

《信息安全原理与实践（第2版）》

图书基本信息

书名：《信息安全原理与实践（第2版）》

13位ISBN编号：9787302317852

10位ISBN编号：7302317852

出版时间：2013-5

出版社：清华大学出版社

作者：【美】斯坦普(Stamp, M.)

页数：463

译者：张戈

版权说明：本站所提供下载的PDF图书仅提供预览和简介以及在线试读，请支持正版图书。

更多资源请访问：www.tushu111.com

内容概要

面向21世纪的信息安全指南

信息安全是一个快速发展的领域。着眼于最富时代感的安全议题，涵盖涉及宽泛的一系列新鲜信息，这本经过充分更新和全面修订的《信息安全原理与实践(第2版)》为读者提供了解决任何信息安全难题所必备的知识 and 技能。

主要内容

通过聚焦于现实世界中的生动实例，并采用一种面向实践的信息安全讲述方法，这本书围绕如下4个重要主题进行组织并展开：

密码学技术：包括经典密码系统、对称密钥加密技术、公开密钥加密技术、哈希函数、随机数技术、信息隐藏技术以及密码分析技术等。

访问控制：包括身份认证和授权、基于口令的安全、访问控制列表和访问能力列表、多级安全性和分隔项技术、隐藏通道和接口控制、诸如BLP和Biba之类的安全模型、防火墙以及入侵检测系统等。

协议：包括简单身份认证协议、会话密钥、完全正向保密、时间戳技术、SSH协议、SSL协议、IPSec协议、Kerberos协议、WEP协议以及GSM协议等。

软件安全：包括软件缺陷和恶意软件、缓冲区溢出、病毒和蠕虫、恶意软件检测、软件逆向工程、数字版权管理、安全软件开发以及操作系统安全等。

在本书第2版中，特别引入了一些比较新的内容，其中涉及的安全主题包括SSH协议和WEP协议、实际的RSA计时攻击技术、僵尸网络以及安全证书等。同时还增加了一些新的背景知识，包括Enigma密码机以及一部分关于经典“橘皮书”之安全观的内容。此外，本书还有一大特色，就是大幅度地扩展和更新课后思考题，并增补了许多新的图解、表格和图形，用以阐明和澄清一些复杂的主题和问题。最后，对于课程开发来说，还有一组综合性的课堂测试用的PowerPoint幻灯片文件以及问题解答手册可供利用。

作者简介

作者简介

我在信息安全领域已有将近20年的经验了，其中包括在行业中和政府里从事的一些宽泛的工作内容。我的职业经历包括在美国国家安全局(National Security Agency, NSA)的7年多，以及随后在一家硅谷创业公司的两年时间。虽然关于我在NSA的工作，我不能说太多，但是我可以告诉你——我的职业头衔曾经是密码技术数学家。在这个行业当中，我参与设计并开发了一款数字版权管理安全产品。这段现实世界中的工作经历，就像三明治一样被夹在学术性的职业生涯之间。身处学术界时，我的研究兴趣则包含了各式各样广泛的安全主题。

当我于2002年重返学术界时，于我而言，似乎没有一本可用的安全教科书能够与现实世界紧密相连。我觉得我可以撰写一本信息安全方面的书籍，以填补这个空缺，同时还可以在书中包含一些对于处于职业生涯的IT专业人士有所裨益的信息。基于我已经接收到的反馈情况，第1版显然已经获得了成功。我相信，从既是一本教科书，又可作为专业人员的工作参考这个双重角色来看，第2版将会被证明更具价值，但是因此我也会产生一些偏见。可以说，我以前的很多学生如今都从业于一些领先的硅谷科技公司。他们告诉我，在我的课程中学到的知识曾令他们受益匪浅。于是，我当然就会很希望，当我之前在业界工作时也能有一本类似这样的书籍作为参考，那样我的同事们和我就也能够受惠于此了。除了信息安全之外，我当然还有自己的生活。我的家人包括我的妻子Melody，两个很棒的儿子Austin(他的名字首字母是AES)和Miles(感谢Melody，他的名字首字母不至于成为DES)。我们热爱户外运动，定期会在附近做一些短途的旅行，从事一些诸如骑自行车、登山远足、露营以及钓鱼之类的活动。此外，我还花了太多的时间，用在我位于Santa Cruz山间的一座待修缮的房子上。

