

高等学校电子商务系列教材

电子商务 安全与保密

祁 明 主编



高等教育出版社

高等学校电子商务系列教材

电子商务安全与保密

祁 明 主编
张 凌 宋全芳 曹妮妮 编著

高等教育出版社

内容摘要

本书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18章,涉及的范围比较广泛,其主要内容有:电子商务安全的现状与趋势、信息加密技术、数字签名技术、身份认证与访问控制、密钥管理与数字证书、WWW安全、防火墙、计算机病毒的防治、安全协议、系统入侵检测、信息隐藏与数字水印、电子邮件安全、移动通信安全、反计算机犯罪、计算机软件保护、系统与产品评估和系统安全保护制度的建立。

本书可作为高等院校计算机、通信、经济信息管理及相关专业本科生或研究生的电子商务教材,也可供从事电子商务研究和应用开发人员学习参考。

图书在版编目(CIP)数据

电子商务安全与保密/祁明主编. —北京:高等教育出版社,2001.7

ISBN 7-04-009279-4

I. 电... II. 祁... III. ①电子商务—安全技术
②电子商务—保密 IV. F713.36

中国版本图书馆 CIP 数据核字(2001)第 26164 号

责任编辑 董建波 封面设计 王凌波 责任印制 杨 明

电子商务安全与保密
祁 明 主编

出版发行 高等教育出版社

社 址 北京市东城区沙滩后街 55 号

电 话 010-64054588

网 址 <http://www.hep.edu.cn>

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

邮政编码 100009

传 真 010-64014048

经 销 新华书店北京发行所

印 刷 中国农业出版社印刷厂

开 本 787×1092 1/16

印 张 28.25

字 数 690 000

版 次 2001 年 7 月第 1 版

印 次 2001 年 7 月第 1 次印刷

定 价 28.00 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

前 言

自有计算机网络以来,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,由此带来的诸如高科技犯罪、机密泄露、黑客入侵、病毒侵扰等问题,其危害之严重、手段之高超,令人惊异。

据美国 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,国内有关专家曾对国内多家网站的安全性做了测试,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。遭到黑客攻击的网站有很多,如,新浪网、中国公众多媒体信息网、国家统计局网站等。总之,互连网与电子商务的安全问题已经引起了人们的恐慌,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。

本书第 1~18 章由华南理工大学祁明博士编写并担任主编,华南理工大学张凌教授和广东省保密局宋全芳研究员参与了系统安全管理和安全产品介绍等章节部分内容的编写,华南理工大学图书馆曹妮妮女士提供并翻译了许多有参考价值的外文资料,华南理工大学计算机系的研究生林卓声、许伯桐、刘迎风等人参与了本教材书稿的校对和其他文字处理工作。

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,又介绍目前已经实用的具体技术;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其来源的广泛性、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的不够全面。另外,本书编写虽力求完美,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。

本书是作者在华南理工大学计算机工程与科学系以及电子商务学院多年教学和研究的基础上写成的。作者在写作过程中参阅了大量的国内外资料。再此,谨向书中提到和参考文献列出的所有作者表示衷心的感谢。本书的编写和有关研究工作还分别得到了 IBM 中国有限公司大学合作部和广东省自然科学基金的资助,也得到了高等教育出版社的热情支持,在此一并表示感谢!

编者

2001 年 6 月于广州



徐如人教授, 无机化学家, 1991年当选为中国科学院院士。1932年2月生于浙江上虞县。1952年毕业于上海交通大学, 任教于吉林大学化学系, 历任教授、化学系主任、合成与催化研究所所长。长期从事无机合成化学、分子筛化学与分子工程学领域的研究与教学。现任《高等学校化学学报(中英文版)》、《无机化学学报》、《应用化学》副主编以及第三届国家自然科学基金委员会委员;《J. Materials Chem.》、《Microporous Materials》、《Catalysis Letters》、《Topics in Catalysis》、《Inorg. Chem. Commun.》与《Microporous and Mesoporous Materials》等国际性专业杂志的顾问编委。1998年当选为国际分子筛协会(IZA)执行理事

