

信息安全系列教材

电子商务信息安全技术

主 编 代春艳 谢晓尧 辛明军 张常有 杨 艺
副主编 何希平 杨德刚 黄同愿 罗 敏 王 赞
吕秋云 杨子光



WUHAN UNIVERSITY PRESS

武汉大学出版社

图灵社区(CIP)目录

主 编 代春艳 谢晓尧 辛明军 张常有 杨 艺

2007.6

信息安全系列教材

电子商务信息安全技术

主 编 代春艳 谢晓尧 辛明军 张常有 杨 艺

副主编 何希平 杨德刚 黄同愿 罗 敏 王 赞 吕秋云 杨子光

参 编 马 骏 吴燕燕 吴海霞 王玉梅 朱东峰 胡晶晶 徐 红

苗 友 设计封面

主 编 黄 斌 设计封面

元 夏 文 金 设计封面

出版发行：武汉大学出版社 (430072 武昌 珞珈山)

电子邮箱：wupress@whu.edu.cn 网址：www.wupress.com.cn

印刷：华中理工大学印刷厂

开本：787mm×1092mm 1/16 印张：17.25 字数：408千字

版次：2007年6月第1版 2007年6月第1次印刷

ISBN 978-7-307-08288-9/F·1056



WUHAN UNIVERSITY PRESS

武汉大学出版社

版权所有 侵权必究 本书如有印刷、装订等质量问题，读者可向当地图书发行单位调换。

图书分类：F713.72

图书在版编目(CIP)数据

电子商务信息安全技术/代春艳,谢晓尧,辛明军,张常有,杨艺主编. —武汉:武汉大学出版社,2007. 6

信息安全系列教材

ISBN 978-7-307-05588-9

I. 电… II. ①代… ②谢… ③辛… ④张… ⑤杨… 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(2007)第 065540 号

责任编辑:黄金文 夏炽元

责任校对:黄添生

版式设计:支 笛

出版发行:武汉大学出版社 (430072 武昌 珞珈山)

(电子邮件:wdp4@whu.edu.cn 网址:www.wdp.com.cn)

印刷:华中科技大学印刷厂

开本:787×1092 1/16 印张:17.25 字数:408 千字

版次:2007 年 6 月第 1 版 2007 年 6 月第 1 次印刷

ISBN 978-7-307-05588-9/F·1056 定价:28.00 元

版权所有,不得翻印;凡购买我社的图书,如有缺页、倒页、脱页等质量问题,请与当地图书销售部门联系调换。

信息安全系列教材

编 委 会

主 任：张焕国，武汉大学计算机学院，教授

副主任：何大可，西南交通大学信息科学与技术学院，教授

黄继武，中山大学信息科技学院，教授

贾春福，南开大学信息技术科学学院，教授

编 委：（排名不分先后）

东 北

张国印，哈尔滨工程大学计算机科学与技术学院副院长，教授

姚仲敏，齐齐哈尔大学通信与电子工程学院，教授

江荣安，大连理工大学电信学院计算机系，副教授

姜学军，沈阳理工大学信息科学与工程学院，副教授

华 北

王昭顺，北京科技大学计算机系副主任，副教授

李风华，北京电子科技学院研究生工作处处长，教授

李 健，北京工业大学计算机学院，教授

王春东，天津理工大学计算机科学与技术学院，副教授

丁建立，中国民航大学计算机学院，教授

武金木，河北工业大学计算机科学与软件学院，教授

张常有，石家庄铁道学院计算机系，副教授

田俊峰，河北大学数学与计算机学院，教授

王新生，燕山大学计算机系，教授

杨秋翔，中北大学电子与计算机科学技术学院网络工程系主任，副教授

西 南

彭代渊，西南交通大学信息科学与技术学院，教授

王 玲，四川师范大学计算机科学学院院长，教授

何明星, 西华大学数学与计算机学院副院长, 教授
代春艳, 重庆工商大学计算机科学与信息工程学院
陈 龙, 重庆邮电大学计算机科学与技术学院, 副教授
杨德刚, 重庆师范大学数学与计算机科学学院
黄同愿, 重庆工学院计算机学院
郑智捷, 云南大学软件学院信息安全系主任, 教授
谢晓尧, 贵州师范大学副校长, 教授

