



Information
Security Management
Handbook
(Volume I)
Fourth Edition

信息安全 管理手册(卷I) (第四版)

[美] Harold F. Tipton Micki Krause 主编 王卫卫 杨波 等译



电子工业出版社

PUBLISHING HOUSE OF ELECTRONICS INDUSTRY

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

电子信息科技专著出版专项资金资助出版

信息安全手册 (卷 I)

(第四版)

Information Security Management Handbook(Volume I)
Fourth Edition

[美] Harold F.Tipton Micki Krause 主编
王卫卫 杨波 等译

电子工业出版社

Publishing House of Electronics Industry

北京 • BEIJING

内 容 简 介

本手册共分 10 个部分。第一部分讨论访问控制系统和方法。第二部分叙述电信与网络安全问题。第三部分讨论安全管理的实现问题。第四部分讨论应用与系统开发安全问题。第五部分讨论密码学,主要是加密技术与实现。第六部分讨论安全结构与模型。第七部分讨论计算机操作安全问题。第八部分讨论业务连续性计划和灾难恢复计划。第九部分讨论法律、调查以及道德规范问题。第十部分讨论物理安全问题。

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。本手册的首要目的是作为应考 CISSP 的主要教材,也可以作为信息安全专业人员、研究人员的参考手册。本手册包括了 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每一章。

Information Security Management Handbook, Fourth Edition, Volume I, Copyright 2000, CRC Press LLC.

本书中文简体版专有出版权由 CRC Press 授予电子工业出版社,未经许可,不得以任何方式复制或抄袭本书的任何部分。

版权贸易合同登记号 图字:01-2002-5472

图书在版编目(CIP)数据

信息安全管理手册.1 卷:第 4 版/(美)泰普顿(Tipton,H.F.), (美)克劳斯(Krause,M.)主编;王卫卫,杨波译. —北京:电子工业出版社,2004.6

书名原文:Information Security Management Handbook(Volume I) Fourth Edition

ISBN 7-5053-9267-0

I.信… II.①泰…②克…③王… ④杨… III.信息系统—安全管理—技术手册 IV.TN309—62

中国版本图书馆 CIP 数据核字(2003)第 095922 号

责任编辑:王春宁

印 刷:北京民族印刷厂

出版发行:电子工业出版社 <http://www.phei.com.cn>

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:787×1092 1/16 印张:27.5 字数:694 千字

印 次:2004 年 6 月第 1 次印刷

印 数:5000 册 定价:49.00 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 zltz@phei.com.cn, 盗版侵权举报请发邮件至 dbqq@phei.com.cn。

译者序

信息在当今社会中的地位和作用越来越重要,已成为社会发展的重要战略资源,信息技术改变着人们的生活和工作方式,信息产业已成为新的经济增长点,社会的信息化已成为当今世界发展的潮流和核心。与此同时,信息的安全问题也已成为世人关注的社会问题。

CISSP (Certified Information System Security Professional)的证书由 International Information Systems Security Certification Consortium (简称为 (ISC)²)发布,其考试内容包括访问控制系统、密码学以及安全管理。目前拥有 CISSP 证书的人越来越受到企业的欢迎。本手册一方面是作为应考 CISSP 的主要教材,另一方面可以作为信息安全专业人员、研究人员的参考手册。

本手册共分 10 个部分,分别介绍访问控制系统和方法、电信与网络安全、安全管理的实现、应用与系统开发安全、密码学、安全结构与模型、操作安全、业务连续性计划和灾难恢复计划、法律及道德规范、物理安全。

参加本手册翻译的有王卫卫、杨波、王立明、符刚、刘秀英、王保仓、于志强、刘涛、吕锡香、程男男、赵志飞、魏凌波、胡明、王春松,由王卫卫统稿和审校。由于译者水平有限,错误在所难免,恳请读者批评指正。

前 言

本书不仅可以供信息安全专业人员作为参考手册，也可以供准备参加 CISSP 考试的人员作为复习资料。随着信息安全问题变得越来越复杂，企业也越来越需要拥有 CISSP 证书的人。