书籍目录

目录

第1章 引言

1

1.1 角色列表

1

1.2 Alice的网上银行

2

1.2.1 机密性、完整性和可用性

2

1.2.2 CIA并不是全部

3

1.3 关于本书

4

1.3.1 密码学技术

5

1.3.2 访问控制

5

1.3.3 协议

6

1.3.4 软件安全

7

1.4 人的问题

7

1.5 原理和实践

8

1.6 思考题

9

第 部分 加密

第2章 加密基础

17

2.1 引言

17

2.2 何谓“加密”

18

2.3 经典加密

19

2.3.1 简单替换密码

20

2.3.2 简单替换的密码分析

22

2.3.3 安全的定义

23

2.3.4 双换位密码

23

2.3.5 一次性密码本

24

2.3.6 VENONA项目

28	
2.3.7	电报密码本
29	
2.3.8	1876选举密码
31	
2.4	现代加密技术的历史
33	
2.5	加密技术的分类
35	
2.6	密码分析技术的分类
37	
2.7	小结
38	
2.8	思考题
38	
	第3章 对称密钥加密
45	
3.1	引言
45	
3.2	流密码加密
46	
3.2.1	A5/1算法
47	
3.2.2	RC4算法
49	
3.3	分组密码加密
50	
3.3.1	Feistel密码
50	
3.3.2	DES
51	
3.3.3	三重DES
57	
3.3.4	AES
59	
3.3.5	另外三个分组密码 加密算法
61	
3.3.6	TEA算法
62	
3.3.7	分组密码加密模式
63	
3.4	完整性
67	
3.5	小结
69	
3.6	思考题
69	
	第4章 公开密钥加密

77	
4.1 引言	77
4.2 背包加密方案	79
4.3 RSA	82
4.3.1 教科书式的RSA体制 范例	84
4.3.2 重复平方方法	85
4.3.3 加速RSA加密体制	86
4.4 Diffie-Hellman密钥交换 算法	87
4.5 椭圆曲线加密	89
4.5.1 椭圆曲线的数学原理	89
4.5.2 基于椭圆曲线的Diffie-Hellman 密钥交换方案	91
4.5.3 现实中的椭圆曲线加密 案例	92
4.6 公开密钥体制的表示方法	93
4.7 公开密钥加密体制的应用	93
4.7.1 真实世界中的机密性	94
4.7.2 数字签名和不可否认性	94
4.7.3 机密性和不可否认性	95
4.8 公开密钥基础设施	97
4.9 小结	99
4.10 思考题	100
第5章 哈希函数及其他	109
5.1 引言	109
5.2 什么是加密哈希函数	110

5.3 生日问题	111
5.4 生日攻击	113
5.5 非加密哈希	113
5.6 Tiger Hash	115
5.7 HMAC	120
5.8 哈希函数的用途	121
5.8.1 网上竞价	122
5.8.2 垃圾邮件减阻	122
5.9 其他与加密相关的主题	123
5.9.1 秘密共享	124
5.9.2 随机数	127
5.9.3 信息隐藏	129
5.10 小结	133
5.11 思考题	134
第6章 高级密码分析	145
6.1 引言	145
6.2 Enigma密码机分析	146
6.2.1 Enigma密码机	147
6.2.2 Enigma的密钥空间	149
6.2.3 转子	151
6.2.4 对Enigma密码机的攻击	153
6.3 WEP协议中使用的RC4	155
6.3.1 RC4算法	156
6.3.2 RC4密码分析攻击	157

