电子信息科技专著出版专项资金资助出版

信息安全管理手册（卷Ⅱ）

（第四版）

Information Security Management Handbook(Volume Ⅱ)
Fourth Edition

[美] Harold F.Tipton　Micki Krause　主编
王顺满　陶然　杨鼎才　郭守刚　等译
王越　主审

電子工業出版社
Publishing House of Electronics Industry
北京·BEIJING

内 容 简 介

信息安全管理技术是当今通信与计算机界的一个热门话题。本书主要从人、网络以及信息系统的运行环境等几个方面对基于 TCP/IP 协议的信息系统安全问题进行讲述，从系统的角度探究信息安全领域的相关问题，具有极强的可读性。

随着信息安全问题变得越来越复杂，拥有 CISSP 证书的人也越来越受到企业的欢迎。本书可作为应考 CISSP 的首选参考教材，也可作为信息安全专业人员、研究人员的参考手册。本书结构紧凑、内容全面、深入浅出，强调理论与实践的结合。书中包括了 CISSP 考试要求的大部分内容，读者可以根据自己需要去单独学习其中的章节。

图书在版编目(CIP)数据

信息安全管理手册. 2 卷：第 4 版/（美）泰普顿（Tipton, H.F.），（美）克劳斯（Krause, M.）主编；王顺满，陶然，杨鼎才等译. —北京：电子工业出版社，2004.1
ISBN 7-5053-9403-7

Ⅰ.信…　Ⅱ.①泰…　②克…　③王…　④陶…　⑤杨…　Ⅲ.信息系统-安全管理-技术手册　Ⅳ.TP309-62

中国版本图书馆 CIP 数据核字（2003）第 108521 号

责任编辑：许　楷
印　　刷：
出版发行：电子工业出版社
　　北京市海淀区万寿路 173 信箱　邮编　100036
经　　销：各地新华书店
开　　本：1/16　印张：　字数：　千字
印　　次：2004 年 1 月第 1 次印刷
印　　数：　　册　　定　价：0.00 元

凡购买电子工业出版社的图书，如有缺损问题，请向购买书店调换。若书店售缺，请与本社发行部联系。联系电话：（010）68279077。质量投诉请发邮件至 zlts@phei.com.cn，盗版侵权举报请发邮件至 dbqq@phei.com.cn。

译 者 的 话

如今，人类已经进入信息社会，日常生活与工作都离不开信息的交流，而信息在为我们带来巨大方便的同时也相应地带来信息传输和存储过程中所遇到的安全问题。信息系统安全是比计算机安全更为广泛的一个概念，它涵盖了与信息有关的所有领域。

本书译自 Harold F. Tipton 与 Micki Krause 主编的 *Information Security Management* 一书。该书为我们详细阐述了在信息安全管理领域中所用到的新技术、新概念等问题。

本书共分 9 篇：

第 1 篇（第 1～2 章）——**存取控制系统与存取控制机制**：主要讲述了用于实现访问控制功能的系统和方法。

第 2 篇（第 3～8 章）——**通信与网络安全**：分别就网络安全以及因特网（Internet）、内联网（Intranet）与外联网（Extranet）安全两个部分来进行阐述。