每年有几百人参加考试，但目前大约只有 2 500 人获得了国际信息系统安全证书联盟 (ISC)² 颁发的 CISSP 证书。考前准备是至关重要的，因为应考者需要完全了解该领域的常用知识。信息安全管理手册 (HISM) 系列书已成为应考者的主要参考书。

本书涵盖了 CISSP 考试所需的大部分内容，读者可以根据自己的需要去单独学习每一章。

第一部分讨论访问控制问题和方法。访问控制包括所有机制：物理访问、逻辑访问与管理访问，目的是保证只允许特殊的授权者或授权过程使用或访问系统。

第二部分讨论电信与网络安全问题。包括两大主题：网络安全以及因特网、内部网、外域网安全问题，目的是保证通过电信传输的信息是完整、可靠的，同时电信媒体是可利用的。

第三部分讨论安全管理实践问题，包括安全意识、企业结构和风险管理。制定合理的安全管理策略、程序、底线和原则可以保证企业有合理、持久的安全性；对信息分类有利于保护敏感信息；安全意识培训可以帮助员工理解并遵守执行企业的安全策略和程序；了解企业结构有助于确定适当的信息安全功能；风险管理是有效利用企业资源的管理工具。

第四部分讨论应用与系统开发安全问题，包括系统与应用软件中可以利用和已经使用的各种控制，以及开发设计系统与应用软件的过程。

第五部分讨论密码学。主要包括从最基本的到最新的加密技术与实现，例如，密钥管理、Kerberos 以及 PKI。

第六部分讨论安全系统结构与模型。计算机结构部分主要讨论计算机的组织和配置以保证计算机安全，模型部分主要讨论维护系统与信息安全的一些概念，本部分还包括个人计算机与局域网 (LAN) 的安全问题。

第七部分讨论操作安全问题。包括围绕着操作者与系统管理权限的数据中心和分布式处理安全问题、计算资源的保护，以及对这些重要资源的威胁将会带来的影响。

第八部分讨论业务连续性计划和灾难恢复计划。本部分的术语非常多，但基本上可以归结为制定具体的协作行动计划以避免或减轻正常的业务信息处理功能遭到破坏时带来的影响。

第九部分讨论法律、调查以及道德规范问题。法律包括信息安全功能面临的法律和约束问题。调查包括成功地调查安全事件并保持证据的真实完整性所需要的原则和原理。道德规范讨论正确与错误行为之间的区别以及自愿做正确的事情。

第十部分讨论物理安全问题。物理安全包括为信息处理活动提供安全的环境，主要讨论如何防止对计算设备的非法的物理与技术访问。

目 录

第一部分 访问控制系统和方法	(1)
第一单元 访问控制	(3)
第1章 基于生物统计学的个人身份识别技术	(3)
1.1 背景和历史	(3)
1.1.1 生物统计学的发展	(4)
1.2 生物统计学身份识别技术的特征	(5)
1.3 生物统计学身份识别技术的历史问题	(7)
1.4 生物统计学身份识别系统与磁卡系统相比的优点	(8)
1.5 生物统计学数据的升级更新	(9)
1.6 各种类型的生物统计学身份识别系统及其特征	(9)
1.7 信息安全的应用	(12)
1.8 总结	(14)
第2章 企业的单开始命令	(15)
2.1 引言	(15)
2.2 单开始命令标准的范围	(17)
2.2.1 功能目标: 用户单开始命令界面	(17)
2.2.2 用户账户管理界面	(18)
2.2.3 非功能目标	(18)
2.2.4 安全目标	(18)
2.2.5 SSOS 范围外的某些方面	(18)
2.3 共享系统	(19)
2.3.1 认证	(19)
2.3.2 通行字同步	(19)
2.3.3 单开始命令	(19)
2.4 通行字同步的优点	(20)
2.4.1 改进的安全性	(20)
2.4.2 更少的侵入	(20)
2.4.3 低成本	(20)
2.5 单开始命令的优点	(20)
2.5.1 方便	(20)
2.5.2 中心化管理	(20)
2.6 SSO 的一个企业解决方案	(20)
2.6.1 企业 SSO 的使用	(21)
2.6.2 远程登录	(21)
2.6.3 通行字的保护	(21)