目 录

第一章 电子商务安全的现状与趋势	1	2.3.7 中国剩余定理	34
1.1 电子商务安全概述	1	2.3.8 二次剩余	34
1.1.1 电子商务安全结构与要求	1	2.3.9 勒让德符号	35
1.1.2 电子商务安全现状	2	2.3.10 雅可比符号	35
1.1.3 网络安全十大不稳定因素	3	2.3.11 Blum 整数	36
1.1.4 触发电子商务安全问题的原因	5	2.3.12 生成元	36
1.1.5 安全问题制约电子商务的发展	5	2.3.13 有限域	37
1.2 电子商务安全隐患与防治措施	8	2.3.14 $GF(p^m)$ 上的计算	37
1.2.1 安全隐患	8	2.4 因子分解	38
1.2.2 防治措施	11	2.4.1 因子分解算法	38
1.3 国外信息安全防范措施	20	2.4.2 模 N 的平方根	39
1.3.1 各国政府解决安全问题的举措	20	2.5 素数生成元	39
1.3.2 新加坡与韩国打击网络犯罪	21	2.5.1 Solovag - Strassen 方法	40
1.3.3 西方国家对付网络犯罪的措施	22	2.5.2 Rabin - Miller 方法	40
1.3.4 美国强调政府与企业的合作	22	2.5.3 Lehmann 方法	41
1.3.5 日本加强反黑客技术	23	2.5.4 强素数	41
1.3.6 加强网络安全的十条建议	24	2.6 有限域上的离散对数	42
思考题	24	2.6.1 离散对数基本定义	42
第二章 信息论与数学基础	25	2.6.2 计算有限群中的离散对数	42
2.1 信息论	25	思考题	42
2.1.1 熵和不确定性	25	第三章 信息加密技术与应用	44
2.1.2 语言信息率	26	3.1 网络通信中的加密方式	45
2.1.3 密码体制的安全性	26	3.1.1 链路 - 链路加密	45
2.1.4 惟一解距离	27	3.1.2 节点加密	45
2.1.5 信息论的应用	27	3.1.3 端 - 端加密	46
2.1.6 混乱和散布	28	3.1.4 ATM 网络加密	46
2.2 复杂性理论	28	3.1.5 卫星通信加密	47
2.2.1 算法的复杂性	28	3.1.6 加密方式的选择	47
2.2.2 问题的复杂性	29	3.2 分组加密与高级加密标准	48
2.2.3 NP - 完全问题	30	3.2.1 分组密码与 DES	48
2.3 数论	31	3.2.2 21 世纪高级加密标准	52
2.3.1 模运算	31	3.3 公钥加密体制	57
2.3.2 素数	32	3.3.1 RSA 加密体制	57
2.3.3 最大公因子	32	3.3.2 背包加密体制	59
2.3.4 取模数求逆元	33	3.3.2 ElGamal 加密体制	60
2.3.5 费马小定理	33	3.4 复合型加密体制 PGP	61
2.3.6 欧拉函数	33	3.4.1 完美的加密 PGP	61

3.4.2 PGP 的多种加密方式	61	5.1.4 SecurID 卡系统	88
3.4.3 PGP 的广泛使用	61	5.2 个人特征识别	88
3.4.4 PGP 商务安全方案	63	5.2.1 机器识别	89
3.5 微软的 CryptoAPI	64	5.2.2 系统误差	89
3.6 对加密系统的计时入侵	66	5.3 签名识别法	89
3.7 加密新法:椭圆曲线加密	66	5.3.1 记录书写过程的技术	90
3.8 加密产品与系统简介	67	5.3.2 签名识别法的使用	90
思考题	68	5.4 指纹识别技术	90
第四章 数字签名技术与应用	69	5.4.1 指纹识别技术简介	91
4.1 数字签名的基本原理	69	5.4.2 指纹取像的几种技术和特点	92
4.1.1 数字签名的要求	69	5.4.3 指纹识别系统中软件和固件	93
4.1.2 数字签名与手书签名的区别	69	5.4.4 指纹识别技术的优缺点	93
4.1.3 数字签名的分类	69	5.4.5 指纹识别技术的可靠性 问题	94
4.1.4 使用数字签名	70	5.4.6 指纹识别技术的应用系统	94
4.2 RSA 签名	71	5.4.7 指纹识别技术的一些应用	94
4.3 ElGamal 签名	71	5.5 语音识别系统	95
4.4 盲签名及其应用	72	5.6 视网膜图像识别系统	95
4.4.1 盲消息签名	72	5.7 识别过程	96
4.4.2 盲参数签名	73	5.7.1 引入阶段	96
4.4.3 弱盲签名	74	5.7.2 识别阶段	96
4.4.4 强盲签名	74	5.7.3 折衷方案	96
4.5 多重签名及其应用	75	5.8 身份识别技术的评估	97
4.6 定向签名及其应用	75	5.8.1 Mitre 评估研究	97
4.6.1 ElGamal 型定向签名	75	5.8.2 语音识别	98
4.6.2 MR 型定向签名方案	76	5.8.3 签名识别	98
4.7 代理签名及其应用	76	5.8.4 指纹识别	99
4.7.1 代理签名的基本要求	77	5.8.5 系统间的比较	99
4.7.2 双重安全代理签名方案	77	5.9 身份识别系统的选择	100
4.8 美国数字签名标准(DSS)	78	5.10 访问控制	100
4.8.1 关注 DSS	78	5.10.1 访问控制的概念与原理	100
4.8.2 NSA 的发展与作用	79	5.10.2 访问控制策略及控制 机构	101
4.8.3 DSS 的进展	80	5.10.3 访问控制措施	102
4.9 世界各国数字签名立法状况	81	5.10.4 信息流模型	104
4.10 数字签名应用系统与产品 介绍	82	5.11 访问控制类产品	105
思考题	84	思考题	108
第五章 身份认证与访问控制	85	第六章 密钥管理与数字证书	109
5.1 口令识别法	85	6.1 密钥的结构与分配	109
5.1.1 用户识别方法分类	85	6.1.1 密钥管理概述	109
5.1.2 不安全口令的分析	86	6.1.2 密钥的组织结构	110
5.1.3 一次性口令	87	6.1.3 多层密钥体制	111

