 34 |
| 2.3 | 公钥算法 | 36 |
| 2.3.1 | RSA | 36 |
| 2.3.2 | Diffie-Hellman | 37 |
| 2.4 | 哈希算法 | 38 |
| 2.4.1 | MD5 | 38 |
| 2.4.2 | SHA | 40 |
| 2.5 | 密码协议 | 41 |
| | 本章实验 | 42 |
| | 思考题 | 42 |
| 第3章 数字认证技术 /43 | | |
| 3.1 | 认证技术概述 | 43 |
| 3.1.1 | 报文鉴别 | 43 |
| 3.1.2 | 身份鉴别 | 44 |
| 3.2 | 密码鉴别 | 44 |
| 3.2.1 | 密码与密码攻击 | 44 |
| 3.2.2 | 验证码 | 47 |
| 3.2.3 | 一次一密密码 | 49 |
| 3.2.4 | 基于挑战/应答的鉴别 | 50 |
| 3.3 | 基于密钥的鉴别 | 52 |
| 3.3.1 | 基于对称密钥的鉴别 | 52 |
| 3.3.2 | 基于非对称密钥的鉴别 | 53 |
| 3.3.3 | 基于第三方的鉴别 | 54 |
| 3.4 | 数字签名 | 55 |
| 3.5 | 认证技术的应用 | 57 |
| 3.5.1 | PPP 中的认证 | 57 |
| 3.5.2 | AAA 协议及其应用 | 67 |
| 3.5.3 | Kerberos 鉴别 | 73 |
| 3.5.4 | S/KEY 一次性密码鉴别 | 77 |

| | |
|------------|----|
| 本章实验 | 79 |
| 思考题 | 79 |

第 4 章 公钥基础设施 /80

| | |
|------------------------------|-----|
| 4.1 PKI 概述 | 80 |
| 4.2 PKI 技术发展及应用现状 | 82 |
| 4.3 PKI 体系结构——PKIX 模型 | 83 |
| 4.4 X.509 证书 | 87 |
| 4.5 PKI 信任模型 | 90 |
| 4.6 密钥和证书的生命周期 | 95 |
| 4.6.1 密钥/证书生命周期管理 | 95 |
| 4.6.2 密钥生命周期 | 97 |
| 4.6.3 证书生命周期 | 98 |
| 4.7 PKI 相关标准 | 100 |
| 4.8 成熟 PKI 系统简介 | 107 |
| 4.8.1 商业应用 | 108 |
| 4.8.2 政府应用 | 109 |
| 4.9 PKI 实施与应用案例 | 111 |
| 4.9.1 小型 PKI 和 CA 设计案例 | 111 |
| 4.9.2 大型 PKI 系统设计案例 | 114 |
| 4.9.3 PKI 应用简介 | 116 |
| 本章实验 | 121 |
| 思考题 | 121 |

第二部分 TCP/IP 网络安全协议

第 5 章 网络层安全协议 /125

| | |
|-----------------------|-----|
| 5.1 IPSec 概述 | 125 |
| 5.2 IPSec 体系结构 | 126 |
| 5.3 Ipsec 的操作模式 | 127 |
| 5.4 安全策略与安全协议 | 129 |
| 5.5 密钥交换协议 | 133 |
| 5.5.1 ISAKMP | 133 |
| 5.5.2 IKE | 135 |

| | | |
|--------------|-------------------|------|
| 5.5.3 | IKE 在 IPSec 中的应用 | 138 |
| 5.6 | 验证头 AH | 139 |
| 5.6.1 | AH 报文格式 | 139 |
| 5.6.2 | AH 操作模式 | 141 |
| 5.6.3 | AH 协议处理过程 | 143 |
| 5.7 | 封装安全载荷 ESP | 144 |
| 5.7.1 | ESP 报文格式 | 144 |
| 5.7.2 | ESP 操作模式 | 145 |
| 5.7.3 | ESP 协议处理及 AH 嵌套 | 148 |
| 5.8 | IPSec 的应用 | 149 |
| | 本章实验 | 151 |
| | 思考题 | 151 |
| 第 6 章 | 传输层安全协议 | /152 |
| 6.1 | SSL 协议 | 152 |
| 6.1.1 | SSL 概述 | 152 |
| 6.1.2 | SSL 连接与会话 | 154 |
| 6.1.3 | SSL 握手协议 | 155 |
| 6.1.4 | SSL 记录集协议 | 160 |
| 6.1.5 | SSL 密码计算 | 161 |
| 6.1.6 | SSL 协议的应用 | 163 |
| 6.2 | SSH 协议 | 164 |
| 6.2.1 | SSH 概述 | 164 |
| 6.2.2 | SSH 协议体系结构 | 165 |
| 6.2.3 | SSH 协议分析 | 166 |
| 6.2.4 | SSH 协议的通信过程 | 172 |
| 6.2.5 | SSH 协议的应用 | 179 |
| 6.3 | SOCKS 协议 | 180 |
| 6.3.1 | SOCKS 协议概述 | 180 |
| 6.3.2 | SOCKS 协议通信过程 | 181 |
| | 本章实验 | 183 |
| | 思考题 | 183 |
| 第 7 章 | 应用层安全协议 | /184 |
| 7.1 | Internet 的应用层安全隐患 | 184 |