2.6.4	通行字改变策略	(21)
2.6.5	审计和预警	(22)
2.6.6	SSO 加密	(22)
2.6.7	其他认证技术的整合	(22)
2.7	SSO 的其他解决方案	(23)
2.7.1	正确的 SSO 解决方案的选取	(23)
2.7.2	开放的结构	(23)
2.7.3	开放式认证	(23)
2.7.4	支持多记录方式	(24)
2.7.5	证书的转发	(24)
2.7.6	支持多服务器、客户机和主机	(24)
2.7.7	无缝的用户和管理界面	(24)
2.7.8	中心化管理	(24)
2.8	结论和总结	(24)
第二部分	电信与网络安全	(27)
第一单元	网络安全	(29)
第 3 章	与外部网的安全连接	(29)
3.1	危险与假设	(29)
3.2	安全策略	(30)
3.2.1	识别和认证	(30)
3.3	口令管理策略	(31)
3.4	软件引导控制	(32)
3.5	防火墙策略	(34)
3.5.1	防火墙认证	(34)
3.5.2	路由和转发	(35)
3.5.3	防火墙的类型	(35)
3.5.4	防火墙的结构	(36)
3.5.5	内域网	(37)
3.5.6	防火墙管理	(37)
3.6	防火墙的其他策略	(38)
3.6.1	网络信任关系	(38)
3.6.2	虚拟专用网 (VPN)	(38)
3.6.3	DNS 和邮件解析	(38)
3.6.4	系统完整性	(39)
3.6.5	文件	(39)
3.6.6	防火墙的物理安全性	(39)
3.6.7	防火墙的事故处理	(39)
3.6.8	服务的恢复	(40)
3.6.9	防火墙的升级	(40)
3.6.10	记录和审计跟踪 (审计/事件报告和总结)	(40)

3.7 小结	(40)
第二单元 因特网、内部网和外域网的安全	(42)
第4章 防火墙：因特网安全的有效解决方案	(42)
4.1 因特网的安全威胁	(42)
4.2 网络安全控制	(43)
4.2.1 加密	(43)
4.2.2 一次性口令	(43)
4.2.3 防火墙	(43)
4.3 防火墙的有效利用	(45)
4.3.1 正确选择防火墙	(45)
4.3.2 防火墙策略的重要性	(46)
4.3.3 安全维护	(46)
4.4 小结	(46)
第5章 因特网安全：周边的安全问题	(47)
5.1 因特网协议	(48)
5.1.1 攻击	(49)
5.1.2 ICMP	(51)
5.1.3 防火墙	(51)
5.1.4 DMZ	(52)
5.1.5 代理服务器	(52)
5.1.6 检测周边	(52)
5.2 总结	(55)
第6章 外域网的访问控制	(56)
6.1 引言	(56)
6.2 谁在线上	(56)
6.3 外域网安全策略	(57)
6.4 网络划分	(58)
6.5 外域网认证	(59)
6.6 外域网授权	(60)
6.7 外域网管理	(60)
6.8 外域网连接协议	(61)
6.9 外域网监控	(61)
6.10 外域网的安全结构	(62)
6.11 VPN 技术	(62)
6.12 其余的风险/漏洞	(63)
6.13 采购外域网	(63)
6.14 汽车网络交换机	(63)
6.15 小结	(64)
第7章 防火墙管理和 Internet 攻击	(66)
7.1 防火墙的基本知识	(66)