6.1.4 密钥的连通与分割	113	7.3.1 Java 的功能	160
6.1.5 密钥的自动分发	115	7.3.2 Java 环境的主要功能特性	162
6.2 第三方密钥托管协议	119	7.3.3 安全性	164
6.2.1 密钥托管的发展	120	7.3.4 Java 与 JavaScript	165
6.2.2 密钥托管的应用	120	7.3.5 JavaScript 的安全性的问题	166
6.2.3 密钥托管的组成	121	思考题	167
6.2.4 美国密钥托管技术标准	121	第八章 防火墙的构造与选择	168
6.2.5 密钥托管的可行性分析	122	8.1 防火墙概述	168
6.2.6 密钥托管存在的问题	122	8.1.1 什么是防火墙	168
6.3 公钥基础设施与认证链	124	8.1.2 防火墙的基本类型	169
6.3.1 数字证书的基本概念	124	8.2 防火墙相关概念与定义	169
6.3.2 公钥基础设施的要求	126	8.2.1 一些有关的定义	169
6.3.3 认证机构间的关系结构	126	8.2.2 包过滤	170
6.3.4 证书政策	128	8.2.3 代理服务	171
6.3.5 认证通道的查找与确认	129	8.2.4 多种技术的混合使用	172
6.3.6 公钥基础设施案例	129	8.3 防火墙的基本体系结构	173
6.4 安全认证机构与系统介绍	130	8.3.1 双宿主主机结构	173
6.4.1 Netscape Certificate Server	130	8.3.2 主机过滤结构	174
6.4.2 VeriSign 数字凭证的 申请操作	131	8.3.3 子网过滤结构	175
6.4.3 国内外其他数字凭证 颁发机构	136	8.4 防火墙体系结构的 种种变化和组合	177
思考题	136	8.4.1 使用多堡垒主机	177
第七章 TCP/IP 服务与 WWW 安全	138	8.4.2 合并内外部路由器	178
7.1 TCP/IP 服务	138	8.4.3 合并堡垒主机与外部路由器	179
7.1.1 远程登录	138	8.4.4 将堡垒主机与内部路由器 合并	179
7.1.2 传输协议	139	8.4.5 采用多内部路由器结构	180
7.1.3 电子邮件	141	8.4.6 使用多外部路由器	183
7.1.4 Usenet 新闻组	141	8.4.7 多参数网络结构	183
7.1.5 万维网	142	8.4.8 双宿主主机加子网过滤	184
7.1.6 域名服务	143	8.5 内部防火墙	184
7.1.7 时间服务	143	8.5.1 实验网络	184
7.1.8 网络文件系统	144	8.5.2 低保密度网络	185
7.2 WWW 的安全	148	8.5.3 高保密度网络	185
7.2.1 HTTP 协议	148	8.5.4 联合防火墙	186
7.2.2 WWW 服务器的安全漏洞	151	8.5.5 共享参数网络	186
7.2.3 CGI 程序的安全性问题	152	8.5.6 内部防火墙堡垒主机的选择	187
7.2.4 Plug-in 的安全性	157	8.6 防火墙的选择与实施	187
7.2.5 SSL 的安全性	158	8.6.1 防火墙的局限性	187
7.2.6 ActiveX 的安全性	158	8.6.2 怎样选择合适的防火墙	188
7.2.7 Cookies 的安全性	159	8.5.3 防火墙的测试	189
7.3 Java 的安全性	159	8.5.4 防火墙的安装	189

