

# 网络安全基础



[网络安全基础 下载链接1](#)

著者:斯托林斯

出版者:清华大学出版社

出版时间:2011-1

装帧:

isbn:9787302239161

《网络安全基础:应用与标准(第4版)》由著名作者William Stallings编写,以当今网络安全的实际解决方案为基础,既简明扼要,又全面系统地介绍了网络安全的主要内容,包括基本原理、重要技术、主要方法和重要的工业标准等。全书共包含11章。除第1章引言外,其余各章分为二大部分叙述:第一部分足密码学,重点介绍分组密码、流密码、消息认证码、安全杂凑函数、公钥密码和数字签名等的基本原理、主要方法和重要应用场景等,并简要介绍了几种常用的典型算法,包括DES算法、AES算法、RC4算法和RSA算法等;第二部分足网络安全应用,简要介绍了传输层安全中的SSL/TLS协议、无线局域网安全及WAP协议、电子邮件安全与PGP及S/MIME协议、IP层安全与IPSec协议等。第三部分足系统安全,简要介绍了入侵检测与口令管

理、恶意软件与防火墙等。

《网络安全基础:应用与标准(第4版)》以最新和实用的网络安全知识为主题,采用深入浅出的叙述手法,每章末尾还给出一定的推荐读物和思考练习题。因此,《网络安全基础:应用与标准(第4版)》既足高等学校网络安全基础课程的好教材,也是工程技术人员和网络爱好者了解网络安全基本概貌的好读物。

作者介绍:

## 目录: 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安全体系架构 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 9
  - 1.4.1 认证 10
  - 1.4.2 访问控制 11
  - 1.4.3 数据机密性 11
  - 1.4.4 数据完整性 11
  - 1.4.5 不可抵赖性 11
  - 1.4.6 可用性服务 12
- 1.5 安全机制 12
- 1.6 网络安全模型 13
- 1.7 标准 15
- 1.8 本书概览 15
- 1.9 推荐读物 15
- 1.10 网络资源 16
- 1.11 关键词、思考题和习题 18
  - 1.11.1 关键词 18
  - 1.11.2 思考题 18
  - 1.11.3 习题 19

### 第1部分 密码学

- ### 第2章 对称加密和消息机密性 23
- 2.1 对称加密原理 23
    - 2.1.1 密码体制 24
    - 2.1.2 密码分析 24
    - 2.1.3 Feistel密码结构 26
  - 2.2 对称分组加密算法 28
    - 2.2.1 数据加密标准 28
    - 2.2.2 三重DES 30
    - 2.2.3 高级加密标准 31
  - 2.3 随机数和伪随机数 34
    - 2.3.1 随机数的应用 34
    - 2.3.2 真随机数发生器、伪随机数生成器和伪随机函数 35
    - 2.3.3 算法设计 36
  - 2.4 流密码和RC4 37
    - 2.4.1 流密码结构 37
    - 2.4.2 RC4算法 38

2.5 分组密码工作模式	40
2.5.1 电子密码本模式	40
2.5.2 密码分组链接模式	41
2.5.3 密码反馈模式	42
2.5.4 计数器模式	43
2.6 推荐读物和网址	45
2.7 关键词、思考题和习题	45
2.7.1 关键词	45
2.7.2 思考题	45
2.7.3 习题	46
第3章 公钥加密和消息认证	50
3.1 消息认证方法	50
3.1.1 利用常规加密的消息认证	50
3.1.2 非加密的消息认证	51
3.2 安全散列函数	53
3.2.1 散列函数的要求	54
3.2.2 散列函数的安全性	54
3.2.3 简单散列函数	55
3.2.4 SHA安全散列函数	56
3.3 消息认证码	59
3.3.1 HMAC	59
3.3.2 基于分组密码的MAC	61
3.4 公钥加密原理	63
3.4.1 公钥加密思想	63
3.4.2 公钥密码系统的应用	65
3.4.3 公钥加密的要求	66
3.5 公钥加密算法	66
3.5.1 RSA公钥加密算法	66
3.5.2 Diffie-Hellman密钥交换	69
3.5.3 其他公钥加密算法	71
3.6 数字签名	72
3.7 推荐读物和网址	72
3.8 关键词、思考题和习题	73
3.8.1 关键词	73
3.8.2 思考题	73
3.8.3 习题	74
第2部分 网络安全应用	
第4章 密钥分配和用户认证	81
4.1 基于对称加密的密钥分配	81
4.2 Kerberos	82
4.2.1 Kerberos版本4	83
4.2.2 Kerberos版本5	91
4.3 基于非对称加密的密钥分配	94
4.3.1 公钥证书	95
4.3.2 基于公钥密码的秘密密钥分发	95
4.4 X.509证书	96
4.4.1 证书	97
4.4.2 X.509版本3	101
4.5 公钥基础设施	102
4.5.1 PKIX管理功能	103
4.5.2 PKIX管理协议	104
4.6 联合身份管理	104
4.6.1 身份管理	104
4.6.2 身份联合	106