第 3 篇（第 9～11 章）——**安全管理问题**：分别就对信息安全问题的认识，安全政策、安全标准、操作步骤和指导方针以及对安全风险管理等三方面进行讲述。

第 4 篇（第 12～16 章）——**应用与系统开发的安全**：分别就信息系统应用安全和信息系统开发中的安全问题进行讲述。

第 5 篇（第 17～20 章）——**密码学**：着重讲述密码学技术及其密码学应用。

第 6 篇（第 21 章）——**结构安全和模式安全**。

第 7 篇（第 22~23 章）——**计算机操作方面的安全问题**。

第 8 篇（第 24 章）——**商业过程中的连续性计划以及灾难恢复计划**。

第 9 篇（第 25～28 章）——**法律、调查和伦理**。

本书由王顺满主持翻译，陶然教授、杨鼎才副教授、郭守刚副研究员、任大伟工程师、魏本杰讲师负责对本书部分初稿的翻译工作，另外参加本书翻译工作的人员还有郎志海、王占禄、卢凤珍、许文权、姬桂霞、李硕、王顺捷、许楠、张阁、王顺成、高巍、王和法、张颖、马涛、刘颖、李娜、王红玉、杜湄楠、李鹏飞等，感谢这些同志在翻译过程中认真负责的工作态度，他们的工作为本书的顺利翻译起到了至关重要的作用。全书由王顺满进行统稿，并对原书中的一些错误进行了修正。

在该书的最后统稿阶段，正赶上北京的“非典”肆虐流行，这次突发疾病的快速流行和蔓延再次为人类敲响警钟！提醒人类只有掌握更多的科学和技术才能够在与自然界和谐生存的世界里，更好地完成从必然王国到自由王国的转变，同时也更加坚定了作者本人克服任何前进中的困难，并最终取得胜利的坚定信心。

本书的翻译工作得到了本人的博士生导师，中国科学院院士、中国工程院院士，北京理工大学名誉校长王越教授的大力支持和指导；同时，在本书的翻译过程中，还得到电子工业出版社竺南直博士的热情鼓励和悉心帮助；其他友人也为本书的顺利完成给予了很大关怀。在此向上述所有给予我帮助的同志、朋友表示衷心的感谢！

另外，我还要感谢我的父母和家人，他们无私和坚定的支持是我不断前进的坚强后盾和

动力源泉；我还要特别感谢我的妻子，她对我的工作和生活给予了很大帮助，并为本书的顺利编写提供了许多宝贵的意见和建议。

虽然译者对网络知识有比较深入的研究，并且在信息安全领域发表过多篇论文，但由于时间仓促、知识水平有限，书中也一定有许多不妥之处，敬请各位读者及时批评指正。

王顺满

2003 年 5 月于北京

原 文 序 言

当今世界，信息技术正在以前所未有的速度向前发展，随之而来的信息安全问题也日益受到人们的关注，这就为信息安全专家不断提出新的挑战。为了满足读者的需求，我们在 *Information Security Management Handbook (Fourth Edition)* 一书中，主要讲述了在信息安全领域中的技术发展趋势、新概念以及随之不断进步的信息安全技术等。按照这一理念，我们把这本书定位在供信息安全专家使用的参考书,同时也可供从事网络与系统管理的人员参考。

在这里，我们将继续使本手册的内容与信息安全通用知识（CBK）的内容尽量保持一致，使本书能够成为信息安全专家们参加信息系统安全职业证书考试（CISSP）所使用的复习参考资料。CISSP 认证考试与 CBK 论坛都受到国际信息系统安全认证联盟（ISC）很大程度上的支持，是全球性公认的，并且已经得到业内人士的高度重视。

在准备 CISSP 认证考试的时候，需要考生们花费很大精力来准备。因为该考试不仅需要对 CBK 知识有很好的理解，同时还需要考生们掌握相当的实际应用技巧。这套手册将作为准备 CISSP 认证考试的考生们所使用的几本非常有价值的参考书之一，特别是其中某些章节的内容是由专门从事这方面考试研究的人员所撰写的，这些内容将具有极高的参考价值。另外，在这本书中还包含有许多实际操作方面的知识，因此该书也非常适合于那些从事实际工作的专家参考。

此外，面对计算机病毒和“蠕虫”病毒的肆虐以及网络黑客们对开放网络协议的恶意攻击等严峻情况，作为公司的首席执行官，他们迫切地需要对本公司的内部重要信息资源进行有力保护，于是就需要雇用大量富有相关经验的信息安全管理人员来对信息进行保护。在这种情况下,是否通过 CISSP 认证考试就被当做公司招聘信息安全管理人员时的首要考虑因素。