8.5.5 防火墙的安装与维护	190	10.1.1 下一代 IP	222
8.7 防火墙的未来	190	10.1.2 安全关联	224
8.8 防火墙产品介绍	191	10.1.3 安全鉴别	224
思考题	193	10.1.4 密封保密负载(ESP)	225
第九章 计算机病毒及其防治技术	194	10.1.5 鉴别与保密的综合	227
9.1 计算机病毒的概念	194	10.2 安全套接层协议(SSL)	227
9.1.1 病毒的产生	194	10.2.1 SSL 协议	228
9.1.2 病毒的特征	195	10.2.2 SSL 提供的安全服务	228
9.1.3 病毒的分类	195	10.2.3 用 SSL 对服务器进行验证	229
9.1.4 病毒的类型	197	10.2.4 SSL 的加密体制	229
9.2 计算机病毒的分析	199	10.3 安全电子交易协议(SET)	230
9.2.1 病毒的破坏现象	200	10.3.1 SET 概述	230
9.2.2 病毒的传播途径	200	10.3.2 SET 的安全机制	233
9.2.3 病毒的表现症状	200	10.3.3 证书发行 (Certificate Issuance)	236
9.3 计算机病毒的防治	201	10.3.4 购物类型	237
9.3.1 思想方面的防范	201	10.3.5 支付处理 (Payment Processing)	238
9.3.2 管理方面的防范	202	10.3.6 SSL 与 SET 协议的比较	245
9.3.3 使用方面的防范	202	思考题	249
9.3.4 清除病毒的原则	203	第十一章 系统入侵的鉴别与防御	250
9.4 网络病毒防治技术	204	11.1 系统入侵的分析	250
9.4.1 网络病毒的特点	204	11.1.1 入侵技术的分类	250
9.4.2 基于网络安全体系的防毒 管理措施	205	11.1.2 安全缺陷的分类	251
9.4.3 基于工作站与服务器的 防毒技术	206	11.1.3 入侵结果的分类	251
9.4.4 网络病毒清除方法	208	11.2 最简单的黑客入侵	252
9.4.5 怎样分辨出真正的病毒警告	208	11.3 TCP 协议劫持入侵	253
9.5 防病毒和杀毒软件	209	11.4 嗅探入侵	254
9.5.1 防病毒软件	209	11.5 主动的非同步入侵	254
9.5.2 常见的杀毒软件	210	11.5.1 非同步后劫持入侵	254
9.6 典型病毒危害与清除	213	11.5.2 TCP ACK 风暴	255
9.6.1 CIH 病毒	213	11.5.3 前期非同步入侵	256
9.6.2 宏病毒	215	11.5.4 空数据非同步入侵	256
9.6.3 大麻病毒	218	11.5.5 Telnet 会话入侵	256
9.6.4 黑色星期五病毒	218	11.5.6 进一步了解 ACK 风暴	257
9.6.5 米开朗基罗病毒	218	11.5.7 检测及其副作用	257
9.6.6 浪漫的“爱虫”病毒	219	11.5.8 防卫非同步后劫持入侵	258
9.7 防病毒、杀病毒软件介绍	220	11.6 另一种嗅探——冒充入侵	258
思考题	221	11.7 关于作假的详述	259
第十章 安全通信协议与交易协议	222	11.8 检查作假	260
10.1 IP _{v6} 安全	222	11.9 防止作假	261
		11.10 关于劫持会话入侵	261

11.10.1 检测劫持会话	261	13.1.3 邮件网关	290
11.10.2 防卫劫持会话	261	13.1.4 邮件格式	291
11.11 超级连接欺骗:SSL 服务器认证中 一种入侵	261	13.1.5 简单邮件传输协议	293
11.11.1 超级链接欺骗的背景	262	13.2 电子邮件安全漏洞与攻击	294
11.11.2 实施超级链接欺骗	262	13.2.1 匿名转发	294
11.11.3 防范超级链接欺骗的方法	263	13.2.2 电子邮件欺骗	295
11.11.4 对超级链接欺骗的长远 考虑	264	13.2.3 E-mail 炸弹与危害	295
11.12 个人用户的信息安全	265	13.2.4 E-mail 炸弹工具	296
11.12.1 与硬件相关的安全防范 常识	266	13.3 保护 E-mail	297
11.12.2 个人的网络安全 防范意识	268	13.4 安全 E-mail 系统的设计	297
11.13 VPN 与企业安全防护	271	13.4.1 安全 E-mail 系统模型	298
11.14 系统监控产品简介	271	13.4.2 安全 E-mail 系统的设计	299
思考题	273	13.5 E-mail 安全协议	300
第十二章 信息隐藏与数字水印	274	13.5.1 S/MIME 协议	300
12.1 信息隐藏技术与应用	274	13.5.2 PGP 协议	300
12.1.1 信息隐藏的概念	274	13.5.3 PGP/MIME 协议	300
12.1.2 信息隐藏与数据压缩	276	13.5.4 MOSS 协议	301
12.1.3 信息隐藏的特性	276	13.5.5 MSP 协议	301
12.1.4 信息隐藏的研究与应用	276	13.6 通过 Outlook Express 收发 安全电子邮件	301
12.2 数字水印技术与应用	278	13.7 电子邮件安全产品与系统介绍	303
12.2.1 数字水印的概念	278	13.7.1 SecMail 安全电子邮件系统	303
12.2.2 数字水印的特性	279	13.7.2 诺方安全电子邮件 服务 iSafe	303
12.2.3 数字水印的分类	280	13.7.3 InterScan eManager 电子邮件 安全管理软件	304
12.2.4 数字水印的重要参数 和变量	281	13.7.4 Trend Micro 企业的 ScanMail	304
12.2.5 水印嵌入算法	282	思考题	304
12.2.6 水印的检测	285	第十四章 移动通信系统安全	305
12.2.7 Cox 的数字水印技术	285	14.1 第三代 PCS 的发展	305
12.2.8 对数字水印的攻击	286	14.2 PCS 的数据库结构与 X.509 认证 架构	306
12.2.9 数字水印的应用及 产品介绍	288	14.2.1 PCS 的数据库结构	306
思考题	288	14.2.2 X.509 认证架构及其在 PCS 中 的应用	307
第十三章 电子邮件安全协议与系统 设计	289	14.3 PCS 系统中的用户登记认证	308
13.1 电子邮件系统	289	14.3.1 系统结构	308
13.1.1 电子邮件	289	14.3.2 用户登记认证协议	309
13.1.2 电子邮件的地址	289	14.4 协议的安全性讨论	309
		14.5 手机病毒及其防治	310
		14.5.1 手机病毒欲乘 Java 强势而来	310

