

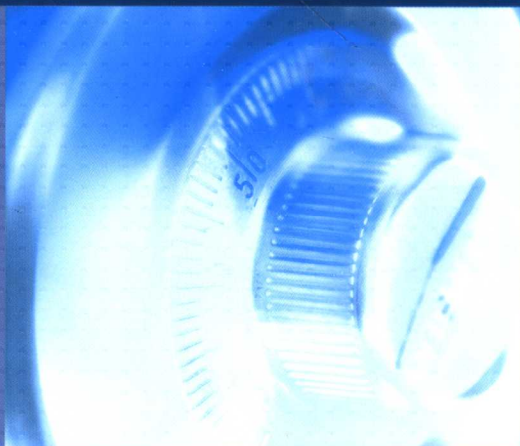


普通高等教育“十一五”国家级规划教材

电子商务 安全与保密

(第2版)

□ 祁 明 主编



高等教育出版社
Higher Education Press

普通高等教育“十一五”国家级规划教材

电子商务安全与保密

(第2版)

祁 明 主 编

毕凌燕 左文明 许伯桐 编 著

高等教育出版社

图书在版编目(CIP)数据

电子商务安全与保密 / 祁明主编. — 2 版. — 北京:
高等教育出版社, 2006.12
ISBN 7-04-020228-X

I. 电... II. 祁... III. 电子商务 - 安全技术 - 高
等学校 - 教材 IV. F713.36

中国版本图书馆 CIP 数据核字(2006)第 131134 号

策划编辑 韩 飞 责任编辑 贺 玲 封面设计 王凌波 责任绘图 朱 静
版式设计 张 岚 责任校对 殷 然 责任印制 陈伟光

出版发行 高等教育出版社
社 址 北京市西城区德外大街 4 号
邮政编码 100011
总 机 010-58581000

经 销 蓝色畅想图书发行有限公司
印 刷 北京宝旺印务有限公司

购书热线 010 - 58581118
免费咨询 800 - 810 - 0598
网 址 <http://www.hep.edu.cn>
<http://www.hep.com.cn>
网上订购 <http://www.landaco.com>
<http://www.landaco.com.cn>
畅想教育 <http://www.widedu.com>

开 本 787 × 1092 1/16
印 张 34
字 数 710 000

版 次 2001 年 7 月第 1 版
2006 年 12 月第 2 版
印 次 2006 年 12 月第 1 次印刷
定 价 35.10 元

本书如有缺页、倒页、脱页等质量问题, 请到所购图书销售部门联系调换。

版权所有 侵权必究

物料号 20228 - 00

内 容 简 介

本书是在第一版同名教材使用五年的基础上修订而成的,在保持原有基本体系结构的同时,添加了许多电子商务安全发展的新理论、新技术和新案例。本书比较系统地介绍了电子商务安全保密的基本理论和实用技术,既简明扼要地介绍了国内外的前沿研究成果,又详细介绍了电子商务中迫切需要的安全保密知识。

本书共分 18 章,涉及的范围比较广泛,主要内容有:电子商务安全的现状与趋势、信息论与数学基础、信息加密技术与应用、数字签名技术与应用、身份认证与访问控制、密钥管理与 PKI 体系、WWW 与 Web 服务安全、防火墙的构造与选择、计算机病毒的产生与防治、安全通信协议与交易协议、网络攻击与防御、信息隐藏与数字水印、电子邮件安全协议与系统设计、移动通信系统安全、反计算机犯罪与网上版权保护、计算机软件综合保护方法、系统评估准则与安全策略、计算机信息系统安全保护制度。

本书的习题有三种类型:复习题、思考题和上网题。这些练习使得老师能够根据学生的背景和需求灵活地调整练习难度和深度,同时也使得学生在掌握基本的知识点之后,在学术研究、技术开发和创业方面更快捷地找到对应的热点话题和课题。

本书可作为高等院校电子商务、物流工程与管理、经济信息管理、计算机科学与技术、通信工程专业及相关专业本科生或研究生的电子商务安全教材,也可供从事电子商务研究和应用开发人员学习参考。

郑 重 声 明

高等教育出版社依法对本书享有专有出版权。任何未经许可的复制、销售行为均违反《中华人民共和国著作权法》，其行为人将承担相应的民事责任和行政责任，构成犯罪的，将被依法追究刑事责任。为了维护市场秩序，保护读者的合法权益，避免读者误用盗版书造成不良后果，我社将配合行政执法部门和司法机关对违法犯罪的单位和个人给予严厉打击。社会各界人士如发现上述侵权行为，希望及时举报，本社将奖励举报有功人员。