在这本以及以后各版本的手册中，我们基本上都是按照 CISSP 认证考试的内容来进行编排的。信息安全领域的研究范围非常广泛，在本手册的部分章节中还对 CBK 的题目给出了专门介绍。另外，在写这本 *Information Security Management Handbook (Fourth Edition)*的时候，我们还在书中提到了在信息安全领域出现的一些新情况和新问题，这样做的目的是为了能够与当前该领域内所讨论和研究的新问题保持同步。

Harold F. Tipton
Micki Krause

目　　录

第 1 篇　存取控制系统与存取控制机制

第 1 章　单点登录 …… (3)
1.1　发展过程 …… (3)
1.2　什么是单点登录 …… (5)
1.3　一些基本问题 …… (6)
1.4　工作机制 …… (7)
1.4.1　单点登录技术能为我们提供什么 …… (8)
1.4.2　本质属性 …… (9)
1.4.3　普遍特征 …… (9)
1.4.4　终端管理工具 …… (10)
1.4.5　应用管理设备 …… (10)
1.4.6　终端管理设备 …… (11)
1.4.7　对移动用户的支持 …… (11)
1.4.8　认证 …… (12)
1.4.9　加密 …… (13)
1.4.10　存取控制 …… (13)
1.4.11　应用控制 …… (15)
1.4.12　管理 …… (16)
1.4.13　对于桌面应用的服务 …… (16)
1.4.14　可靠性与性能 …… (17)
1.5　要求 …… (18)
1.5.1　要求的目标 …… (18)
1.5.2　基本要求 …… (18)
1.5.3　假设条件 …… (18)
1.5.4　安全管理 …… (18)
1.5.5　认证和授权 …… (20)
1.5.6　存取控制 …… (22)
1.5.7　数据的完整性/可靠性/加密 …… (22)
1.6　结论 …… (23)
第 2 章　中心认证服务系统 …… (25)
2.1　AAA 服务的主要特征 …… (26)
2.2　远程拨入用户的鉴别服务（RADIUS） …… (27)
2.2.1　把 AA 标准加入到远程拨入用户的鉴别服务：鉴别和授权 …… (27)
2.2.2　第三个 A（计费）：是一个可选项 …… (28)

2.2.3 进一步的思考以及其他相关性能 (28)
2.2.4 最简单的方法 (29)
2.2.5 绊脚石：复杂性与远程拨入用户的鉴别服务在其他方面的局限 (31)
2.3 终端存取控制器与存取控制系统（TACACS） (31)
2.3.1 TACACS 的认证功能 (32)
2.3.2 TACACS 的授权功能 (32)
2.3.3 TACACS 的记录功能 (32)
2.3.4 其他处理优势 (33)
2.3.5 Cisco：应用 TACACS (33)
2.3.6 TACACS 的局限性 (36)
2.4 DIAMETER：两次远程拨入用户的鉴别服务 (36)
2.4.1 任何事情都需要一个好的基础 (37)
2.4.2 进行认证所采用的方式 (37)
2.4.3 代理功能 (37)
2.4.4 DIAMETER 的授权功能 (38)
2.4.5 对任何事件都进行统计 (38)
2.4.6 安全、标准以及其他问题 (39)

第 2 篇　通信与网络安全

第 3 章　电子邮件安全问题 (43)
3.1 电子邮件服务的类型 (46)
3.1.1 Sendmail (46)
3.1.2 保护电子邮件 (47)
3.2 对电子邮件参与者进行认证 (48)
3.2.1 电子邮件的网络结构 (49)
3.2.2 功能不完善的电子邮件网关 (49)
3.3 电子邮件系统的工作原理 (51)
3.3.1 IP 数据流的控制 (51)
3.3.2 TCP/IP 的五层结构 (52)
3.3.3 多用途的网际邮件扩充协议（MIME） (52)
3.3.4 因特网信息存取协议 (54)
3.3.5 邮局协议 (54)
3.3.6 加密与认证 (56)
3.3.7 加密 (57)
3.3.8 数字认证 (58)
3.3.9 安全套接层（SSL） (60)
3.3.10 安全电子邮件的实现方法 (60)
3.3.11 电子邮件传送的安全问题 (61)
3.4 结论 (63)