14.5.2 手机病毒雾里看花	311	15.6.3 S-tool	343
14.5.3 手机病毒入侵移动通信	312	15.7 版权保护综合服务体系	345
14.5.4 手机病毒的发展趋势	312	思考题	345
14.6 移动电话计费系统的安全设计	313	第十六章 计算机软件综合保护方法	347
14.6.1 业务处理和系统整体结构	313	16.1 计算机软件呼唤保护	347
14.6.2 安全问题	314	16.1.1 以法律手段来实现软件保护	347
14.6.3 针对现有系统的解决方案	316	16.1.2 以技术手段来实现软件保护	348
思考题	318	16.2 软件产品的法律保护手段	348
第十五章 反计算机犯罪与网上版权		16.2.1 计算机软件的作品性特点与	
保护	319	版权法	348
15.1 来自网络的黑色恐怖	320	16.2.2 计算机软件的工具性特点与	
15.2 计算机犯罪的概念与趋势	320	专利法	349
15.2.1 计算机犯罪的概念与特点	320	16.2.3 计算机软件的综合保护措施	350
15.2.2 计算机犯罪分子的类型	321	16.3 软加密保护方式	351
15.2.3 计算机犯罪的一般方法	322	16.3.1 商品化计算机软件加密	
15.2.4 计算机犯罪的可能趋势	322	的特点	351
15.2.5 计算机犯罪的防范对策	323	16.3.2 商品化计算机软件加密	
15.2.6 信息安全管理策略	326	的原则	351
15.2.7 分布式计算安全的常用方法	327	16.3.3 商品化计算机软件加解密	
15.2.8 计算机犯罪的技术对策	328	体系的设想	352
15.3 网上版权保护	328	16.3.4 密码方式	352
15.3.1 中外版权保护发展史	329	16.3.5 电子注册加密方式	353
15.3.2 网上版权保护的5点探问	330	16.3.6 电话授权的加密方法	353
15.3.3 呼唤新游戏规则	331	16.4 软盘加密方式	355
15.3.4 网络上版权保护的辩证思考	333	16.4.1 软盘加密方式简介	355
15.3.5 网上知识产权实话实说	334	16.4.2 软盘加密方式的原理及种类	355
15.3.6 纯数字杂志谁先支付稿酬	336	16.4.3 软盘加密方式的特点	356
15.4 互联网电子出版发行系统概述	338	16.4.4 软盘软加密方式的优缺点	356
15.4.1 对电子出版的结构和协议方面		16.4.5 光盘加密方式	357
的要求	338	16.5 反动态跟踪技术	357
15.4.2 电子出版物的安全分配系统	339	16.5.1 概念	357
15.4.3 接入控制	340	16.5.2 修改动态调试环境需要的中断	
15.4.4 文件递送和演示	340	向量	357
15.5 数字版权保护技术的分类	340	16.5.3 封锁键盘输入	358
15.5.1 锁定数据盒	341	16.5.4 封锁屏幕显示	358
15.5.2 标记数据	341	16.5.5 修改堆栈指令	358
15.5.3 版权标记需具备的特征	341	16.6 硬加密保护方式	358
15.5.4 版权保护基础设施	342	16.6.1 软盘的硬加密法	358
15.6 版权保护软件	343	16.6.2 增加ROM片加密技术	359
15.6.1 Digimare	343	16.6.3 针孔加密技术	359
15.6.2 Stego和EzStego	343	16.6.4 软盘硬加密方式的优缺点	360
		16.7 软件狗加密方式	360