| | | |
|-------|--------------------|-----|
| 7.2 | WWW 安全 | 186 |
| 7.2.1 | WWW 安全保障体系 | 186 |
| 7.2.2 | HTTP 安全协议 | 189 |
| 7.3 | 电子邮件安全协议 | 190 |
| 7.3.1 | 电子邮件及其安全性概述 | 190 |
| 7.3.2 | S/MIME | 192 |
| 7.3.3 | PGP | 199 |
| 7.3.4 | 垃圾邮件防御技术介绍 | 209 |
| 7.4 | DNS 安全协议 | 211 |
| 7.4.1 | DNS 脆弱性分析 | 211 |
| 7.4.2 | DNS 安全防护策略 | 216 |
| 7.4.3 | DNSSEC 协议概述 | 217 |
| 7.4.4 | DNSSEC 密钥管理 | 221 |
| 7.4.5 | DNSSEC 签名验证及公钥信任机制 | 223 |
| 7.4.6 | TSIG 和 TKEY | 225 |
| 7.5 | SNMP 安全协议 | 227 |
| 7.5.1 | SNMP 及其安全性概述 | 227 |
| 7.5.2 | SNMPv3 的体系结构 | 228 |
| 7.5.3 | SNMPv3 安全服务的实现 | 232 |
| | 本章实验 | 235 |
| | 思考题 | 235 |

第三部分 网络安全技术与应用

第 8 章 企业级安全技术

/239

| | | |
|-------|-----------|-----|
| 8.1 | 虚拟专用网 | 239 |
| 8.1.1 | VPN 概述 | 239 |
| 8.1.2 | VPN 分类 | 242 |
| 8.1.3 | PPTP | 243 |
| 8.1.4 | L2F/L2TP | 250 |
| 8.1.5 | MPLS VPN | 254 |
| 8.1.6 | VPN 实施示例 | 261 |
| 8.2 | 访问控制与安全审计 | 263 |
| 8.2.1 | 访问控制策略 | 263 |
| 8.2.2 | 访问控制实施模型 | 268 |

| | | |
|----------------------------|---------------|-------------|
| 8.2.3 | 访问控制实施策略 | 271 |
| 8.2.4 | 访问控制语言 | 274 |
| 8.2.5 | 安全审计 | 275 |
| 8.3 | 防火墙技术 | 280 |
| 8.3.1 | 防火墙概述 | 280 |
| 8.3.2 | 防火墙分类 | 281 |
| 8.3.3 | 防火墙相关技术 | 285 |
| 8.3.4 | 防火墙应用模式 | 291 |
| 8.4 | 入侵检测系统 | 296 |
| 8.4.1 | 入侵检测概述 | 296 |
| 8.4.2 | 入侵检测系统的分类 | 298 |
| 8.4.3 | 入侵检测系统模型 | 303 |
| 8.4.4 | 分布式入侵检测系统 | 306 |
| 8.4.5 | SNORT 入侵检测系统 | 309 |
| 8.4.6 | 入侵检测的发展趋势 | 314 |
| | 本章实验 | 315 |
| | 思考题 | 315 |
| 第 9 章 无线网络及移动 IP 安全 | | /316 |
| 9.1 | 无线网络安全概述 | 316 |
| 9.1.1 | 无线网络及其分类 | 316 |
| 9.1.2 | 无线网络安全性分析 | 318 |
| 9.2 | 常用无线局域网安全技术 | 321 |
| 9.2.1 | 传统安全措施 | 321 |
| 9.2.2 | 增强安全机制 | 324 |
| 9.3 | 802.11X 认证机制 | 327 |
| 9.3.1 | 802.1x 框架结构 | 327 |
| 9.3.2 | 802.1x 安全性分析 | 332 |
| 9.3.3 | 高层认证协议 | 333 |
| 9.3.4 | 802.1x 协议技术特点 | 337 |
| 9.4 | WAPI | 338 |
| 9.4.1 | WAPI 的工作原理 | 339 |
| 9.4.2 | WAPI 的特点 | 340 |
| 9.5 | 移动 IP 安全概述 | 341 |
| 9.5.1 | 移动 IP 概述 | 341 |

| | | |
|--------------------------------------|----------------------------|-----|
| 9.5.2 | 移动 IP 的工作原理 | 342 |
| 9.5.3 | 移动 IP 面临的安全威胁及对策 | 346 |
| 9.6 | 移动 IP 安全机制 | 351 |
| 9.6.1 | 基于 AAA 的移动 IP 认证机制 | 351 |
| 9.6.2 | 基于公钥的移动 IP 安全构架 | 353 |
| 9.6.3 | 移动 IPSec 方案 | 356 |
| 9.6.4 | 穿越防火墙的 IP 移动方案 | 357 |
| | 思考题 | 358 |
| 第 10 章 Web Service 与网络安全 /359 | | |
| 10.1 | Web Service 及其安全性概述 | 359 |
| 10.1.1 | Web Service 简介 | 359 |
| 10.1.2 | Web Service 的安全性需求 | 361 |
| 10.2 | Web Service 安全技术概述 | 362 |
| 10.2.1 | XML 签名 | 363 |
| 10.2.2 | XML 加密 | 365 |
| 10.2.3 | Soap 消息安全保护 | 366 |
| 10.3 | WS-Security | 367 |
| 10.3.1 | WS-Security 消息模型 | 369 |
| 10.3.2 | WS-Security 基本语法要素 | 369 |
| 10.3.3 | WS-Security 安全令牌信任机制 | 372 |
| 10.4 | 网格及其安全性概述 | 373 |
| 10.4.1 | 网格体系结构及其特性 | 373 |
| 10.4.2 | 网格环境中的安全挑战 | 377 |
| 10.4.3 | 网格的安全性需求及其安全架构 | 379 |
| 10.5 | 网络安全基础设施 | 380 |
| 10.5.1 | GSI 概述 | 380 |
| 10.5.2 | GSI 关键技术 | 381 |
| | 思考题 | 386 |
| 参考文献 /387 | | |