华 东

徐炜民, 上海大学计算机工程与科学学院, 教授
楚丹琪, 上海大学教务处, 副教授
孙 莉, 东华大学计算机科学与技术学院, 副教授
李继国, 河海大学计算机及信息工程学院, 副教授
张福泰, 南京师范大学数学与计算机科学学院, 教授
王 箭, 南京航空航天大学信息科学技术学院, 副教授
张书奎, 苏州大学计算机科学与技术学院, 副教授
殷新春, 扬州大学信息工程学院副院长, 教授
林柏钢, 福州大学数学与计算机科学学院, 教授
唐向宏, 杭州电子科技大学通信工程学院, 教授
侯整风, 合肥工业大学计算机学院计算机系主任, 教授
贾小珠, 青岛大学信息工程学院, 教授
郑汉垣, 福建龙岩学院数学与计算机科学学院副院长, 高级实验师

中 南

钟 珞, 武汉理工大学计算机学院院长, 教授
赵俊阁, 海军工程大学信息安全系, 副教授
王江晴, 中南民族大学计算机学院院长, 教授
宋 军, 中国地质大学(武汉)计算机学院
麦永浩, 湖北警官学院信息技术系副主任, 教授
亢保元, 中南大学数学科学与计算技术学院, 副教授
李章兵, 湖南科技大学计算机学院信息安全系主任, 副教授
唐韶华, 华南理工大学计算机科学与工程学院, 教授
杨 波, 华南农业大学信息学院, 教授

王小明，暨南大学计算机科学系，教授

喻建平，深圳大学计算机系，教授

何炎祥，武汉大学计算机学院院长，教授

王丽娜，武汉大学计算机学院副院长，教授

执行编委：黄金文，武汉大学出版社计算机图书事业部主任，副编审

内 容 简 介



本书从技术角度出发，讲授构建和实施安全电子商务系统所必需的基本理论、方法和技术。主要内容包括网络安全技术、密码技术、身份认证技术、电子商务安全协议、网络安全支付技术、移动商务安全技术、电子商务安全防范体系以及一些典型的电子商务系统解决方案等。本书观点新颖，论述深入浅出，内容丰富，可读性和实践性强，特别适合作为高等学校电子商务、信息安全、管理信息系统、计算机科学技术等本科专业教材，也可作为计算机和电子商务领域研究人员和专业技术人员的参考书。



前 言



随着网络、通信技术的飞速发展,电子商务已经成为经济全球化的助推器,它改变了传统的商业运作模式,给世界范围内的商务交易活动带来了新的契机。2005年,网络经济蓬勃发展,全球网民达到 9.7 亿人,全球货物贸易额达到 10.4 万亿美元,服务贸易额达到 2.4 万亿美元,分别比 1996 年增长了近一倍。根据联合国贸发会议的统计数据,预计 2006 年世界电子商务交易额将达 12.8 万亿美元,占全球商品销售的 18%。美国的信息化建设已经进入比较高级的阶段,目前 90% 以上的企业使用了互联网,60% 的小企业、80% 的中型企业、90% 以上的大型企业已经借助互联网广泛地开展商务活动。据日本经济产业省的数据,2003~2004 年度日本企业间电子商务达 7453 亿美元,比上年增长 67.2%,其中,90% 为企业间大宗交易;面向个人电子商务达 425 亿美元,比上年增长 64.8%。电子商务在我国也取得了较快发展。中国互联网络信息中心(CNNIC)2006 年 7 月发表的第十八次统计报告显示,截止到 2006 年 6 月 30 日,我国网民人数达到了 1.23 亿人,其中经常上网购物的人达到 3 000 万人,占网民的 26%。据 2006 年 7 月 17 日在北京召开的中国电子商务应用高峰论坛上发布的消息显示,2005 年中国电子商务交易额超过了 7 000 亿元,在过去两年中,中国电子商务交易额每年保持 50%~60% 的增长速度,未来几年内仍将以较快的速度发展。

电子商务在提高商务效率、降低商务交易成本的同时,也遇到了非常严峻的挑战。电子商务自从诞生之日起,安全问题就像幽灵一样如影随形而至,成为制约其进一步发展的重要瓶颈。由于 Internet 的开放性和其他各种因素的影响,在进行电子商务(特别是网络支付)活动时,需要通过 Internet 传输消费者和商家的一些机密信息,如用户信用卡号、商家用户信息和订购信息等,而这些信息一直是网络非法入侵者或黑客的攻击目标。如何保证电子商务安全,如何对敏感信息和个人信息提供机密性保障、认证交易双方的合法身份、保证数据的完整性和交易的不可否认性等,是电子商务发展中迫切需要解决的问题。各种网络安全事故的发生,使越来越多的行家意识到,人们普遍对电子商务安全意识的淡薄和安全人才的奇缺是电子商务交易出现安全漏洞的一个非常重要的原因。因此,出现了一批与电子商务安全相关的新兴职业,如电子保安、电子商务律师、电子商务司法人员、电子商务法官、电子商务安全警察、电子商务安全员、电子商务安全策划,等等。毫无疑问,电子商务安全知识及其应用技术已成为电子商务从业人员应了解和掌握的必备知识,也成为众多学者、研究、开发人员、政府人员和管理人员关注的目标。