6.3.3 RC4攻击的预防	161
6.4 线性和差分密码分析	161
6.4.1 数据加密标准DES之快速浏览	162
6.4.2 差分密码分析概览	163
6.4.3 线性密码分析概览	165
6.4.4 微小DES	166
6.4.5 针对TDES加密方案的差分密码分析	169
6.4.6 针对TDES加密方案的线性密码分析攻击	173
6.4.7 对分组加密方案设计的提示	175
6.5 格规约和背包加密	176
6.6 RSA计时攻击	182
6.6.1 一个简单的计时攻击	183
6.6.2 Kocher计时攻击	185
6.7 小结	189
6.8 思考题	189
第 部分 访问控制	
第7章 认证	199
7.1 引言	199
7.2 身份认证方法	200
7.3 口令	200
7.3.1 密钥和口令	201
7.3.2 口令的选择	202
7.3.3 通过口令对系统进行攻击	

203	
7.3.4	口令验证
204	
7.3.5	口令破解中的数学分析
205	
7.3.6	其他的口令问题
208	
7.4	生物特征技术
209	
7.4.1	错误的分类
211	
7.4.2	生物特征技术实例
212	
7.4.3	生物特征技术的错误率
216	
7.4.4	生物特征技术总结
216	
7.5	你具有的身份证明
217	
7.6	双因素认证
218	
7.7	单点登录和Web cookie
218	
7.8	小结
219	
7.9	思考题
220	
	第8章 授权
229	
8.1	引言
229	
8.2	授权技术发展史简介
230	
8.2.1	橘皮书
230	
8.2.2	通用准则
233	
8.3	访问控制矩阵
234	
8.3.1	访问控制列表和访问能力列表
234	
8.3.2	混淆代理人
236	
8.4	多级安全模型
237	
8.4.1	Bell-LaPadula模型
238	
8.4.2	Biba模型

240	
8.5 分隔项(compartment)	
241	
8.6 隐藏通道	
242	
8.7 推理控制	
244	
8.8 CAPTCHA	
245	
8.9 防火墙	
247	
8.9.1 包过滤防火墙	
248	
8.9.2 基于状态检测的包过滤 防火墙	
250	
8.9.3 应用代理	
250	
8.9.4 个人防火墙	
252	
8.9.5 深度防御	
252	
8.10 入侵检测系统	
253	
8.10.1 基于特征的入侵检测 系统	
254	
8.10.2 基于异常的入侵检测 系统	
255	
8.11 小结	
259	
8.12 思考题	
259	
第 部分 协议	
第9章 简单认证协议	
269	
9.1 引言	
269	
9.2 简单安全协议	
270	
9.3 认证协议	
272	
9.3.1 利用对称密钥进行认证	
275	
9.3.2 利用公开密钥进行认证	
278	
9.3.3 会话密钥	
279	

9.3.4 完全正向保密(Perfect Forward Secrecy)