反盗版举报电话：(010) 58581897/58581896/58581879

传 真：(010) 82086060

E - mail：dd@hep.com.cn

通信地址：北京市西城区德外大街4号

高等教育出版社打击盗版办公室

邮 编：100011

购书请拨打电话：(010)58581118

前 言

自计算机网络出现以来,网络的安全就成为网络使用者不得不面对的问题。如今,随着网络应用水平的提高和电子商务的大力开展,计算机系统的安全隐患也日渐突出,诸如高科技犯罪、机密泄露、黑客入侵、病毒侵扰等,其危害之严重、手段之高超令人惊异。

据美国联邦调查局 FBI 的调查,美国每年因为网络安全造成的经济损失超过 170 亿美元,大约 75% 的公司的财政损失是由于计算机系统的安全问题造成的,但其中只有 17% 的公司愿意报告遭受过黑客的袭击,而大部分公司由于担心负面影响而不愿声张。

中国的网络安全和电子商务安全情况并不乐观。最近,国家有关专家曾对国内多家网站的安全性能做了测试,结果令人震惊——在测试的网站中有近 90% 的网站存在着不同程度的安全隐患。黑客攻击网站的例子举不胜举,如新浪网、中国公众多媒体信息网、国家统计局网站等。总之,互联网与电子商务的安全问题已经引起了人们的担忧,各国政府、IT 厂商和业界同仁在感到震惊的同时,也开始积极思考对策和提供针对不同需求的解决方案。

为了普及计算机网络和电子商务的安全保密技术,推进我国信息安全产业的发展,增进与国内外同行之间的交流,我们编著了这本教材。

本书四位作者都来自华南理工大学电子商务学院。全书由祁明担任主编,其中第 1~4 章和第 17、18 章由祁明编写,第 8、9、14、15 章由毕凌燕编写,第 5、12、13、16 章由左文明编写,第 6、7、10、11 章由许伯桐编写。

在写作过程中,作者试图从理论和实践相结合的角度较系统地介绍电子商务安全保密的基本理论和实用技术。既介绍国内外的前沿研究成果,又介绍目前已经成熟的实用技术;既注重介绍安全保密的基本概念和算法,又照顾到学习电子商务课程学生来源的广泛性、知识背景的多样性和要求的多层次性。尽管作者有以上初衷,但因学术水平有限和篇幅所限,许多与电子商务有关的安全保密技术未能介绍或介绍得不够全面。另外,本书编校虽力求完美,然而谬误之处在所难免,对此,作者恳请读者的理解和批评指正。

本书是作者在 2001 年第一版教材五年多教学和研究的基础上修改而成的。作者在写作过程中参阅了大量的国内外资料,在此谨向书中所提到的和参考文献所列出的各位作者表示衷心的感谢。

本书的编写和有关研究工作还得到了高等教育出版社的热情关心和支持,在此我们深表谢意!