本书由九章组成:第 1 章主要分析电子商务面临的各种安全性威胁,讨论电子商务活动的安全需求,并系统地介绍电子商务安全架构,让读者对本书所讨论的电子商务安全技术有一个总体概要的认识。第 2 章主要探讨网络安全技术,重点介绍防火墙技术、VPN 技术、网络入侵检测技术及计算机病毒。第 3 章对经典密码技术进行了探讨。第 4 章就身份认证的一些基本概念、分类以及体系展开阐述,着重介绍了一次一密、X.509 以及 Kerberos 认证协议,同时对数字证书和认证机构进行了介绍;并对安全认证体系的实施标准中 PKI 公钥设施、



PKIX 证书实施标准以及 X.500 目录服务协议标准进行了重点介绍。第 5 章对安全电子交易协议 (Secure Electronic Transaction, SET) 和安全套接层协议 (Secure Socket Layer, SSL) 这两种安全支付协议进行详细的研究和比较。第 6 章首先介绍网络支付内涵及其安全, 分析电子商务实体各方对网络支付的安全需求和问题, 然后介绍网络支付系统安全体系, 在此基础上, 阐述发展到现在一些行之有效的安全电子商务支付机制, 最后介绍了网络银行系统的安全和两大主流支付系统的支付情况。第 7 章主要介绍了移动商务安全的基本概念、协议、安全措施等。第 8 章主要介绍了安全防范策略、系统物理安全防范、黑客防范策略、交易风险与系统灾难管理。第 9 章主要介绍 CA 公司的 eTrust 企业管理安全解决方案、3Com 公司无线网络安全解决方案的核心技术、美国联邦 PKI 解决方案以及典型电子商务系统安全解决方案: 包括××集团 B2B 电子商务系统安全解决方案、中国××银行网上银行安全建设解决方案、网上证券交易 CA 安全解决方案等。

本书具有如下特点:

(1) 实用性强。本书以技术为主线, 突出实际应用, 对照书中的方案和方法, 极易找出适合本单位、本部门需求的电子商务安全解决方案, 这对电子商务人才的培养具有重要的意义。

(2) 内容丰富。本书知识全面, 既有网络基础知识、密码基础知识、又有安全协议标准、社会安全基础设施等方方面面的电子商务安全知识, 使读者对电子商务安全有一个完整的认识。

(3) 系统性强。本书分别从电子商务网络层安全、密码层、认证层、协议层、应用层与读者探讨电子商务的安全问题及解决方案, 使读者对电子商务安全有一个深层次的理解。

(4) 内容新颖。本书跟踪了当前电子商务发展的许多热点, 如 PKI、安全电子支付、移动商务安全、电子政务安全和企业信息化安全等。

(5) 便于学习。本书每章都有本章要点和本章小结, 便于有重点和有针对性地教学和学习; 每章末附有习题, 便于读者思考; 对较复杂的概念、过程、原理等配有图解, 便于讲解和自学; 使用本书的教师可以经由出版社确认向作者提供电子讲稿。

总体上讲, 本书观点新颖, 论述深入浅出, 内容丰富, 可读性和实践性强, 特别适合作为高等学校电子商务、信息安全、管理信息系统、计算机科学技术等本科专业教材, 也可作为计算机和电子商务领域的研究人员和专业技术人员的参考书。

本书由武汉大学出版社组织编写, 经过武汉大学、重庆工商大学、贵州师范大学、重庆师范大学、重庆工学院、上海大学、中国地质大学、杭州电子科技大学等十多所院校的教授、专家讨论而定。本书第 1 章由重庆工商大学的代春艳和上海大学的辛明军编写; 第 2, 第 3 章由石家庄铁道学院的张常有、杨子光主编, 王玉梅、朱东峰、胡晶晶、徐红参编; 第 4 章由重庆工学院的黄同愿编写; 第 5 章由罗敏编写; 第 6 章由重庆工商大学的杨艺编写, 王赞、吴海霞参编; 第 7 章由上海大学的辛明军编写, 杭州电子科技大学通信工程学院的吕秋云参编; 第 8 章由重庆师范大学的杨德刚编写; 第 9 章由重庆工商大学的代春艳主编, 马骏、吴燕燕参编。在本书的统稿工作中, 贵州师范大学的谢晓尧教授、上海大学的辛明军研究员、重庆工商大学的何希平副教授、杨艺副教授等都付出了辛勤的劳动。在本书的撰写过程中, 得到了武汉大学出版社黄金文主任的鼎力支持, 得到了武汉大学计算机学院的王丽娜教授精心指点, 得到了河北工业大学的武金木教授的热心帮助, 还得到了重庆工商大学及其兄弟院校的有关领导和同事们的关心和支持, 在此一一深表谢意。本书涉及面较广, 同时因为作者