第 4 章　ATM 技术的完整性与安全性 …… (65)
4.1　ATM 的商业应用：计算机与网络 …… (65)
4.1.1　个人计算机（PC）的桌面环境 …… (65)
4.1.2　局域网与广域网 …… (66)
4.2　ATM 在商业领域中的应用：远程通信 …… (66)
4.3　ATM 技术的特点与功能组件 …… (67)
4.3.1　B-ISDN 传输网络 …… (67)
4.3.2　实际路径与虚拟路径 …… (68)
4.3.3　信道的格式 …… (68)
4.3.4　适配层 …… (68)
4.3.5　STM 与 ATM 的比较 …… (69)
4.4　宽带信号传输网络 …… (69)
4.4.1　ATM 在宽带信息发送系统中的作用 …… (70)
4.4.2　ATM 信令系统 …… (70)
4.5　ATM 网络的流量管理 …… (71)
4.5.1　功能和目标 …… (71)
4.5.2　ATM 网络的数据流控制 …… (72)
4.5.3　ATM 网络的拥塞控制 …… (74)
4.5.4　ATM 网络的恢复控制 …… (75)
4.6　结论 …… (76)
第 5 章　安全的远程接入系统介绍 …… (77)
5.1　远程接入的安全目标 …… (78)
5.1.1　对远端用户和主机的可靠性认证 …… (78)
5.1.2　高级存取控制方法 …… (79)
5.1.3　对重要数据的保护 …… (79)
5.1.4　网络使用的日志和审计功能 …… (79)
5.1.5　工作环境的透明复制 …… (80)
5.1.6　对远端用户和工作地点的连接 …… (80)
5.1.7　减少费用 …… (81)
5.2　远程接入的工作机理 …… (82)
5.3　虚拟专用网（VPN） …… (85)
5.4　选择一个远程端接入系统 …… (86)
5.5　远程接入策略 …… (87)
第 6 章　数据报的嗅探以及对网络的监视 …… (91)
6.1　嗅探器（Sniffer）的基本特点 …… (91)
6.1.1　拓扑、媒体及其位置关系 …… (92)
6.1.2　嗅探器是如何工作的 …… (93)
6.3　安全考虑 …… (97)
6.4　CIA …… (98)

6.4.1 攻击方法 …… (99)
6.4.2 攻击类型 …… (101)
6.5 对嗅探的防范措施 …… (104)
6.5.1 安全政策 …… (104)
6.5.2 强认证方案 …… (105)
6.5.3 加密技术 …… (105)
6.5.4 交换网络环境 …… (106)
6.5.5 检测嗅探器 …… (106)
6.6 实现嗅探功能的工具 …… (107)
6.6.1 操作工具 …… (108)
6.6.2 网络专用攻击工具 …… (110)
6.7 结论 …… (112)
第 7 章 封装技术：把企业网当成一个外域网 …… (113)
7.1 安全文本 …… (114)
7.2 一个非常有名的网络格言 …… (115)
7.3 网络安全与一个有名的网络格言 …… (115)
7.4 因特网安全结构元素 …… (116)
7.5 封装方法 …… (117)
7.6 被封装的部分 …… (117)
7.7 网络监控工具 …… (118)
7.8 采取封装技术所带来的好处 …… (119)
7.9 封装技术的局限性 …… (119)
7.10 封装技术的应用 …… (120)
7.11 信息收集 …… (120)
7.12 规划 …… (120)
7.13 最初模型 …… (121)
7.14 应用 …… (121)
7.15 完善 …… (122)
7.16 结论 …… (123)
第 8 章 IPSec 虚拟专用网 …… (125)
8.1 发展史 …… (125)
8.2 建立标准的不同模块 …… (126)
8.3 虚拟专用网的功能介绍 …… (127)
8.4 基础知识 …… (128)
8.5 通信模式 …… (129)
8.5.1 传输模式 …… (129)
8.5.2 隧道模式 …… (130)
8.6 对数据的保护和验证 …… (130)
8.6.1 鉴别和完整性 …… (131)