编 者

2006 年 7 月于广州

目 录

第1章 电子商务安全的现状与趋势1

1.1 电子商务安全概述1

1.1.1 电子商务安全结构与要求1

1.1.2 电子商务安全案例与分析2

1.1.3 涉密计算机网络的六大隐患3

1.1.4 新一代信息安全与十大关系4

1.1.5 信息安全重要事件8

1.2 中国信息安全战略与对策10

1.2.1 信息安全保障体系六大要素10

1.2.2 国家信息安全应急响应体系13

1.2.3 国家信息安全标准体系15

1.2.4 电子政务信息安全等级保护18

1.2.5 金字工程与信息安全21

1.3 国外信息安全战略与对策23

1.3.1 新加坡与韩国打击网络犯罪的措施23

1.3.2 英国政府大力遏制网络犯罪24

1.3.3 美国信息安全体系与应急策略24

1.3.4 日本计算机病毒与信息安全对策30

1.3.5 俄罗斯信息安全学说32

1.3.6 瑞士政府信息化与安全战略34

复习题36

思考题36

上网题36

第2章 信息论与数学基础37

2.1 信息论37

2.1.1 熵和不确定性37

2.1.2 语言信息率38

2.1.3 密码体制的安全性39

2.1.4 唯一解距离39

2.1.5 信息论的运用40

2.1.6 混乱和散布40

2.2 复杂性理论40

2.2.1 算法的复杂性41

2.2.2 问题的复杂性42

2.2.3 NP 完全性问题42

2.3 数论43

2.3.1 模运算44

2.3.2 素数45

2.3.3 最大公因子45

2.3.4 取模数求逆元46

2.3.5 费马小定理46

2.3.6 欧拉函数46

2.3.7 中国剩余定理47

2.3.8 二次剩余47

2.3.9 勒让德符号48

2.3.10 雅可比符号48

2.3.11 Blum 整数49

2.3.12 生成元49

2.3.13 有限域50

2.3.14 $GF(p^m)$ 上的计算51

2.4 因子分解52

2.4.1 因子分解算法52

2.4.2 模 n 的平方根53

2.5 素数生成元54

2.5.1 Solovag-Strassen 方法54

2.5.2 Rabin-Miller 方法55

2.5.3 Lehmann 方法55

2.5.4 强素数55

2.6 有限域上的离散对数	56	复习题	90
2.6.1 离散对数基本定义	56	思考题	90
2.6.2 计算有限群中的离散对数	56	上网题	91
复习题	57	第4章 数字签名技术与应用	92
思考题	57	4.1 数字签名的基本原理	92
上网题	57	4.1.1 数字签名的基本要求	92
第3章 信息加密技术与应用	58	4.1.2 数字签名与手写签名的区别	92
3.1 网络通信中的加密方式	59	4.1.3 数字签名的分类	93
3.1.1 链路-链路加密	59	4.1.4 数字签名的使用模式	93
3.1.2 节点加密	60	4.1.5 数字签名应用实例	94
3.1.3 端到端加密	60	4.2 RSA 签名	95
3.1.4 加密方式的选择	61	4.3 ElGamal 签名	96
3.2 分组加密体制与标准	62	4.4 盲签名及其应用	97
3.2.1 数据加密标准 (DES)	63	4.4.1 盲消息签名	97
3.2.2 国际数据加密算法 (IDEA)	68	4.4.2 盲参数签名	98
3.2.3 高级加密标准 (AES)	68	4.4.3 弱盲签名	98
3.3 公钥加密体制	75	4.4.4 强盲签名	99
3.3.1 RSA 加密体制	76	4.5 多重签名及其应用	100
3.3.2 背包加密体制	78	4.6 定向签名及其应用	100
3.3.3 ElGamal 加密体制	80	4.6.1 ElGamal 型定向签名	101
3.4 复合型加密体制 PGP	80	4.6.2 MR 型定向签名方案	101
3.4.1 完美的加密 PGP	80	4.7 代理签名及其应用	102
3.4.2 PGP 的多种加密方式	81	4.7.1 代理签名的基本要求	102
3.4.3 PGP 的广泛应用	82	4.7.2 双重安全代理签名方案	103
3.4.4 PGP 商务安全方案	83	4.8 美国数字签名标准 (DSS)	104
3.5 量子密码技术	84	4.8.1 Hash 函数	105
3.5.1 量子密码学的基本概念	84	4.8.2 DSS 原理	106
3.5.2 量子密码学的发展现状	85	4.8.3 DSA 算法	107
3.5.3 量子密码学的主要应用	86	4.9 世界各国签名立法状况	108
3.6 椭圆曲线加密	87	4.9.1 电子签名与数字签名	108
3.6.1 有限域上的椭圆曲线定义	87	4.9.2 中国电子签名法	109
3.6.2 椭圆曲线上的密码算法	88	4.10 数字签名产品与系统介绍	111
3.6.3 椭圆曲线密码算法的讨论	88	复习题	115
3.7 加密产品与系统简介	89	思考题	115

