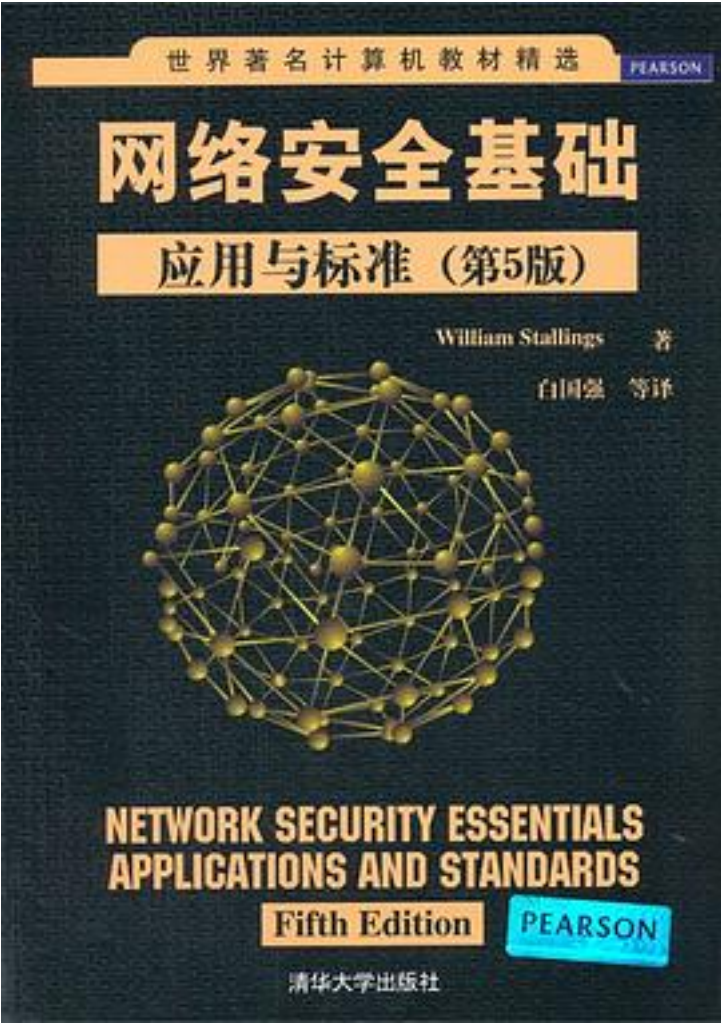


网络安全基础 (第5版)



[网络安全基础 \(第5版\) 下载链接1](#)

著者:William Stallings

出版者:清华大学出版社

出版时间:2014-5

装帧:

isbn:9787302348078

作者介绍:

目录: 第1章 引言 1

1.1 计算机安全概念 2

1.1.1 计算机安全的定义 2

1.1.2 计算机安全挑战 5

1.2 OSI安全体系结构 6

1.3 安全攻击 6

1.3.1 被动攻击 7

1.3.2 主动攻击 8

1.4 安全服务 8

1.4.1 认证 8

1.4.2 访问控制 9

1.4.3 数据机密性 10

1.4.4 数据完整性 10

1.4.5 不可抵赖性 10

1.4.6 可用性服务 10

1.5 安全机制 11

1.6 网络安全模型 12

1.7 标准 14

1.8 本书概览 14

1.9 推荐读物 14

1.10 网络资源 15

1.11 关键词、思考题和习题 16

1.11.1 关键词 16

1.11.2 思考题 16

1.11.3 习题 17

第1部分 密码学

第2章 对称加密和消息机密性 21

2.1 对称加密原理 21

2.1.1 密码体制 22

2.1.2 密码分析 23

2.1.3 Feistel密码结构 24

2.2 对称分组加密算法 26

2.2.1 数据加密标准 26

2.2.2 三重DES 27

2.2.3 高级加密标准 28

2.3 随机数和伪随机数 31

2.3.1 随机数的应用 32

2.3.2 真随机数发生器、伪随机数生成器和伪随机函数 32

2.3.3 算法设计 33

2.4 流密码和RC4 34

2.4.1 流密码结构 34

2.4.2 RC4算法 35

2.5 分组密码工作模式 37

2.5.1 电子密码本模式 37

2.5.2 密码分组链接模式 38

2.5.3 密码反馈模式 39

2.5.4 计数器模式 40

2.6 推荐读物 42

2.7 关键词、思考题和习题 42

2.7.1 关键词 42

2.7.2 思考题 42

- 2.7.3 习题 43
- 第3章 公钥密码和消息认证 47
 - 3.1 消息认证方法 47
 - 3.1.1 利用常规加密的消息认证 48
 - 3.1.2 非加密的消息认证 48
 - 3.2 安全散列函数 51
 - 3.2.1 散列函数的要求 51
 - 3.2.2 散列函数的安全性 52
 - 3.2.3 简单散列函数 52
 - 3.2.4 SHA安全散列函数 54
 - 3.3 消息认证码 56
 - 3.3.1 HMAC 56
 - 3.3.2 基于分组密码的MAC 58
 - 3.4 公钥密码原理 61
 - 3.4.1 公钥密码思想 61
 - 3.4.2 公钥密码系统的应用 62
 - 3.4.3 公钥密码的要求 63
 - 3.5 公钥密码算法 63
 - 3.5.1 RSA公钥密码算法 64
 - 3.5.2 Diffie-Hellman密钥交换 66
 - 3.5.3 其他公钥密码算法 69
 - 3.6 数字签名 70
 - 3.7 推荐读物 70
 - 3.8 关键词、思考题和习题 71
 - 3.8.1 关键词 71
 - 3.8.2 思考题 71
 - 3.8.3 习题 71
- 第2部分 网络安全应用
- 第4章 密钥分配和用户认证 79
 - 4.1 基于对称加密的密钥分配 79
 - 4.2 Kerberos 80
 - 4.2.1 Kerberos版本4 81
 - 4.2.2 Kerberos版本5 89
 - 4.3 基于非对称加密的密钥分配 92
 - 4.3.1 公钥证书 92
 - 4.3.2 基于公钥密码的秘密密钥分发 92
 - 4.4 X.509证书 93
 - 4.4.1 证书 94
 - 4.4.2 X.509版本3 98
 - 4.5 公钥基础设施 100
 - 4.5.1 PKIX管理功能 100
 - 4.5.2 PKIX管理协议 101
 - 4.6 联合身份管理 101
 - 4.6.1 身份管理 102
 - 4.6.2 身份联合 103
 - 4.7 推荐读物 106
 - 4.8 关键词、思考题和习题 107
 - 4.8.1 关键词 107
 - 4.8.2 思考题 108
 - 4.8.3 习题 108
- 第5章 网络访问控制和云安全 112
 - 5.1 网络访问控制 112
 - 5.1.1 网络访问控制系统的组成元素 113
 - 5.1.2 网络访问强制措施 114

5.2 可扩展认证协议	115
5.2.1 认证方法	115
5.2.2 EAP交换协议	116
5.3 IEEE 802.1X基于端口的网络访问控制	118
5.4 云计算	120
5.4.1 云计算组成元素	120
5.4.2 云计算参考架构	122
5.5 云安全风险和对策	124
5.6 云端数据保护	126
5.7 云安全即服务	129
5.8 推荐读物	131
5.9 关键词、思考题和习题	132
5.9.1 关键词	132
5.9.2 思考题	132
5.9.3 习题	132
第6章 传输层安全	133
6.1 Web安全需求	133
6.1.1 Web安全威胁	134
6.1.2 Web流量安全方法	135
6.2 安全套接字层和传输层安全	135
6.2.1 SSL体系结构	135
6.2.2 SSL记录协议	137
6.2.3 修改密码规格协议	139
6.2.4 警报协议	139
6.2.5 握手协议	140
6.2.6 密码计算	145
6.3 传输层安全	146
6.3.1 版本号	146
6.3.2 消息认证码	146
6.3.3 伪随机函数	147
6.3.4 警报码	148
6.3.5 密码套件	148
6.3.6 客户端证书类型	148
6.3.7 certificate_verify和finished消息	149
6.3.8 密码计算	149
6.3.9 填充	149
6.4 HTTPS	150
6.4.1 连接初始化	150
6.4.2 连接关闭	150
6.5 SSH	151
6.5.1 传输层协议	151
6.5.2 用户身份认证协议	155
6.5.3 连接协议	156
6.6 推荐读物	160
6.7 关键词、思考题和习题	160
6.7.1 关键词	160
6.7.2 思考题	160
6.7.3 习题	160
第7章 无线网络安全	162
7.1 无线安全	162
7.1.1 无线网络安全威胁	163
7.1.2 无线安全措施	163
7.2 移动设备安全	164
7.2.1 安全威胁	165