281

9.3.5 相互认证、会话密钥以及PFS

283

9.3.6 时间戳

283

9.4 身份认证和TCP协议

285

9.5 零知识证明

287

9.6 最佳认证协议

291

9.7 小结

291

9.8 思考题

291

第10章 真实世界中的安全协议

301

10.1 引言

301

10.2 SSH

302

10.3 SSL

303

10.3.1 SSL协议和中间人攻击

305

10.3.2 SSL连接

306

10.3.3 SSL和IPSec

307

10.4 IPSec

308

10.4.1 IKE阶段一：数字签名方式

310

10.4.2 IKE阶段一：对称密钥方式

312

10.4.3 IKE阶段一：公开密钥加密方式

313

10.4.4 IPSec cookie

314

10.4.5 IKE阶段一小结

315

10.4.6 IKE阶段二

315	
10.4.7	IPSec和IP数据报
316	
10.4.8	运输和隧道方式
317	
10.4.9	ESP和AH
318	
10.5	Kerberos
320	
10.5.1	Kerberos化的登录
321	
10.5.2	Kerberos中的票据
322	
10.5.3	Kerberos的安全性
323	
10.6	WEP
324	
10.6.1	WEP协议的认证
324	
10.6.2	WEP协议的加密
325	
10.6.3	WEP协议的不完整性
326	
10.6.4	WEP协议的其他问题
326	
10.6.5	实践中的WEP协议
327	
10.7	GSM
328	
10.7.1	GSM体系架构
328	
10.7.2	GSM安全架构
330	
10.7.3	GSM认证协议
332	
10.7.4	GSM安全缺陷
332	
10.7.5	GSM安全小结
335	
10.7.6	3GPP
335	
10.8	小结
336	
10.9	思考题
336	
	第 部分 软件
	第11章 软件缺陷和恶意软件

347	
11.1 引言	347
11.2 软件缺陷	348
11.2.1 缓冲区溢出	350
11.2.2 不完全仲裁	360
11.2.3 竞态条件	361
11.3 恶意软件	362
11.3.1 Brain病毒	364
11.3.2 莫里斯蠕虫病毒	364
11.3.3 红色代码病毒	366
11.3.4 SQL Slammer蠕虫	366
11.3.5 特洛伊木马示例	367
11.3.6 恶意软件检测	368
11.3.7 恶意软件的未来	370
11.3.8 计算机病毒和生物学病毒	372
11.4 僵尸网络	373
11.5 基于软件的各式攻击	374
11.5.1 腊肠攻击	374
11.5.2 线性攻击	375
11.5.3 定时炸弹	376
11.5.4 软件信任	376
11.6 小结	377
11.7 思考题	378
第12章 软件中的安全	387
12.1 引言	

387	
12.2	软件逆向工程
388	
12.2.1	Java字节码逆向工程
390	
12.2.2	SRE示例
391	
12.2.3	防反汇编技术
395	
12.2.4	反调试技术
396	
12.2.5	软件防篡改
397	
12.2.6	变形2.0
398	
12.3	数字版权管理
399	
12.3.1	何谓DRM
399	
12.3.2	一个真实世界中的DRM系统
403	
12.3.3	用于流媒体保护的DRM
405	
12.3.4	P2P应用中的DRM
407	
12.3.5	企业DRM
408	
12.3.6	DRM的败绩
409	
12.3.7	DRM小结
409	
12.4	软件开发
410	
12.4.1	开源软件和闭源软件
411	
12.4.2	寻找缺陷
413	
12.4.3	软件开发相关的其他问题
414	
12.5	小结
417	
12.6	思考题
418	
	第13章 操作系统和安全

427	
13.1 引言	427
13.2 操作系统的安全功能	427
13.2.1 隔离控制	428
13.2.2 内存保护	428
13.2.3 访问控制	430
13.3 可信操作系统	430
13.3.1 MAC、DAC以及其他	431
13.3.2 可信路径	432
13.3.3 可信计算基	433
13.4 下一代安全计算基	435
13.4.1 NGSCB特性组	436
13.4.2 引人入胜的NGSCB应用	438
13.4.3 关于NGSCB的非议	438
13.5 小结	440
13.6 思考题	440
附录	445
参考文献	463

精彩书评

1、有些信息安全的教科书会堆砌大块干燥乏味且一无是处的理论说辞。任何一本这样的著作，读来都会像研读一本微积分教材那般充满刺激和挑战。另外的一些读本所提供的内容，则看起来就像是一种对于信息的随机性收集，而其中的信息却是显然毫不相干的事实罗列。这就会给人们留下一种印象，安全实际上根本不是一个有机结合的主题。而这本书则是着眼于对实践问题的研究，同时尽量覆盖了足够多的基本原理，以备可以在这个领域中展开更深入的研究。并且也力争尽可能地最小化所需要的背景知识。特别是，对于数学形式的表达，已经控制到了最低限度。

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:www.tushu111.com