上网题	115	5.7.2 视网膜图像识别系统	137
第 5 章 身份认证与访问控制	116	5.8 掌纹识别技术	137
5.1 口令识别法	116	5.8.1 掌纹识别的特点	137
5.1.1 用户识别方法分类	116	5.8.2 掌纹识别技术	138
5.1.2 不安全口令的分析	117	5.9 生物特征识别技术的发展前景	138
5.1.3 一次性口令	118	5.9.1 生物特征识别系统的评价	138
5.1.4 SecurID 卡系统	121	5.9.2 生物识别技术的发展前景	139
5.2 指纹识别技术	121	5.10 访问控制	140
5.2.1 指纹识别技术简介	122	5.10.1 访问控制的概念与原理	140
5.2.2 指纹取像的几种技术和特点	122	5.10.2 访问控制策略及控制机构	141
5.2.3 指纹识别系统中的软件和固件	123	5.10.3 访问控制模型	142
5.2.4 指纹识别技术的优缺点	124	5.11 访问控制类产品	147
5.2.5 指纹识别技术的可靠性问题	125	复习题	152
5.2.6 指纹识别技术的应用系统	125	思考题	152
5.2.7 指纹识别技术的一些应用	126	上网题	152
5.3 人脸识别技术	126	第 6 章 密钥管理与 PKI 体系	153
5.3.1 人脸识别技术简介	126	6.1 密钥的结构与分配	153
5.3.2 人脸识别中的关键技术	127	6.1.1 密钥管理概述	153
5.3.3 人脸识别应用系统	128	6.1.2 密钥的自动分配	154
5.4 签名鉴别与笔迹鉴别	128	6.1.3 密钥共享	158
5.4.1 联机签名鉴别	129	6.1.4 第三方密钥托管协议	158
5.4.2 脱机签名鉴别	130	6.2 公钥基础设施	161
5.4.3 笔迹鉴别	130	6.2.1 PKI 概述	161
5.5 声纹识别技术	131	6.2.2 PKIX 模型	162
5.5.1 声纹识别特点	131	6.2.3 交叉认证	165
5.5.2 声纹识别技术的分类	132	6.2.4 PKI 信任模型	166
5.5.3 声纹识别系统研究关键问题	132	6.2.5 PMI 模型	172
5.5.4 声纹识别技术应用领域	133	6.2.6 PKI 与 PMI 的关系	174
5.6 虹膜识别技术	134	6.3 数字证书	175
5.6.1 虹膜识别技术	134	6.3.1 数字证书的基本概念	175
5.6.2 虹膜识别的关键技术	134	6.3.2 X.509 公钥证书格式	176
5.6.3 虹膜识别技术的应用	135	6.3.3 属性证书	176
5.7 视网膜图像识别技术	136	6.4 国家 PKI 战略与发展	177
5.7.1 视网膜识别技术的特点	136	6.4.1 中国国家 PKI 体系框架	177

6.4.2 美国联邦 PKI 体系框架	180	8.2.3 代理服务	222
6.4.3 加拿大 PKI 体系框架	181	8.2.4 深度包检测	223
6.4.4 美加两国 PKI 体系对比	182	8.2.5 分布式防火墙	224
复习题	183	8.3 防火墙的体系结构	225
思考题	183	8.3.1 双宿主主机结构	225
上网题	183	8.3.2 主机过滤结构	226
第 7 章 WWW 与 Web 服务安全	184	8.3.3 子网过滤结构	227
7.1 TCP/IP 服务安全	184	8.4 防火墙的选择与实施	231
7.1.1 WWW 服务器的安全	184	8.4.1 防火墙的局限性	231
7.1.2 Web 客户端安全	192	8.4.2 怎样选择合适的防火墙	232
7.1.3 FTP 协议	194	8.4.3 防火墙的测试	233
7.1.4 Telnet 协议	195	8.4.4 防火墙的安装	234
7.1.5 DNS 的安全性	195	8.4.5 防火墙的管理与维护	234
7.1.6 NFS 和 NIS 安全	196	8.5 防火墙产品介绍	234
7.2 Web 服务安全	197	8.5.1 企业防火墙	234
7.2.1 Web 服务简介	197	8.5.2 个人防火墙	236
7.2.2 XML 及 Web 服务安全标准	200	复习题	237
7.2.3 Web 服务安全协议栈	204	思考题	238
7.3 Web 编程的安全性	207	上网题	238
7.3.1 J2EE 的安全结构	207	第 9 章 计算机病毒的产生与预防	239
7.3.2 ASP.NET 应用程序安全模型	209	9.1 计算机病毒的概念	239
7.3.3 Web 服务安全编程工具	212	9.1.1 病毒的产生	240
7.3.4 输入检查与输出过滤	214	9.1.2 病毒的特征	240
复习题	215	9.1.3 病毒现象和传播途径	241
思考题	215	9.2 传统病毒的工作原理	242
上网题	215	9.2.1 传统病毒的工作机理	242
第 8 章 防火墙的构造与选择	216	9.2.2 引导型病毒工作原理	243
8.1 防火墙概述	216	9.2.3 文件型病毒的工作原理	246
8.1.1 什么是防火墙	216	9.3 网络病毒的工作原理	247
8.1.2 防火墙的功能	217	9.3.1 木马病毒的工作原理	247
8.1.3 防火墙有关术语	218	9.3.2 蠕虫病毒的工作原理	250
8.2 防火墙的分类	219	9.4 典型病毒的危害与清除	252
8.2.1 包过滤防火墙	219	9.4.1 CIH 病毒	252
8.2.2 状态包检测防火墙	221	9.4.2 宏病毒	255