8.6.2 保密和加密 …… (131)
8.7 对连接所进行的管理 …… (131)
8.8 VPN（虚拟专用网）的组建 …… (133)
8.9 跟踪 …… (134)
8.9.1 通信规则 …… (134)
8.9.2 对安全关联的控制 …… (136)
8.10 提供多层安全数据流 …… (136)
8.11 密钥问题 …… (137)
8.12 密钥发展史 …… (137)
8.13 IPSec 网络密钥交换 …… (138)
8.14 阶段和模式 …… (139)
8.15 系统信任的建立 …… (139)
8.16 密钥共享 …… (140)
8.17 单一密钥体系 …… (140)
8.17.1 对称密钥 …… (140)
8.17.2 多密钥 …… (142)
8.18 密钥的建立 …… (143)
8.18.1 手动分配密钥方式 …… (143)
8.18.2 自动分配密钥方式 …… (143)
8.19 转换主流技术 …… (144)
8.19.1 性能 …… (144)
8.19.2 互操作性 …… (145)
8.19.3 可扩展性 …… (145)
8.20 VPN 的市场 …… (146)
8.20.1 远程访问 …… (146)
8.20.2 外围网络的访问 …… (147)
8.20.3 对内部网络的保护 …… (148)
8.21 在实现 VPN 时应该考虑到的问题 …… (148)
8.21.1 系统需求 …… (148)
8.21.2 安全策略 …… (148)
8.21.3 应用性能 …… (149)
8.21.4 培训 …… (149)
8.22 对 IPSec VPN 的展望 …… (149)
8.23 结论 …… (151)

第 3 篇　安全管理问题

第 9 章　穿透性测试 …… (155)
9.1 什么是穿透性测试 …… (155)
9.2 术语 …… (156)

9.3 为什么要进行测试 …… (157)
9.4 穿透性测试的类型 …… (158)
9.5 穿透性测试工作的条件 …… (159)
9.6 基本攻击策略 …… (161)
9.7 规划测试过程 …… (163)
9.8 执行测试 …… (164)
9.9 报告测试结果 …… (167)
9.10 结论 …… (168)
第 10 章 构建信息安全技术的模块 …… (169)
10.1 安全理念 …… (173)
10.1.1 投入产出比（ROI）：什么是安全理念的基础 …… (173)
10.1.2 例子 …… (173)
10.2 原因 …… (174)
10.3 安全管理的神话 …… (174)
10.3.1 安全技术可以解决所有问题 …… (174)
10.3.2 我已经制定出安全政策，现在就可以完成所有安全任务 …… (175)
10.3.3 公布信息安全政策和标准之后，所有人就都会遵从该安全政策和标准 …… (175)
10.3.4 完全遵循信息安全产品供应商所提供的方法：这是保证组织信息安全的最好方法 (176)
10.4 构建安全桥梁：信息安全控制要符合组织的商业需要 …… (176)
10.5 解决商业需要 …… (177)
10.6 铺设路基：安全政策和标准 …… (177)
10.7 看门人：技术 …… (178)
10.8 提供传输：传播 …… (179)
10.9 专家与傻瓜：执行推荐标准 …… (179)
10.9.1 专家：执行推荐 …… (180)
10.9.2 分层安全 …… (180)
10.9.3 功能标准 …… (182)
10.9.4 使用计算机政策 …… (182)
10.9.5 安全底线 …… (182)
10.9.6 技术和物理安全 …… (182)
10.9.7 操作步骤和指导方针 …… (182)
10.10 警察来了 …… (183)
第 11 章 信息安全领域中的商业问题：通过管理手段向需要保护的重要机密信息和产品进行安全防护 …… (185)
11.1 信息安全现状 …… (185)
11.2 高级管理人员对信息安全的态度 …… (186)
11.3 高层管理者的信息安全观点 …… (187)
11.4 信息安全技术所能起到的积极作用 …… (187)
11.5 将信息安全研究与应用当成一个产业来看待 …… (189)