4.7 推荐读物和网址	109
4.8 关键词、思考题和习题	110
4.8.1 关键词	110
4.8.2 思考题	111
4.8.3 习题	111
第5章 传输层安全	115
5.1 Web安全需求	115
5.1.1 Web安全威胁	116
5.1.2 Web流量安全方法	117
5.2 安全套接字层和传输层安全	117
5.2.1 SSL体系结构	117
5.2.2 SSL记录协议	119
5.2.3 密码变更规格协议	121
5.2.4 报警协议	122
5.2.5 握手协议	122
5.2.6 密码计算	127
5.3 传输层安全	128
5.3.1 版本号	128
5.3.2 消息认证码	128
5.3.3 伪随机函数	129
5.3.4 报警码	130
5.3.5 密码构件	131
5.3.6 客户端证书类型	131
5.3.7 certificate_verify和finished消息	131
5.3.8 密码计算	132
5.3.9 填充	132
5.4 HTTPS	132
5.4.1 连接发起	133
5.4.2 连接关闭	133
5.5 安全盾	133
5.5.1 传输层协议	134
5.5.2 用户身份验证协议	137
5.5.3 连接协议	139
5.6 推荐读物和网址	142
5.7 关键词、思考题和习题	143
5.7.1 关键词	143
5.7.2 思考题	143
5.7.3 习题	143
第6章 无线网络安全	145
6.1 IEEE 802.11无线局域网概述	145
6.1.1 Wi-Fi联盟	146
6.1.2 IEEE 802协议架构	146
6.1.3 IEEE 802.11网络组成与架构模型	148
6.1.4 IEEE 802.11服务	148
6.2 IEEE 802.11i 无线局域网安全	150
6.2.1 IEEE 802.11i服务	151
6.2.2 IEEE 802.11i操作阶段	152
6.2.3 发现阶段	153
6.2.4 认证阶段	154
6.2.5 密钥管理阶段	156
6.2.6 保密数据传输阶段	159
6.2.7 IEEE 802.11i伪随机数函数	160
6.3 无线应用协议概述	161
6.3.1 操作概述	162

6.3.2 无线置标语言	163
6.3.3 WAP的结构	164
6.3.4 无线应用环境	165
6.3.5 WAP协议结构	165
6.4 无线安全传输层	167
6.4.1 WTLS会话和连接	167
6.4.2 WTLS协议结构	168
6.4.3 密码算法	172
6.5 无线应用协议的端到端安全	174
6.6 推荐读物和网址	176
6.7 关键词、思考题和习题	177
6.7.1 关键词	177
6.7.2 思考题	178
6.7.3 习题	178
第7章 电子邮件安全	180
7.1 PGP	180
7.1.1 符号约定	181
7.1.2 操作描述	181
7.1.3 加密密钥和密钥环	185
7.1.4 公钥管理	190
7.2 S/MIME	194
7.2.1 RFC 5322	194
7.2.2 多用途网际邮件扩展	194
7.2.3 S/MIME的功能	199
7.2.4 S/MIME消息	201
7.2.5 S/MIME证书处理过程	204
7.2.6 增强的安全性服务	206
7.3 域名密钥识别邮件	206
7.3.1 互联网邮件体系结构	206
7.3.2 E-mail威胁	208
7.3.3 DKIM策略	209
7.3.4 DKIM的功能流程	210
7.4 推荐读物和网址	211
7.5 关键词、思考题和习题	212
7.5.1 关键词	212
7.5.2 思考题	212
7.5.3 习题	212
附录7A 基-64转换	213
第8章 IP安全	215
8.1 IP安全概述	215
8.1.1 IPsec的应用	216
8.1.2 IPsec的好处	216
8.1.3 路由应用	217
8.1.4 IPsec文档	217
8.1.5 IPsec服务	218
8.1.6 传输模式和隧道模式	218
8.2 IP安全策略	219
8.2.1 安全关联	219
8.2.2 安全关联数据库	220
8.2.3 安全策略数据库	221
8.2.4 IP通信进程	222
8.3 封装安全载荷	224
8.3.1 ESP格式	224
8.3.2 加密和认证算法	225