9.4.3 QQ 尾巴病毒	258	10.4 EDI 的安全	292
9.4.4 冲击波病毒	259	10.4.1 EDI 概述	292
9.4.5 证券大盗	260	10.4.2 EDI 系统面临的安全威胁	293
9.5 反计算机病毒技术	261	10.4.3 EDI 系统的安全策略	294
9.5.1 病毒防治技术	261	10.4.4 EDI 安全服务的实现	295
9.5.2 病毒检测技术	264	10.4.5 EDI 的安全模型	295
9.5.3 病毒清除技术	265	10.5 RADIUS 协议	296
9.6 杀毒软件介绍	267	10.5.1 RADIUS 概述	296
复习题	269	10.5.2 操作过程	297
思考题	269	10.5.3 认证码	298
上网题	269	10.5.4 RADIUS 代理	299
第 10 章 安全通信协议与交易协议	270	10.5.5 RADIUS 应用	299
10.1 IPSec 协议	270	复习题	300
10.1.1 IPSec 概述	270	思考题	300
10.1.2 安全关联	271	上网题	300
10.1.3 IP 认证协议	271	第 11 章 网络攻击与防御	301
10.1.4 IP 安全封装负载协议 (ESP)	272	11.1 网络攻击方法分析	301
10.1.5 鉴别与保密的综合	274	11.1.1 网络攻击概述	301
10.1.6 密钥管理协议	274	11.1.2 网络攻击分类	303
10.2 安全套接层 (SSL) 协议	275	11.2 常用的攻击工具与防范方法	304
10.2.1 SSL 协议概述	275	11.2.1 安全扫描	304
10.2.2 SSL 记录协议	276	11.2.2 监听	306
10.2.3 SSL 握手协议	276	11.2.3 恶意代码	307
10.2.4 SSL 提供的安全服务	278	11.2.4 缓冲区溢出	310
10.2.5 SSL、SSH 和 S-HTTP 的对比	279	11.2.5 拒绝服务攻击	310
10.3 安全电子交易 (SET) 协议	279	11.2.6 脚本攻击	311
10.3.1 SET 概述	279	11.2.7 口令攻击	312
10.3.2 双签名机制	280	11.2.8 欺骗攻击	312
10.3.3 证书发行	282	11.2.9 防火墙攻击	313
(certificate issuance)	282	11.3 入侵检测技术	314
10.3.4 支付流程	284	11.3.1 IDS 概论	314
(payment processing)	284	11.3.2 入侵检测系统模型	315
10.3.5 SET 协议的不足	289	11.3.3 入侵检测系统分类	316
10.3.6 SET 与 3D-Secure	290	11.3.4 入侵检测技术的发展趋势	318