11.6 迎接信息安全的挑战 (189)
11.7 结论 (190)

第 4 篇 应用与系统开发的安全

第 12 章 PeopleSoft 软件的安全性 (195)
12.1 网络的安全性 (196)
12.2 数据库管理系统的安全性 (196)
12.3 操作系统的安全性 (197)
12.4 PeopleSoft 应用程序的安全性 (197)
12.4.1 用户登录的安全性（Sign-on Security） (198)
12.4.2 控制台安全性（Panel Security） (199)
12.4.3 访问安全性（Query Security） (202)
12.4.4 水平安全性（Row-level security） (204)
12.5 结论 (207)
第 13 章 万维网应用的安全 (209)
13.1 网络应用的历史：进行控制的必要性 (209)
13.2 网络应用安全如何满足因特网的整体安全策略 (210)
13.2.1 整体简短的描述 (210)
13.2.2 认证 (211)
13.3 为什么要为网络采用认证/访问控制结构 (211)
13.4 项目概要 (212)
13.5 项目规划与初始阶段 (213)
13.5.1 项目的组成 (213)
13.5.2 角色和责任 (214)
13.6 要求 (214)
13.6.1 定义商业要求 (214)
13.6.2 定义技术要求 (215)
13.6.3 风险评估 (216)
13.6.4 优先权和选择准则 (217)
13.7 产品基础结构的选择策略 (217)
13.8 设计 (219)
13.8.1 服务器基础结构 (219)
13.8.2 网络 (220)
13.8.3 目录服务 (220)
13.8.4 开发环境 (221)
13.8.5 管理责任 (221)
13.9 测试 (222)
13.10 结论 (223)
第 14 章 常见系统设计缺陷和安全问题 (225)

14.1 不可执行的限制 (226)
14.2 复杂性 (226)
14.3 不完全参数检查与执行 (227)
14.4 不完全错误处理 (228)
14.5 对使用时间的检查 (228)
14.6 无效的约束 (229)
14.7 复杂的控制方式 (229)
14.8 不必要的功能 (230)
14.9 逃避机制 (230)
14.10 过多的权力 (232)
14.11 特殊权限的失效 (232)
14.12 不安全的默认值设置 (233)
14.13 对应用程序控制方法的绝对信任 (233)
14.14 建议 (234)
第 15 章 数据中心和数据仓库 (235)
15.1 什么是数据中心和数据仓库 (235)
15.1.1 数据仓库与数据中心之间的主要差别 (235)
15.1.2 数据仓库与数据中心的相同点 (236)
15.2 数据质量 (238)
15.2.1 在 DW 设计中加入元数据 (238)
15.2.2 元数据模型的标准化 (238)
15.2.3 设置用户对数据质量的期望 (238)
15.3 数据仓库的使用 (239)
15.3.1 用户的类型 (239)
15.3.2 应用的技巧 (240)
15.3.3 结果 (242)
15.4 对数据仓库的投资收益 (242)
15.4.1 成本 (242)
15.4.2 投资收益 (243)
15.5 对成功的衡量 (243)
15.6 要避免的错误 (244)
15.7 数据仓库的实现过程 (246)
15.7.1 通常需要考虑的问题 (246)
15.7.2 对数据仓库运行是否成功的定性衡量 (246)
15.8 数据仓库的安全问题 (247)
15.8.1 DW 设计的检查 (248)
15.8.2 数据仓库的安全性检查 (251)
15.8.3 数据仓库的运行过程 (252)
15.8.4 对数据仓库的维护 (253)