16.7.1 硬件钥匙的结构分析	360	17.9.4 数据管理	383
16.7.2 软件锁的设计思路	361	17.10 系统备份和紧急恢复	386
16.7.3 用C语言实现软件加密	361	17.10.1 系统备份	386
16.7.4 软件狗加密方式的优点	362	17.10.2 数据备份	387
16.8 软件狗与指纹识别技术相结合的 保护方法	362	17.10.3 紧急恢复	390
16.8.1 新软件加密方法的 可行性研究	362	17.11 审计与评估	391
16.8.2 新方法与传统方法的比较	365	17.11.1 安全审计	391
16.9 基于数字签名的软件保护方案	365	17.11.2 网络安全评估	391
16.9.1 数字签名与软件保护	366	17.12 网络安全解决方案介绍	394
16.9.2 基于代理签名的软件鉴别	366	思考题	395
16.10 计算机软件保护产品介绍	367	第十八章 计算机信息系统安全	
16.10.1 美国圣天诺	367	保护制度	396
16.10.2 北京彩虹金天地	368	18.1 安全等级保护制度	398
16.10.3 深思洛克	368	18.1.1 信息安全等级	398
16.10.4 美国RAINBOW	368	18.1.2 计算机信息系统的安全等级	399
思考题	369	18.1.3 计算机安全等级	400
第十七章 系统评估准则与安全策略	370	18.1.4 物理环境安全等级	402
17.1 安全标准的简要发展史	370	18.2 有害数据防治管理制度	405
17.2 可信计算机系统评估准则	370	18.2.1 有害数据与计算机病毒	405
17.3 欧洲信息技术安全评估准则	371	18.3 信息流管理制度	406
17.4 加拿大可信计算机产品评估准则	372	18.3.1 信息流管理控制的有关概念	406
17.5 美国联邦信息技术安全准则	373	18.3.2 计算机信息网络国际联网 保护管理办法	408
17.6 国际通用准则	374	18.3.3 计算机信息媒体进出境申报 制度	410
17.7 中国测评认证标准	375	18.4 计算机信息系统安全技术和专用 产品管理制度	411
17.7.1 测评认证制度	375	18.4.1 计算机信息系统安全专用产品的 有关概念	411
17.7.2 安全产品控制	375	18.4.2 计算机安全专用产品管理的 一般原则	412
17.7.3 中国开展信息安全测评认证的 紧迫性	375	18.4.3 计算机信息系统安全专用 产品的分类	413
17.7.4 测评认证的标准与规范	376	18.4.4 计算机安全专用产品的管理 制度	415
17.7.5 中国测评认证标准 与工作体系	376	18.5 计算机案件报告制度	418
17.8 安全策略	378	18.5.1 认真执行计算机案件报告制度	418
17.8.1 制定安全策略原则	378	18.5.2 计算机安全事件报告内容	419
17.8.2 制定安全策略的目的和内容	379	思考题	420
17.8.3 制定实施方案	381	附录	421
17.8.4 安全策略的层次	381	参考文献	438
17.9 安全管理的实施	382		
17.9.1 安全管理的类型	382		
17.9.2 安全管理的行政原则	383		
17.9.3 安全管理基础	383		

第一章 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,但我国现有的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 e-business 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。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袭击的严峻考验。这样,安全问题便成了电子商务系统的首要问题。

目前,Internet 上影响交易最大的阻力是交易安全,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,甚至于金融单位之间,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都不尽相同,都造成使用者有无所适从的感觉。以上种种,令不少有兴趣的 Internet 网上购物者因担忧而犹豫不前。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,这是网上交易的基础,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,电子商务安全技术的发展状况和实际应用。

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

在给安全性下更详细的定义时,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、计算机或其程序访问、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、破坏或处理能力的丧失。

以上几类安全性之间的关系,可用如图 1.1 所示的安全环表示:

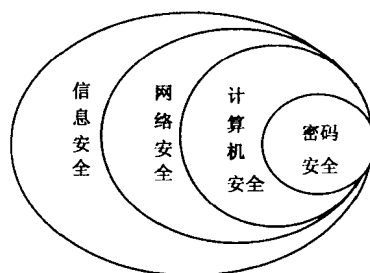


图 1.1 安全环

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 7 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	保持个人的、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、数据和服务能由合法的人员访问
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 电子商务安全现状

2000 年 2 月 7 日、8 日、9 日这三天,美国许多著名的网站先后遭到互联网历史上最严重的计算机黑客攻击,在美国社会引起了强烈震动。

黑客 3 天来的袭击,造成的间接和直接经济损失达 10 亿美元。2 月 7 日,除了免费电子邮件等三个站点未受影响外,雅虎的大部分网络服务陷于瘫痪。雅虎是全球第二大搜索引擎网站,每天被浏览页次达 4.65 亿次,其股市价值达 930 亿美元。8 日上午,先是当天股市的网络销售公司购买网站死机,再是网上电子拍卖网站电子港湾、网上书店及商品销售的亚马逊网站告急。电子港湾的注册用户达 1 000 万,是每月浏览达 15 亿次的网上拍卖网站,8 日下午 6 时,商品买卖一度被停止数小时。当晚,美国有线电视新闻网宣布,其网站因负荷超载,从下午 7 时至 8 时 45 分信息传送被阻断。2 月 9 日,电子商务网站再度遭殃,电子交易网站在股市开市前遭到持续 1 小时的攻击;信息技术公司的科技新闻网站 ZDNet 约有 70% 的内容被中断 2 小时,上网者无法接触到包括网站新闻和产品浏览等信息的信息。

美国联邦计算机案件处理中心主任大卫加诺说:“全美至少有数百台计算机受到袭击。所幸

的是,黑客并未进入这些网络内部,窃取业务和客户资料。如此众多的大型网站,特别是新兴的电子商务网站,在3天的短时间内连续遭到黑客攻击,这在因特网历史上还是第一次。”有关专家称,此事将进一步引起人们对网络安全和电子商务风险的关注。

近年来,网络技术和电子商务迅猛发展,人们在网络上进行从购买书、日用品到计算机、房产交易以及股票炒作、资金运作等活动剧增,网络安全问题成为人们一直关注的话题。电子安全的重要性已不言而喻。安全问题是电子商务推进中的最大路障。营造信誉良好、安全可靠的交易环境才能让众多的企业和消费者支持电子商务,否则消费者不信任网上交易,企业没有把握在网上营销,电子商务便只能是“水中花、镜中月”。尽管政府以及一些企业已意识到这一问题,但因为一直缺乏一个安全保护的完整概念,所以很多人在安全认知上仅限于对防火墙的了解,而防火墙只是安全保护的一个方面,绝不等于全部,这也正是实施了防火墙的网络仍有漏洞的原因所在。