7.1.1	拥有防火墙的好处	(66)
7.1.2	防火墙的局限性	(67)
7.2	防火墙和本地安全策略	(67)
7.3	防火墙的评估准则	(68)
7.4	防火墙技术	(68)
7.5	创建防火墙策略与标准	(70)
7.5.1	为什么要建立防火墙策略和标准	(70)
7.5.2	策略和标准的发展过程	(70)
7.5.3	策略结构	(71)
7.6	防火墙标准	(72)
7.7	与防火墙有关的法律问题	(73)
7.8	防火墙的意外事件计划	(74)
7.8.1	防火墙中断	(74)
7.8.2	一些重要的攻击、探测和弱点	(74)
7.9	结论	(76)
	参考文献	(76)
第 8 章	网络层安全	(77)
8.1	引言	(77)
8.2	网络层的结构、服务和协议	(77)
8.3	安全服务体系结构设置	(78)
8.4	终端系统层安全	(79)
8.5	子网层安全	(79)
8.6	网络层安全协议	(80)
8.7	安全数据传输	(80)
8.8	连接的建立和释放	(81)
8.9	小结	(82)
第 9 章	传输层安全	(83)
9.1	引言	(83)
9.2	传输层概述	(83)
9.3	子网可靠性	(84)
9.4	传输分类	(85)
9.5	传输程序	(85)
9.6	加速数据	(88)
9.7	服务质量	(88)
9.8	安全体系结构	(89)
9.9	安全机制	(89)
9.10	安全关联的属性	(90)
9.11	安全关联协议	(90)
9.12	常用缩写列表	(90)
第 10 章	网络应用层的安全协议	(92)

10.1	我们不再局限于堪萨斯州了	(92)
10.2	在安全措施下逐层观察	(92)
10.3	应用层安全——ALS 101	(93)
10.4	交互性——ALS 成功的关键	(93)
10.4.1	标准的安全服务——最大限度的信息保护	(94)
10.4.2	算法的可靠性和正确性	(94)
10.4.3	标准化的杂乱信息仍是杂乱信息	(94)
10.5	范例——VISA 卡的安全电子贸易协议	(95)
10.6	从明信片到信件——安全的电子信息	(96)
10.7	驯服 HTTP——网络应用安全	(98)
10.8	不要给我钱——货币交易的安全性	(100)
10.9	如果现在还没有加密	(101)
	参考文献	(101)
第 11 章	通信协议和服务的安全	(103)
11.1	引言	(103)
11.2	协议	(104)
11.3	网络互联协议	(104)
11.3.1	网络互联协议 6.0 (下一代网际协议)	(105)
11.3.2	用户数据包协议 (UDP)	(105)
11.3.3	传输控制协议 (TCP)	(106)
11.3.4	远程登录	(106)
11.3.5	文件传输协议 (FTP)	(107)
11.3.6	串行线路因特网协议 (SLIP)	(107)
11.3.7	点到点协议 (PPP)	(107)
11.3.8	超文本传输协议 (HTTP)	(107)
11.4	安全协议	(108)
11.4.1	安全传输层 (SSL)	(108)
11.4.2	安全超文本传输协议 (S-http)	(108)
11.4.3	安全文件传输协议 (S-ftp)	(109)
11.4.4	安全电子交易 (SET)	(109)
11.4.5	点到点隧道协议 (PPTP)	(109)
11.4.6	转发第二层协议 (L2F)	(110)
11.4.7	第二层隧道协议 (L2TP)	(110)
11.4.8	因特网安全协议 (Secure-IP 或 IPSEC)	(110)
11.4.9	因特网安全协会密钥管理协议 (ISAKMP)	(110)
11.4.10	密码认证协议 (PAP)	(110)
11.4.11	竞争握手认证协议 (CHAP)	(110)
11.5	服务	(111)
11.5.1	文件传输	(111)
11.5.2	安全框架 (SSH2)	(111)