7.2.2 移动设备安全策略	166
7.3 IEEE 802.11无线局域网概述	168
7.3.1 Wi-Fi联盟	168
7.3.2 IEEE 802协议架构	169
7.3.3 IEEE 802.11网络组成与架构模型	170
7.3.4 IEEE 802.11服务	171
7.4 IEEE 802.11i无线局域网安全	172
7.4.1 IEEE 802.11i服务	173
7.4.2 IEEE 802.11i操作阶段	173
7.4.3 发现阶段	175
7.4.4 认证阶段	177
7.4.5 密钥管理阶段	178
7.4.6 保密数据传输阶段	181
7.4.7 IEEE 802.11i伪随机数函数	182
7.5 推荐读物	183
7.6 关键词、思考题和习题	184
7.6.1 关键词	184
7.6.2 思考题	184
7.6.3 习题	185
第8章 电子邮件安全	187
8.1 PGP	187
8.1.1 符号约定	188
8.1.2 操作描述	188
8.2 S/MIME	192
8.2.1 RFC 5322	192
8.2.2 多用途网际邮件扩展	193
8.2.3 S/MIME的功能	198
8.2.4 S/MIME消息	199
8.2.5 S/MIME证书处理过程	202
8.2.6 增强的安全性服务	204
8.3 DKIM	204
8.3.1 互联网邮件体系结构	204
8.3.2 E-mail威胁	206
8.3.3 DKIM策略	207
8.3.4 DKIM的功能流程	208
8.4 推荐读物	209
8.5 关键词、思考题和习题	209
8.5.1 关键词	209
8.5.2 思考题	210
8.5.3 习题	210
第9章 IP安全	211
9.1 IP安全概述	212
9.1.1 IPSec的应用	212
9.1.2 IPSec的好处	212
9.1.3 路由应用	213
9.1.4 IPSec文档	214
9.1.5 IPSec服务	214
9.1.6 传输模式和隧道模式	214
9.2 IP安全策略	216
9.2.1 安全关联	216
9.2.2 安全关联数据库	216
9.2.3 安全策略数据库	217
9.2.4 IP通信进程	218
9.3 封装安全载荷	220

- 9.3.1 ESP格式 220
- 9.3.2 加密和认证算法 221
- 9.3.3 填充 222
- 9.3.4 防止重放服务 222
- 9.3.5 传输模式和隧道模式 223
- 9.4 安全关联组合 226
 - 9.4.1 认证加保密 226
 - 9.4.2 安全关联的基本组合 227
- 9.5 因特网密钥交换 228
 - 9.5.1 密钥确定协议 229
 - 9.5.2 报头和载荷格式 231
- 9.6 密码套件 235
- 9.7 推荐读物 236
- 9.8 关键词、思考题和习题 237
 - 9.8.1 关键词 237
 - 9.8.2 思考题 237
 - 9.8.3 习题 237
- 第3部分 系统安全
- 第10章 恶意软件 241
 - 10.1 恶意软件类型 242
 - 10.1.1 恶意软件的分类 242
 - 10.1.2 攻击套件 243
 - 10.1.3 攻击源头 243
 - 10.2 传播-感染内容-病毒 243
 - 10.2.1 病毒的本质 244
 - 10.2.2 病毒分类 246
 - 10.3 传播-漏洞利用-蠕虫 248
 - 10.3.1 目标搜寻 249
 - 10.3.2 蠕虫传播模式 249
 - 10.3.3 蠕虫病毒技术现状 251
 - 10.3.4 恶意移动代码 251
 - 10.3.5 客户端漏洞和网站挂马攻击 252
 - 10.4 传播-社会工程-垃圾邮件与特洛伊木马 252
 - 10.4.1 垃圾（未经同意而发送给接收者的巨量）邮件 252
 - 10.4.2 特洛伊木马 253
 - 10.5 载荷-系统破坏 253
 - 10.5.1 实质破坏 254
 - 10.5.2 逻辑炸弹 254
 - 10.6 载荷-攻击代理-僵尸病毒与机器人 254
 - 10.6.1 机器人的用途 255
 - 10.6.2 远程控制设备 255
 - 10.7 载荷-信息窃取-键盘监测器、网络钓鱼与间谍软件 256
 - 10.7.1 证书窃取、键盘监测器和间谍软件 256
 - 10.7.2 网络钓鱼和身份窃取 256
 - 10.7.3 侦察和间谍 257
 - 10.8 载荷-隐身-后门与隐匿程序 257
 - 10.8.1 后门 257
 - 10.8.2 隐匿程序 258
 - 10.9 防护措施 258
 - 10.9.1 恶意软件防护方法 258
 - 10.9.2 基于主机的扫描器 259
 - 10.9.3 边界扫描方法 261
 - 10.9.4 分布式情报搜集方法 263
 - 10.10 分布式拒绝服务攻击 264