为了对电子商务的安全问题有更感性的认识,我们可以分析一下黑客盗取信用卡的过程。黑客在互联网的新闻组上发布带有后门病毒的程序,并鼓励人们下载到自己的PC机上,一旦某台PC机下载了此程序,那么他就成为黑客可以侵略的对象。黑客可以浏览被入侵者PC机上的全部信息资源,可以实时地掌握被入侵者的桌面使用情况。如果被入侵者此时输入信用卡号,那么黑客就可以易如反掌地窃取到这一代码,这是信用卡被盗用的主要原因。即使你不曾在公共信息场所下载软件,你也很有可能成为无辜的受害者,因为黑客程序中的后门病毒具有很强的蔓延性,即一台PC机被感染后,病毒可通过此PC机上的地址簿向所有这些地址的PC机传播,然后按同样的方法再进一步把态势扩大。这些几何级的增长使病毒的蔓延速度极快,覆盖范围极广。所以,不经意间或许你的PC机就已成为黑客的盘中餐,而一个网上交易的网站一旦发生消费者信用卡泄露事件,那么将不会再有人去访问这个站点。因此,要使电子商务能健康、蓬勃地发展,就必须用全面的电子商务安全解决方案提供交易的信任保障。

电子商务站点上的安全漏洞会造成网上交易用户的账号、交易密码泄露,恶意攻击者可以使他人资金泄露,甚至可以使用他人资金进行网上交易。中国互联网中心于2000年2月18日发布的《中国互联网络发展状况统计报告》中关于电子商务的调查表明,安全可靠性是52.26%的电子商务用户最关心的问题。安全漏洞的存在,直接影响国内电子商务站点的信誉程度。网上交易安全性若不能得到保证,就必将影响国内电子商务的顺利发展。

电子商务的安全问题是一个涉及范围极广的社会问题,希望有越来越多的企业和个人加入到关心电子商务的行列中来,一起为开创新商务时代出力献策!

1.1.3 网络安全十大不稳定因素

1. Cookie:这种“网络小甜饼”是一些会自动运行的小程序。网络设计师使用它们来提供方便而高效的服务。但同时通过使用这些小程序,商业公司和网络入侵者能够轻易获得他人机器上的信息。

2. Java:Java作为一种技术,到底是否成功,一直备受争议。但至少有一点是肯定的,有很多利用Java的漏洞成功入侵提供网络服务的服务器的案例。

3. CGI:很难想像没有CGI技术,网站会是什么样子。可能会很难看,可能使用会不太方便,但人们留在服务器上的隐私会得到更大的保障。

4. 电子邮件病毒:超过 85% 的人使用互联网是为了收发电子邮件,没有人统计其中有多少人正使用直接打开附件的邮件阅读软件。“爱虫”发作时,全世界有数不清的人惶恐地发现,自己存放在电脑上的重要文件、不重要的文件以及其他所有文件,已经被删得干干净净。

5. 认证和授权:每当有窗口弹出,问使用者是不是使用本网站的某某认证时,绝大多数人会毫不犹豫地按下“Yes”,但如果商店的售货员问:“把钱包给我,请相信我会取出合适数量的钱付款,您说好吗?”你一定会斩钉截铁地回答:“No!”这两种情况本质上没有什么不同。

6. 微软:微软的软件产品越做越大,发现漏洞之后用来堵住漏洞的补丁也越做越大,但是又有多少普通用户真正会去下载它们?

7. 比尔盖茨:很多技术高手就是因为看不惯他,专门写病毒让微软程序出问题,攻击使用微软技术的站点。但盖茨没有受到太大影响,遭罪的是普通人。

8. 自由软件:有了自由软件,才有互联网今天的繁荣。自由软件要求所有结果必须公开,据说让全世界的程序员一起来查找漏洞,效率会很高。这要求网络管理员有足够的责任心和技术能力根据最新的修补方法消除漏洞。不幸的是,跟薪水和股权相比,责任心和技术能力显得没有那么重要。

9. ICP:人们提供私人信息,ICP 让其注册,并提供免费服务,获得巨大的注意力,以及注意力带来的风险投资。这是标准的注意力经济模式。但并没有太多人去留意有很多经济状况不太好的 ICP 把用户的信息卖掉,换钱去了。

10. 网络管理员:管理员可以得到人们的个人资料、看他们的信、知道他们的信用卡号码,如果做些手脚的话,还能通过网络控制他们的机器。人们只能期望这些人技术高超、道德高尚。

早些时候,电子商务网站 eBay、Amazon.com 和 Buy.com、门户网站 Yahoo!、新闻网站 CNN.com 等著名站点均遭到黑客攻击。联邦调查局也成为了一个类似攻击的目标,该局的网站在 2000 年 2 月 18 日被关闭了 3 个多小时,当时黑客向该网站发送了大量虚假信号使其被堵塞。