11.6 结论	(111)
第三部分 安全管理练习	(113)
第一单元 安全意识	(115)
第 12 章 安全意识计划	(115)
12.1 引言	(115)
12.2 信息安全计划的关键目标	(115)
12.3 信息安全计划的关键因素	(116)
12.4 安防意识计划的目标	(116)
12.5 明确当前的培训需求	(117)
12.6 安防意识计划的发展	(118)
12.7 传递警示信息的方法	(119)
12.8 发布关键因素	(120)
12.9 典型的信息发布方式	(120)
12.10 何时实施安防意识计划	(121)
12.11 高级管理层的信息发布	(121)
12.12 信息安全消息	(122)
12.13 信息安全的自我评价	(122)
12.14 小结	(124)
第二单元 组织结构	(125)
第 13 章 企业安全结构	(125)
13.1 引言	(125)
13.1.1 企业	(125)
13.2 20 世纪 90 年代的企业安全状况	(125)
13.3 结构的定义	(126)
13.4 传统 IT 环境	(127)
13.5 现代 IT 环境	(127)
13.6 其他安全结构要求	(128)
13.7 安全结构	(128)
13.8 策略	(128)
13.8.1 管理目的描述	(128)
13.9 重要的安全服务	(129)
13.10 建议的企业安全结构	(129)
13.11 附录	(131)
13.11.1 附录 I	(131)
13.11.2 附录 II	(132)
13.11.3 附录 III	(132)
13.11.4 附录 IV	(133)
第 14 章 IPSEC 简介	(134)
14.1 IPSEC 的特点	(134)
14.1.1 变换无关的独立保密与认证功能	(134)

14.1.2	单向结构网络层的实现	(134)
14.1.3	主机与网关拓扑	(135)
14.1.4	密钥管理	(135)
14.2	IPSEC 的实现与结构	(135)
14.2.1	安全关联 (SA)	(135)
14.2.2	安全参数索引 (SPI)	(136)
14.2.3	认证功能	(136)
14.2.4	保密性功能	(138)
14.2.5	密钥管理	(139)
14.2.6	因特网安全关联与密钥管理协议 (ISAKMP)	(139)
14.3	综述	(141)
第三单元 风险管理		(142)
第 15 章	风险分析与评估	(142)
15.1	术语与定义	(143)
15.2	信息风险管理的中心任务	(145)
15.2.1	建立信息风险管理 (IRM) 策略	(145)
15.2.2	建立并投资一个信息风险管理小组	(146)
15.2.3	建立信息风险管理的系统方法和工具	(146)
15.2.4	鉴定并衡量风险	(146)
15.2.5	建立风险的接受标准	(147)
15.2.6	缓解风险	(147)
15.2.7	监控信息风险管理的性能	(148)
15.2.8	阻力和益处	(148)
15.2.9	定性方法与定量方法	(150)
15.2.10	风险度量标准的要素	(150)
15.2.11	定性方法和定量方法的赞成与反对观点	(152)
15.2.12	经济影响分析与风险评估	(153)
15.2.13	对象读者所关心的问题	(153)
15.3	风险管理的任务	(155)
15.3.1	方案筛分	(155)
15.3.2	资产鉴定和评估	(157)
15.3.3	脆弱性分析	(158)
15.3.4	危险/脆弱性/资产的联系	(159)
15.3.5	风险削减分析	(162)
15.3.6	自动化工具	(165)
15.4	总结	(166)
第 16 章	保护高科技商业秘密	(167)
16.1	商业秘密综述及其重要性	(167)
16.1.1	专有信息和商业秘密	(168)
16.1.2	1996 年经济间谍法 (EEA, Economic Espionage Act)	(168)