8.3.3 填充	225
8.3.4 反重放服务	226
8.3.5 传输模式和隧道模式	226
8.4 安全关联组合	230
8.4.1 认证加保密	230
8.4.2 安全关联的基本组合	231
8.5 网络密钥交换	232
8.5.1 密钥确定协议	233
8.5.2 报头和载荷格式	236
8.6 密码组件	239
8.7 推荐读物和网址	240
8.8 关键词、思考题和习题	241
8.8.1 关键词	241
8.8.2 思考题	241
8.8.3 习题	241
第3部分 系统安全	
第9章 入侵者	245
9.1 入侵者简介	245
9.1.1 入侵者行为模式	246
9.1.2 入侵技术	248
9.2 入侵检测	250
9.2.1 审计记录	251
9.2.2 统计异常检测	252
9.2.3 基于规则的入侵检测	255
9.2.4 基率谬误	256
9.2.5 分布式入侵检测	257
9.2.6 蜜罐	258
9.2.7 入侵检测交换格式	259
9.3 口令管理	259
9.3.1 口令保护	259
9.3.2 口令选择策略	263
9.4 推荐读物和网址	267
9.5 关键词、思考题和习题	268
9.5.1 关键词	268
9.5.2 思考题	268
9.5.3 习题	269
附录9A 基率谬误	271
第10章 恶意软件	274
10.1 恶意软件类型	274
10.1.1 后门	275
10.1.2 逻辑炸弹	276
10.1.3 特洛伊木马	276
10.1.4 可移动代码	277
10.1.5 多威胁恶意代码	277
10.2 病毒	278
10.2.1 病毒的本质	278
10.2.2 病毒分类	281
10.2.3 病毒工具包	282
10.2.4 宏病毒	282
10.2.5 电子邮件病毒	283
10.3 病毒对策	283
10.3.1 反病毒方法	283
10.3.2 高级反病毒技术	284
10.3.3 行为阻断软件	286

10.4 蠕虫	287
10.4.1 莫里斯蠕虫	288
10.4.2 蠕虫传播模式	289
10.4.3 近期蠕虫攻击	290
10.4.4 蠕虫病毒技术现状	290
10.4.5 手机蠕虫	291
10.4.6 蠕虫对策	291
10.5 分布式拒绝服务攻击	295
10.5.1 DDoS攻击描述	295
10.5.2 构造攻击网络	297
10.5.3 DDoS防范	298
10.6 推荐读物和网址	299
10.7 关键词、思考题和习题	300
10.7.1 关键词	300
10.7.2 思考题	300
10.7.3 习题	300
第11章 防火墙	303
11.1 防火墙的必要性	303
11.2 防火墙特征	304
11.3 防火墙类型	305
11.3.1 包过滤防火墙	305
11.3.2 状态检测防火墙	309
11.3.3 应用层网关	310
11.3.4 链路层网关	310
11.4 防火墙载体	311
11.4.1 堡垒主机	311
11.4.2 主机防火墙	312
11.4.3 个人防火墙	312
11.5 防火墙的位置和配置	314
11.5.1 停火区网段	314
11.5.2 虚拟私有网	315
11.5.3 分布式防火墙	315
11.5.4 防火墙位置和拓扑结构总结	316
11.6 推荐读物和网址	317
11.7 关键词、思考题和习题	318
11.7.1 关键词	318
11.7.2 思考题	318
11.7.3 习题	319
附录A 一些数论结果	322
A.1 素数和互为素数	322
A.1.1 因子	322
A.1.2 素数	322
A.1.3 互为素数	323
A.2 模运算	324
附录B 网络安全教学项目	326
B.1 研究项目	326
B.2 黑客项目	327
B.3 编程项目	327
B.4 实验训练	328
B.5 实际安全评估	328
B.6 写作作业	328
B.7 阅读与综述作业	328
. . . . . (收起)	

[网络安全基础 下载链接1](#)

## 标签

网络安全

安全

网络

计算机-安全

计算机

信息安全

网络编程

在库

## 评论

没有第5版可以给我标记....

---

其实还是看英文的比较好~ 中文直译的句子逻辑太绕~

---

回头再看，才能理解为什么这书算名著。

## 网络安全基础 下载链接1

## 书评

让人怀疑译者的水平！要么就是太不负责任！

刚刚看到第二章，错误已经不下十处，特别是习题的翻译，简直让我哭笑不得。

这样的书是怎么出版的？建议大家看英文版吧，中文版是没法看下去了。

比如queries本来是指查询，楞是翻译成质疑。

习题2.1中，对一段英文进行加密，居然把...

本来想在读英文原版的时候参考一下翻译，但是很多地方需要自己重新查词，因为翻译离原文的意思相差太远，而且翻译得十分拗口。

如果直接当作教科书看，很多语意是不通顺的。评论到底要多长啊？

作者写过很多书，涉及计算机很多行业，但是都不精通，因此，他的书很适合一般人入门。翻译一般，但也可以看懂。。。。。

网络安全基础 下载链接1