11.3.5 入侵检测系统实例: Snort	320	13.1.6 POP3 协议	358
11.4 计算机犯罪勘查技术	321	13.2 电子邮件安全漏洞与保护	359
11.4.1 计算机取证技术	321	13.2.1 匿名转发	359
11.4.2 入侵追踪技术	324	13.2.2 电子邮件欺骗	360
11.4.3 蜜罐与蜜网	327	13.2.3 电子邮件炸弹与危害	361
复习题	330	13.2.4 E-mail 炸弹工具	361
思考题	331	13.2.5 垃圾邮件	362
上网题	331	13.3 保护 E-mail 与反垃圾邮件	363
第 12 章 信息隐藏与数字水印	332	13.3.1 PGP	363
12.1 信息隐藏技术与应用	332	13.3.2 反垃圾邮件技术	364
12.1.1 信息隐藏的概念	332	13.4 安全电子邮件系统的设计	369
12.1.2 信息隐藏的特性	334	13.4.1 安全电子邮件系统模型	369
12.1.3 信息隐藏的研究与应用	335	13.4.2 安全电子邮件系统的设计	369
12.2 数字水印技术与应用	337	13.5 电子邮件安全协议	371
12.2.1 数字水印的概念	337	13.5.1 S/MIME 协议	372
12.2.2 数字水印的特性	338	13.5.2 PGP 协议	372
12.2.3 典型的数字水印系统模型	339	13.5.3 PGP/MIME 协议	372
12.2.4 数字水印的分类	340	13.5.4 MOSS 协议	372
12.2.5 数字水印的重要参数和变量	342	13.5.5 MSP 协议	372
12.2.6 水印嵌入算法	343	13.5.6 PEM	373
12.2.7 水印检测	345	13.6 通过 Outlook Express 收发安全	
12.2.8 对数字水印的攻击	346	电子邮件	373
12.2.9 安全水印体系	348	13.6.1 获取一个私人的数字证书	373
12.2.10 数字水印的应用及产品介绍	350	13.6.2 对电子邮件进行数字签名	374
复习题	351	13.6.3 对电子邮件加密	374
思考题	352	13.6.4 管理他人的数字证书	375
上网题	352	13.7 安全电子邮件系统与产品介绍	375
第 13 章 电子邮件安全协议与系统设计	353	13.7.1 SecMail 安全电子邮件系统	376
13.1 电子邮件系统	353	13.7.2 诺方企业电子邮件安全解决	
13.1.1 电子邮件	353	方案	376
13.1.2 电子邮件地址	354	13.7.3 InterScan eManager 邮件安全	
13.1.3 邮件网关	355	管理软件	376
13.1.4 邮件格式	355	13.7.4 Trend Micro 面向企业的 ScanMail	377
13.1.5 简单邮件传送协议	357	13.7.5 赛门铁克	377

13.7.6 CipherTrust	378	15.3.2 黑客信息收集技术	417
13.7.7 IronPort	379	15.3.3 黑客攻击技术	418
13.7.8 启明星辰	379	15.3.4 黑客攻击防范	420
复习题	380	15.4 网上版权保护	421
思考题	380	15.4.1 中外版权保护发展史	421
上网题	381	15.4.2 数字产品的版权纠纷	423
第 14 章 移动通信系统安全	382	15.4.3 数字版权保护技术的分类	424
14.1 移动电子商务发展概况	382	15.4.4 版权保护软件	428
14.1.1 移动电子商务的概念	382	15.5 Apabi 数字版权保护解决方案	429
14.1.2 移动电子商务的应用分类	383	复习题	431
14.2 移动通信的发展	385	思考题	431
14.2.1 移动通信发展历程	385	上网题	431
14.2.2 无线网络框架	387	第 16 章 计算机软件综合保护方法	432
14.2.3 无线网络协议	387	16.1 计算机软件呼唤保护	432
14.3 移动电子商务安全框架	389	16.1.1 以法律手段实现软件保护	432
14.3.1 无线公钥基础框架 WPKI 体系	390	16.1.2 以技术手段实现软件保护	433
14.3.2 无线传输层安全协议 WTLS 协议	391	16.2 软件产品的法律保护手段	433
14.4 手机病毒及其防治	395	16.2.1 计算机软件的作品性特点与 版权法	433
14.4.1 手机病毒原理以及症状	395	16.2.2 计算机软件的工具性特点与 专利法	434
14.4.2 手机病毒趋势及应对策略	396	16.2.3 计算机软件的综合保护措施	435
14.5 移动电子商务安全解决方案	399	16.3 软加密保护方式	437
复习题	402	16.3.1 商品化计算机软件加密的特点	437
思考题	402	16.3.2 商品化计算机软件加密的原则	437
上网题	402	16.3.3 商品化计算机软件加解密体系的 设想	438
第 15 章 反计算机犯罪与网上版权保护	403	16.3.4 密码方式	438
15.1 计算机犯罪概述	404	16.3.5 电子注册加密方式	439
15.1.1 计算机犯罪的概念与特点	404	16.3.6 电话授权的加密方法	440
15.1.2 计算机犯罪分子的类型	405	16.4 软盘加密方式	441
15.1.3 计算机犯罪的基础方法和手段	405	16.4.1 软盘加密方式简介	441
15.2 反计算机犯罪	406	16.4.2 软盘加密方式原理及种类	442
15.2.1 计算机犯罪的侦察与取证	406	16.4.3 软盘加密方式的特点	442
15.2.2 计算机犯罪的防范和对策	410		
15.3 黑客文化	415		
15.3.1 黑客渊源	415		