10.10.1 DDoS攻击描述	264
10.10.2 构造攻击网络	266
10.10.3 DDoS防护措施	267
10.11 推荐读物	267
10.12 关键词、思考题和习题	268
10.12.1 关键词	268
10.12.2 思考题	269
10.12.3 习题	269
第11章 入侵者	272
11.1 入侵者	272
11.1.1 入侵者行为模式	273
11.1.2 入侵技术	275
11.2 入侵检测	276
11.2.1 审计记录	278
11.2.2 统计异常检测	279
11.2.3 基于规则的入侵检测	281
11.2.4 基率谬误	283
11.2.5 分布式入侵检测	283
11.2.6 蜜罐	285
11.2.7 入侵检测交换格式	286
11.3 口令管理	288
11.3.1 口令的脆弱性	288
11.3.2 使用散列后的口令	289
11.3.3 用户口令选择	291
11.3.4 口令选择策略	293
11.3.5 Bloom滤波器	295
11.4 推荐读物	296
11.5 关键词、思考题和习题	297
11.5.1 关键词	297
11.5.2 思考题	297
11.5.3 习题	298
第12章 防火墙	301
12.1 防火墙的必要性	301
12.2 防火墙特征	302
12.3 防火墙类型	303
12.3.1 包过滤防火墙	303
12.3.2 状态检测防火墙	306
12.3.3 应用层网关	307
12.3.4 链路层网关	308
12.4 防火墙载体	308
12.4.1 堡垒主机	309
12.4.2 主机防火墙	309
12.4.3 个人防火墙	309
12.5 防火墙的位置和配置	310
12.5.1 停火区网段	310
12.5.2 虚拟私有网	312
12.5.3 分布式防火墙	313
12.5.4 防火墙位置和拓扑结构总结	314
12.6 推荐读物	314
12.7 关键词、思考题和习题	315
12.7.1 关键词	315
12.7.2 思考题	315
12.7.3 习题	315
附录A 一些数论结果	319

A.1 素数和互为素数	319
A.1.1 因子	319
A.1.2 素数	319
A.1.3 互为素数	320
A.2 模运算	320
附录B 网络安全教学项目	322
B.1 研究项目	322
B.2 黑客项目	323
B.3 编程项目	323
B.4 实验训练	324
B.5 实际安全评估	324
B.6 防火墙项目	324
B.7 案例学习	324
B.8 写作作业	325
B.9 阅读/报告作业	325
参考文献	326
• • • • •	(收起)

[网络安全基础 \(第5版\)_下载链接1](#)

标签

计算机

网络安全

网络

教材

WilliamStallings

1

评论

比较好的覆盖了网络安全的诸多概念，对于具体实现的描述也相对清晰，同时包括了一些有用的经验。遗憾的是翻译依旧存在错误，第七第九章略繁琐，而且缺失了对spoofi

ng等的介绍。总的来说可以对网络安全有一个大致的把握，也能够拓展一些思路。

翻译一般。一些专业名词及缩写应该要给出英文全名。书的内容，介绍的都比较基础，都是之前看过的东西了，和期望有些落差

本书比较有价值的部分就是把各种安全通信协议的流程与标准理得很清晰。不过我大一听老师讲此书的时候僵在那不动，大三了再重看这本书依旧僵住，可以说是非常垃圾了。
。

1.存在翻译的很好的国外教材 2.这本书的翻译真是.....严重影响阅读效率

[网络安全基础 \(第5版\) 下载链接1](#)

书评

[网络安全基础 \(第5版\) 下载链接1](#)