16.1.3	知识产权的价值	(169)
16.1.4	敏感信息常常是数字与便携的	(170)
16.1.5	“失控”的风险不断增加	(170)
16.1.6	标准保密信息	(170)
16.2	敏感专有信息的新威胁	(171)
16.2.1	商业道德与忠诚度的下降	(171)
16.2.2	因特网: 黑客的练武场	(172)
16.2.3	间谍威胁的增长	(172)
16.2.4	全球化经营的影响	(173)
16.2.5	网络、电脑和电话的威胁	(173)
16.3	应该怎么办	(174)
16.3.1	保护商业秘密信息的必要措施	(174)
16.3.2	推荐保护措施	(174)
16.4	结论: 不能单单依赖法庭保护你的秘密	(176)
第 17 章	医疗卫生行业中的信息安全管理	(177)
17.1	引言	(177)
17.2	医疗信息系统的历史和管理上的先天不足	(177)
17.3	医疗卫生组织面临的挑战, 有关信息系统	(178)
17.4	医疗公司要实现顾客中心系统必须克服的困难	(179)
17.5	历史的重演	(182)
17.6	最近几个月提出的大量隐私法律	(183)
17.6.1	Kennedy-Kassebaum 法案: 背景	(183)
17.6.2	《为了记录》: 一份报告	(183)
17.7	HIPAA 的行政简化版: 安全标准	(184)
17.8	总结	(186)
第四部分	应用和系统开发的安全问题	(187)
第一单元	应用安全	(189)
第 18 章	面向对象数据库的安全模型	(189)
18.1	引言	(189)
18.2	数据库安全基础	(189)
18.2.1	自主型与强制型访问控制策略	(190)
18.3	关系型数据库管理系统与面向对象数据库管理系统在安全方面的区别	(190)
18.3.1	关系型 DBMS 的安全问题	(190)
18.3.2	面向对象数据库管理系统的特征	(191)
18.3.3	已经提出的 OODBMS 安全模型	(191)
18.4	结论	(193)
第五部分	密码学	(195)
第一单元	密码技术及其实现	(197)
第 19 章	密码学基础和加密方法	(197)
19.1	基本定义	(197)

19.2	相关历史	(198)
19.3	现代密码学基础	(199)
19.4	流密码	(200)
19.5	分组密码	(202)
19.6	密码分析	(204)
19.7	密钥(密码变量)管理	(208)
19.8	公钥密码学	(209)
19.8.1	中间人	(211)
19.9	椭圆曲线加密	(212)
19.9.1	Diffie 和 Hellman 密钥分配算法	(212)
19.10	结论	(214)
	参考文献	(214)
第 20 章	密钥管理的原则和应用	(215)
20.1	引言	(215)
20.2	背景知识	(215)
20.3	密钥管理定义	(216)
20.4	密钥管理的功能	(216)
20.4.1	密钥的产生	(217)
20.4.2	密钥分配	(217)
20.4.3	安装	(217)
20.4.4	存储	(217)
20.4.5	密钥更换	(218)
20.4.6	密钥控制	(218)
20.4.7	销毁	(218)
20.5	现代密钥管理	(218)
20.6	密钥管理原则	(220)
20.7	非对称密钥加密	(221)
20.8	混合加密体系	(222)
20.9	公钥认证	(222)
20.10	使用认证管理密钥	(223)
20.11	实现	(225)
20.11.1	Kerberos 密钥分配中心	(225)
20.11.2	PGP	(225)
20.11.3	ViaCrypt PGP 商业版	(226)
20.11.4	RSA 安全 PC	(226)
20.11.5	BBN SafeKeyper	(227)
20.11.6	加密套接字协议层(SSL)	(227)
20.12	密钥管理建议	(227)
第 21 章	分布式系统中 Kerberos 的实现	(229)
21.1	发展历史	(229)

21.1.1	现在的开发情况	(229)
21.2	标准与实现	(230)
21.3	对 Kerberos 的认知与 Kerberos 技术	(230)
21.3.1	信任、标识和代价	(231)
21.3.2	技术影响	(232)
21.3.3	协议的放置	(232)
21.3.4	口令	(233)
21.3.5	密码系统	(233)
21.3.6	在线操作	(233)
21.4	组织模式	(234)
21.5	信任模型	(234)
21.5.1	直接信任	(235)
21.5.2	间接信任	(235)
21.6	安全模型	(236)
21.6.1	证书	(236)
21.6.2	证书的使用期限	(237)
21.6.3	能限	(237)
21.6.4	委托	(237)
21.7	安全服务	(238)
21.7.1	认证	(238)
21.7.2	安全信道	(238)
21.7.3	完整性	(239)
21.7.4	保密性	(239)
21.7.5	访问控制	(239)
21.7.6	授权	(239)
21.7.7	不可否认	(239)
21.7.8	可获取性	(240)
21.8	功能概述	(240)
21.8.1	组成部分	(240)
21.8.2	认证	(241)
21.8.3	证书缓存	(243)
21.8.4	票据认证	(243)
21.9	功能描述	(245)
21.9.1	初始化认证	(245)
21.9.2	预认证	(245)
21.9.3	KDC-客户交互	(246)
21.9.4	初始票据	(246)
21.9.5	票据创建	(247)
21.9.6	客户-服务交互	(247)
21.9.7	重发保护	(248)