16.4.4 软盘软加密方式的优缺点	443	16.11.4 星之盾	460
16.4.5 光盘加密方式	443	复习题	461
16.5 反动态跟踪技术	444	思考题	461
16.5.1 概念	444	上网题	461
16.5.2 修改动态调试环境需要的 中断向量	444	第 17 章 系统评估准则与安全策略	462
16.5.3 封锁键盘输入	445	17.1 安全标准的简要发展史	462
16.5.4 封锁屏幕显示	445	17.2 可信计算机系统评估准则	462
16.5.5 修改堆栈指令	445	17.3 欧洲信息技术安全评估准则	463
16.6 硬加密保护方式	445	17.4 加拿大可信计算机产品评估准则	464
16.6.1 软盘的硬加密法	445	17.5 美国联邦信息技术安全准则	465
16.6.2 增加 ROM 片加密技术	446	17.6 国际通用准则	466
16.6.3 针孔加密技术	447	17.7 中国测评认证标准	466
16.6.4 软盘硬加密方式的优缺点	447	17.7.1 测评认证制度	467
16.7 软件狗加密方式	448	17.7.2 安全产品控制	467
16.7.1 硬件钥匙的结构分析	448	17.7.3 中国开展信息安全测评认证的 紧迫性	467
16.7.2 软件锁的设计思路	448	17.7.4 测评认证的标准与规范	467
16.7.3 用 C 语言实现软件加密	449	17.7.5 中国测评认证标准与工作体系	468
16.7.4 软件狗加密方式的优点	449	17.8 安全策略	470
16.8 软件狗与指纹识别技术相结合的 保护方法	449	17.8.1 制定安全策略原则	470
16.8.1 新软件加密方法的可行性研究	449	17.8.2 制定安全策略的目的和内容	472
16.8.2 新方法与传统方法的比较	453	17.8.3 制定实施方案	473
16.9 基于数字签名的软件保护方案	454	17.8.4 安全策略的层次	474
16.9.1 数字签名与软件保护	454	17.9 安全管理的实施	475
16.9.2 基于代理签名的软件鉴别	455	17.9.1 安全管理的类型	475
16.10 软件水印	456	17.9.2 安全管理的行政原则	475
16.10.1 软件水印的分类	456	17.9.3 安全管理基础	476
16.10.2 软件水印算法	457	17.9.4 数据管理	476
16.10.3 软件水印系统的攻击	458	17.10 系统备份和紧急恢复	479
16.11 计算机软件保护产品介绍	458	17.10.1 系统备份	479
16.11.1 SafeNet	459	17.10.2 数据备份	481
16.11.2 阿拉丁	459	17.10.3 紧急恢复	484
16.11.3 深思洛克	460	17.11 审计与评估	485
		17.11.1 安全审计	485

17.11.2 网络安全评估·····	486	管理制度·····	507
复习题·····	488	18.4.1 计算机信息系统安全专用产品的 有关概念·····	507
思考题·····	489	18.4.2 计算机安全专用产品管理的一般 原则·····	509
上网题·····	489	18.4.3 计算机信息系统安全专用产品的 分类·····	510
第 18 章 计算机信息系统安全保护制度 ·····	490	18.4.4 计算机安全专用产品的管理制度·····	513
18.1 安全等级保护制度·····	492	18.5 计算机事件报告制度·····	516
18.1.1 信息安全等级·····	492	18.5.1 认真执行计算机事件报告制度·····	516
18.1.2 计算机信息系统的安全等级·····	494	18.5.2 计算机安全事件报告内容·····	517
18.1.3 计算机安全等级·····	494	复习题·····	519
18.1.4 物理环境安全等级·····	497	思考题·····	519
18.2 有害数据防治管理制度·····	500	上网题·····	519
18.3 信息流管理制度·····	502	附录一 黑客与计算机安全站点介绍 ·····	520
18.3.1 信息流管理控制的有关概念·····	502	附录二 电子商务安全期刊介绍 ·····	522
18.3.2 计算机信息网络国际联网安全 保护管理办法·····	504	参考文献 ·····	524
18.3.3 计算机信息媒体进出境申报制度·····	506		
18.4 计算机信息系统安全技术和专用产品			