研究和教育机构 SANS(系统管理、连网及安全学会)目前公布,Internet 存在十大安全威胁。威胁名单包括那些最经常地被用来入侵计算机网络的软件弱点。SANS 学会公布这一名单旨在帮助系统管理员识别那些应当被立即清除的弱点,以挫败黑客的攻击行动。

列于名单榜首的是一些针对目录服务——明确地说就是伯克利 Internet 名称域(BIND)的攻击活动。这个学会说,在那些使用最广泛的域名服务工具中,BIND 可以让人们通过名称找到系统的位置,而不必知道具体的 IP 地址。

排名第二的是公用网关接口(CGI)程序,即一项确定在网页上运行外部程序规则的标准。许多 Web 服务器带有一些缺省安装的 CGI 程序,使它们很容易遭到黑客的攻击。

名列第三的是针对网络系统上的共享文件的入侵行动。众所周知,黑客们一直利用一项叫做“远程过程调用(RPC)”的功能,此项功能可以让一台计算上的程序与另一台计算机上的程序“交谈”。

这份报告也提到了文件共享程序、通用电子邮件程序和用户 ID 或口令访问中的 Internet 安全缺陷。该报告说,一些管理员要么忘记了一个默认口令,要么没有时间修改安装在系统上的默认口令。大多数“Demo”或“Guest”口令广为人知,使得这一弱点可能成为黑客攻击一个计算机系统的最容易的方法。

SANS 学会的研究主任 Alan Paller 说,这份十大安全威胁名单是全国各地的代表一致得

出的结果,这些代表包括联邦调查局、国家安全局、设在大学的技术研究部门和 CERT 协调中心。

1.1.4 触发电子商务安全问题的原因

日益严重的网络信息安全问题,不仅使上网企业、机构及用户蒙受了巨大经济损失,而且使国家的安全与主权面临严重威胁。要避免网络信息安全问题,首先必须搞清楚触发这一问题的原因。归纳起来,主要有以下几个方面。

(1) 黑客的攻击。由于缺乏针对网络犯罪卓有成效的反击和跟踪手段,因此黑客的攻击不仅“杀伤力”强,而且隐蔽性好。目前,世界上有 20 多万个黑客网站,其攻击方法达几千种之多。

(2) 管理的欠缺。网站或系统的严格管理是企业、机构及用户免受攻击的重要措施。事实上,很多企业、机构及用户的网站或系统都疏于这方面的管理。据 IT 界企业团体 ITAA 的调查显示,美国 90% 的 IT 企业对黑客攻击准备不足。目前,美国 75%~85% 的网站都抵挡不住黑客的攻击,约有 75% 的企业网上信息失窃,其中 25% 的企业损失在 25 万美元以上。

(3) 网络的缺陷。因特网的共享性和开放性使网上信息安全存在先天不足,因为因特网最初的设计考虑是该网不会因局部故障而影响信息的传输,但它仅是信息高速公路的雏形,在安全可靠、服务质量、带宽和方便性等方面存在着不适应性。

(4) 软件的漏洞或“后门”。1999 年底保加利亚软件测试专家发现微软网络浏览器 IE 存在安全漏洞,它可以使不怀好意的网站管理人员入侵访问者的计算机文件,随后微软公司承认这一事实。

(5) 人为的触发。基于信息战和对他国监控的考虑,个别国家或组织有意识触发网络信息安全问题。

1.1.5 安全问题制约电子商务的发展

网络这个给人们带来种种实惠的事物,怎么这么脆弱?其实,有矛才有盾,所谓“魔高一尺,道高一丈”。在已具备一定技术条件的情况下,就应该联合起来建立中国网络防御长城。

2000 年 5 月 4 日,菲律宾一名电脑高手制造出一种称为“爱虫”的电脑病毒,短短四五天内侵袭了全世界 100 多万台计算机,造成数十亿美元的损失。“CIH”、“梅丽莎”、“爱虫”等电脑病毒不断兴风作浪,一次又一次敲响了信息安全的警钟。

一台计算机、一条电话线、一个 Modem 就能发动全球信息战。随着新经济时代的来临,网络中无所不包的信息资源,方便的查询和通信方式使网络用户呈几何级数增长,新的挑战——电子攻击也随之而生。

据美国联邦调查局的调查,美国每年因为网络安全造成的经济损失超过 170 亿美元。2001 年 2 月,黑客大肆攻击雅虎、EBAY 等著名商业网站及其他各类站点,造成了直接经济损失 12 亿美元,并引起股市动荡。早在 1997 年,美国就出现了两次大的互联网络瘫痪事件,使人们感受到信息战争的巨大威胁。著名的美国联机公司因人为操作的技术上失误,使其 600 万用户陷入瘫痪 10 小时。

863 安全责任专家、上海格尔软件公司总经理吴田平博士说,从军事意义上看,信息是最精确的制导武器。它可以直接瞄准军事系统的首脑机关。除了特殊用途,军用装备采用很多民用