15.8.5 对数据仓库的完善 …… (253)
15.9 结论 …… (254)
第 16 章 减轻电子商务操作过程中的安全风险：公用基础设施在现实世界中的应用 …… (255)
16.1 网络安全：存在的问题 …… (255)
16.2 为什么在电子商务中采用密码技术是有用的 …… (257)
16.3 使用 PKI 技术来对应用进行认证 …… (260)
16.4 PKI 的组成 …… (263)
16.5 使用 PKI 带来的其他方面的好处：减少注册次数 …… (265)
16.6 PKI 的操作 …… (267)
16.7 实现 PKI 操作 …… (269)
16.8 结论 …… (271)

第 5 篇 密码学

第 17 章 密码学概论 …… (275)
17.1 加密技术是怎样失败的 …… (275)
17.2 对加密技术的攻击 …… (275)
17.3 密钥的泄露 …… (276)
17.4 建立可靠的加密系统是很难实现的 …… (277)
17.4.1 加解密算法发展史 …… (277)
17.4.2 实现过程 …… (278)
17.4.3 应用过程中的问题 …… (278)
17.4.4 操作过程中的问题 …… (278)
17.5 加密的类型 …… (279)
17.5.1 对称加密算法 …… (279)
17.5.2 非对称（公钥）加密算法 …… (279)
17.5.3 其他加密算法 …… (280)
17.6 加密服务 …… (282)
17.6.1 在商业交易过程中所起到的作用（可以当做目击证人） …… (284)
17.6.2 密钥恢复 …… (285)
17.7 密码学应用 …… (285)
17.8 结论 …… (288)
第 18 章 密码学应用的三种新模型 …… (289)
18.1 介绍 …… (289)
18.2 商业分析 …… (290)
18.3 接收模型 …… (291)
18.4 网络分层模型 …… (293)
18.5 拓扑模型 …… (296)
18.6 信息状态模型 …… (298)
18.7 模型的应用 …… (300)

第 19 章　加密系统的攻击和防御 …… (301)
19.1　密码学概述 …… (301)
19.2　密码类型 …… (302)
19.2.1　替代密码 …… (302)
19.2.2　一次一密型的密码体系 …… (303)
19.2.3　置换密码 …… (303)
19.2.4　序列密码 …… (303)
19.2.5　分组密码 …… (303)
19.3　密钥类型 …… (304)
19.4　对称密钥密码学 …… (304)
19.5　非对称密钥密码学 …… (304)
19.6　散列函数 …… (305)
19.6.1　MD5 …… (305)
19.6.2　SHA …… (305)
19.7　隐写术 …… (305)
19.8　密钥分配 …… (305)
19.9　密钥管理 …… (306)
19.10　公开的和专有的算法和系统 …… (306)
19.11　典型的攻击类型 …… (306)
19.12　标准密码分析方法 …… (306)
19.12.1　反向推断 …… (307)
19.12.2　推测 …… (307)
19.12.3　频率分析 …… (307)
19.12.4　穷尽攻击 …… (307)
19.12.5　惟密文攻击 …… (308)
19.12.6　已知明文攻击 …… (308)
19.12.7　选择明文攻击 …… (308)
19.12.8　生日攻击 …… (308)
19.12.9　拆分攻击 …… (308)
19.12.10　重放攻击 …… (308)
19.12.11　中间人攻击 …… (308)
19.12.12　字典攻击 …… (309)
19.12.13　随机数生成器攻击 …… (309)
19.12.14　推理 …… (309)
19.13　现代攻击 …… (310)
19.13.1　旁路攻击 …… (310)
19.13.2　操作系统缺陷 …… (311)
19.13.3　驻留内存 …… (311)
19.13.4　临时文件 …… (311)