第 1 章 电子商务安全的现状与趋势

电子商务已成为业界的新热点,但我国大多数电子商务系统只是在一般 Web 站点的基础上增加了简单的产品目录和订购单。这种比较初级的电子商务系统因还没有与内部网连接,也就没有涉及太多的安全问题。然而,随着信息化进程的深入,它们即将被新的、真正的电子商务系统所取代,即 Web 站点与公司的后端数据库系统相连接,这样就可以向客户提供有关产品的库存、发货情况以及账款状况的实时信息。这种充分集成的电子商务系统可以向客户提供只能通过 Web 才能得到的重要服务,同时还可以帮助商家实现业务处理的流水化。由于这种新的完整的电子商务系统可以将内部网与 Internet 连接,使小到本企业的商业机密、商务活动的正常运转,大至国家的政治、经济机密都将面临网上黑客与病毒的严峻考验。这样,安全问题便成了电子商务系统的首要问题。

目前,影响 Internet 交易的最大阻力是交易安全,使用者担心在网络上传输的信用卡及个人资料信息被截取,或是不幸遇到“黑店”,信用卡资料被不正当运用。另一方面,特约商店也担心收到的是被盗用的信用卡号码,或是交易不认账等,还有可能因网络不稳定或是应用软件设计不良导致被黑客侵入所引发的损失。由于在消费者、特约商店,甚至与金融单位之间的权责关系还未理清,以及每一家电子商场或商店的支付系统所使用的安全控管机制不一致等问题,都会造成使用者有无所适从的感觉。以上种种令不少对 Internet 网有兴趣的购物者因担忧安全而犹豫不前。因此,电子商务顺利开展的核心和关键问题是保证交易的安全性,这是网络交易的基础,也是电子商务技术的难点所在。

本章着重介绍电子商务系统安全的基本概念、安全性的基本要求、国内外电子商务安全技术的发展和实际应用状况。

1.1 电子商务安全概述

1.1.1 电子商务安全结构与要求

1. 安全性定义

在给安全性下一个详细的定义前,通常需要先定义一系列新的术语。为了理解本章所述各种安全性的含意,有必要先了解以下术语:

(1) 密码安全

通信安全的最核心部分,由技术上提供强韧的密码系统及其正确应用来实现。

(2) 计算机安全

一种确定的状态,使计算机化数据和程序文件不致被非授权人员、计算机或其他程序所访问、获取或修改。安全的实施可通过限制被授权人员使用计算机系统的物理范围、利用特殊(专用)软件和将安全功能构造于计算机操作规程中等方法来实现。

(3) 网络安全

包括所有保护网络的措施:物理设施的保护、软件及职员的安全,以防止非授权的访问、偶发或蓄意的常规手段的干扰或破坏。因此,有效的安全措施是技术与人事管理的一种均衡或合理配合。

(4) 信息安全

保护信息财富,使之免遭偶发的或有意的非授权泄露、修改、破坏。

以上几类安全性之间的关系,可用图 1.1 所示的安全环表示。

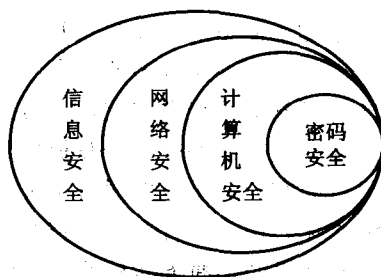


图 1.1 安全环

2. 电子商务安全的基本要求

表 1.1 列出了电子商务所需的七种安全性要求。其中,保密性、完整性和不可否认性最为关键。

表 1.1 网络安全性要求

术 语	定 义
保密性	保障个人的、专用的和高度敏感数据的机密
认证性	确认通信双方的合法身份
完整性	保证所有存储和管理的信息不被篡改
可访问性	保证系统、数据和服务能被合法地访问
防御性	能够阻挡不希望的信息或黑客
不可否认性	防止通信或交易双方对已进行业务的否认
合法性	保证各方的业务符合可适用的法律和法规

1.1.2 电子商务安全案例与分析

近年来,随着网络技术和电子商务的迅猛发展,人们在网络上购买书、日用品、计算机或是进行房产交易、股票炒作、资金运作等活动剧增,随之而来的网络安全问题日益引起人们的关注。

2004 年 9 月,浙江某大学计算机系学生谢某因在网上开设“91See”影院网站并提供