21.9.8	会话密钥	(249)
21.9.9	跨域认证	(250)
21.9.10	票据限制	(251)
21.9.11	代理服务	(253)
21.9.12	授权	(253)
21.9.13	能限与委托	(254)
21.10	管理	(257)
21.10.1	用户	(257)
21.10.2	假设条件	(258)
21.10.3	运作	(259)
21.10.4	名和定位	(262)
21.10.5	协同工作能力	(264)
21.10.6	性能	(264)
21.10.7	配备要求	(266)
21.10.8	部署	(267)
21.11	发展动态	(269)
21.11.1	标准	(269)
21.11.2	相关技术	(270)
21.12	得到的教训	(275)
21.12.1	风险、顾虑和价值	(275)
21.12.2	分布式安全	(276)
	参考文献	(276)
第 22 章	PKI 初步	(280)
22.1	方法和初步讨论	(280)
22.2	不断变化的网络系统	(280)
22.3	不断发展的商务网络	(281)
22.3.1	安全机制的瓦解和重建	(282)
22.3.2	加密的定义	(282)
22.4	着手 PKI	(283)
22.4.1	数字证书和证书授权	(283)
22.4.2	使用证书的场所	(284)
22.4.3	PKI 怎样满足这些商务环境的需求	(284)
22.4.4	针对市场的明确决策	(284)
22.5	证书、证书管理机构和注册管理机构	(284)
22.5.1	必须考虑的 PKI 的功能实体是谁或是什么	(285)
22.5.2	其他的实体	(285)
22.5.3	证书撤销列表(CRL)	(286)
22.5.4	PKI 怎样满足今天开放式系统的安全需要	(288)
22.5.5	实施 PKI 节省成本的做法需要什么	(289)
22.6	CA 试验需要考虑的事项	(289)

22.6.1	试验的类型	(289)
22.6.2	PKI 是一个例外的方法还是众多可供选择的方法中的一种	(289)
第六部分	安全系统结构和模型	(291)
第一单元	微型计算机和局域网的安全	(293)
第 23 章	微型计算机和局域网的安全	(293)
23.1	引言	(293)
23.1.1	台式环境的重要性	(293)
23.1.2	采取的方法	(293)
23.1.3	集中的、分层的基于设计的方法	(293)
23.2	台式系统的安全：问题、威胁和后果	(294)
23.2.1	微机的普遍性	(294)
23.2.2	台式系统的体系结构	(295)
23.3	台式机的安全策略和意识	(296)
23.3.1	自上而下的方法	(296)
23.3.2	细节问题	(296)
23.3.3	台式系统的安全意识	(297)
23.4	台式计算机和便携式计算机的物理安全性	(297)
23.5	台式系统的数据备份	(298)
23.5.1	备份的类型和设备	(298)
23.5.2	提倡备份	(300)
23.5.3	备份方法	(301)
23.5.4	备份体制	(302)
23.5.5	备份管理和存储	(302)
23.5.6	远程备份	(303)
23.6	病毒和其他恶意代码的防治措施	(304)
23.6.1	恶意代码	(304)
23.6.2	病毒	(305)
23.6.3	特洛伊木马病毒	(305)
23.6.4	蠕虫	(306)
23.6.5	逻辑炸弹	(306)
23.6.6	恶意代码的防御措施	(306)
23.6.7	与病毒同步	(307)
23.6.8	基本准则	(307)
23.6.9	引导区病毒	(308)
23.6.10	寄生病毒	(308)
23.6.11	多重病毒和伴侣病毒	(309)
23.6.12	其他病毒	(309)
23.6.13	隐身病毒和多态病毒	(310)
23.6.14	宏病毒	(310)
23.7	访问控制和加密	(311)