19.13.5 差分电源分析 …… (311)
19.13.6 并行计算 …… (311)
19.13.7 分布式计算 …… (312)
19.13.8 破解 DES 算法 …… (312)
19.13.9 RSA-155（512 比特）分解法 …… (313)
19.14 快速 RSA 破解器 …… (313)
19.15 密码保护系统 …… (314)
19.15.1 设计、分析和测试 …… (314)
19.15.2 选择合适的密钥长度 …… (314)
19.15.3 随机数生成器 …… (315)
19.15.4 源代码审查 …… (315)
19.15.5 供应商的安全保证 …… (315)
19.15.6 高级加密算法 …… (316)
19.16 结论 …… (316)
第 20 章 对信息的认证过程 …… (317)
20.1 对信息进行认证的技术发展史 …… (317)
20.2 为什么要对信息进行认证 …… (318)
20.3 技术回顾 …… (318)
20.3.1 散列函数 …… (318)
20.3.2 加密 …… (319)
20.3.3 消息认证码 …… (323)
20.4 对信息进行认证的必要性 …… (324)
20.4.1 伪装 …… (324)
20.4.2 内容篡改 …… (324)
20.4.3 序列更改 …… (325)
20.4.4 传输过程更改 …… (325)
20.5 认证操作的基础 …… (325)
20.5.1 加密 …… (325)
20.5.2 消息摘要 …… (325)
20.5.3 消息认证码 …… (326)
20.6 散列处理的处理过程 …… (326)
20.7 消息认证码以及操作过程 …… (327)
20.7.1 基于分组的加密模式 …… (327)
20.7.2 基于散列函数的模式 …… (328)
20.7.3 基于流密码加密的模式 …… (329)
20.7.4 无条件保密模式 …… (330)
20.8 在加密过程中对信息进行的认证操作 …… (330)
20.8.1 速度问题 …… (330)
20.8.2 有限的约束条件 …… (330)

20.8.3 应用问题 …… (330)
20.8.4 系统操作 …… (331)
20.8.5 校验和编码 …… (331)
20.8.6 对现有资源的利用 …… (332)
20.9 安全问题考虑 …… (332)
20.10 结论 …… (333)

第 6 篇 结构安全和模式安全

第 21 章 UNIX 操作系统的安全性分析 …… (337)
21.1 操作系统的安全性服务 …… (337)
21.2 认证和鉴别 …… (338)
21.3 访问控制 …… (339)
21.4 可用性和完整性 …… (340)
21.5 审计 …… (341)
21.6 用户如何实施安全性要求 …… (341)
21.7 其他方面的问题 …… (342)
21.7.1 传统 UNIX 操作系统的安全脆弱性 …… (342)
21.7.2 TCP 封装 …… (342)
21.7.3 注册或警告标志 …… (343)
21.8 结论 …… (343)

第 7 篇 计算机操作方面的安全问题

第 22 章 黑客攻击工具和采用的技术手段 …… (347)
22.1 警告 …… (347)
22.2 在计算机攻击程序中的普遍特征 …… (348)
22.2.1 越来越智能化，同时还伴随无知者进行攻击的情况 …… (348)
22.2.2 广泛分布的高性能攻击工具 …… (348)
22.3 网络映射和端口扫描工具 …… (348)
22.4 对网络易受攻击性的扫描 …… (350)
22.5 Wardialing …… (351)
22.6 网络开发：嗅探、欺骗以及截获会话 …… (352)
22.6.1 嗅探器 …… (352)
22.6.2 IP 地址欺骗 …… (353)
22.6.3 截获会话攻击 …… (354)
22.7 拒绝服务攻击 …… (355)
22.7.1 残缺包攻击 …… (355)
22.7.2 包泛滥攻击 …… (356)
22.7.3 对拒绝服务的网络攻击所采取的防御措施 …… (357)
22.8 基于堆栈缓冲区溢出的网络攻击 …… (358)