水平有限，疏漏之处在所难免，恳请读者批评指正。有关意见请发电子邮件至 daichunyan@ctbu.edu.cn，不胜感激！

作 者

2007年3月30日

目 录

第1章 绪论	1
【本章要点】	1
1.1 电子商务安全概况	1
1.1.1 电子商务安全现状	1
1.1.2 电子商务面临的安全威胁	2
1.1.3 电子商务的安全需求	5
1.2 电子商务信息安全研究的主要内容	7
1.2.1 电子商务安全概念与特点	7
1.2.2 电子商务的安全技术基础	8
1.2.3 电子商务的安全体系结构	10
1.3 电子商务安全与其他领域的交融	15
1.3.1 政务信息化	15
1.3.2 社会信息化	16
1.3.3 企业信息化	17
1.3.4 社区信息化	17
【本章小结】	18
【思考与练习】	18
第2章 网络安全技术	19
【本章要点】	19
2.1 网络安全基础	19
2.1.1 网络安全的定义	19
2.1.2 网络安全防范的内容	20
2.1.3 网络安全防范技术	20
2.1.4 网络安全关键技术	20
2.2 防火墙技术	21
2.2.1 防火墙的定义和功能	21
2.2.2 防火墙的分类	22
2.2.3 防火墙的体系结构	25
2.2.4 防火墙的基本技术	27
2.2.5 创建防火墙的步骤	27
2.3 VPN 技术	29
2.3.1 VPN 的概念	29



2.3.2 VPN 的适用特点	29
2.3.3 VPN 的基本类型	30
2.3.4 VPN 的基本技术	31
2.4 网络入侵检测	36
2.4.1 IDS 的基本模型	36
2.4.2 IDS 的分类	36
2.4.3 入侵检测系统的关键技术	38
2.5 计算机病毒及其防治	39
2.5.1 计算机病毒的一般特性	39
2.5.2 计算机病毒的分类	40
2.5.3 病毒的防范技术	41
【本章小结】	42
【思考与练习】	42
第3章 密码技术	43
【本章要点】	43
3.1 加密技术	43
3.1.1 密码算法	43
3.1.2 经典密码体制	44
3.1.3 对称密码体制	46
3.1.4 非对称密码体制	49
3.2 数字签名技术	51
3.2.1 RSA 数字签名体制	52
3.2.2 ElGamal 数字签名体制	52
3.2.3 数字签名标准 DSS	53
3.3 密钥管理技术	53
3.3.1 密钥的产生和装入	54
3.3.2 对称密码体制的密钥分配	55
3.3.3 公钥密码体制的密钥分配	56
3.3.4 密钥托管	57
【本章小结】	57
【思考与练习】	57
第4章 电子商务的安全认证体系	58
【本章要点】	58
4.1 身份认证与认证体系	58
4.1.1 身份认证的概念	58
4.1.2 身份认证的分类	60
4.1.3 身份认证体系	60
4.2 身份认证协议	61



4.2.1 一次一密机制	64
4.2.2 X.509 认证协议	65
4.2.3 Kerberos 认证协议	66
4.3 数字证书与认证机构	69
4.3.1 数字证书概述	69
4.3.2 数字认证的安全机理	70
4.3.3 数字证书的认证机构	71
4.4 安全认证体系及其实施标准	71
4.4.1 PKI 的体系	72
4.4.2 PKI 的主要功能	74
4.4.3 PKI 公钥设施标准	76
4.4.4 PKIX 证书实施标准	77
4.4.5 X.500 目录服务协议标准	77
【本章小结】	78
【思考与练习】	78
第5章 电子商务的安全服务协议	80
【本章要点】	80
5.1 SET 协议的相关技术概述	80
5.1.1 SET 支付系统协议分析	80
5.1.2 SET 的加密技术和认证技术	82
5.2 SET 证书管理及处理流程	88
5.2.1 SET 协议分析	88
5.2.2 SET 协议的证书管理	90
5.2.3 SET 处理流程	93
5.3 安全套接层协议 SSL	97
5.3.1 SSL 协议概述	97
5.3.2 SSL 握手和记录协议	99
5.3.3 SSL 协议安全性分析	103
5.4 SSL 协议的功能设计	106
5.4.1 SSL 协议的加密原理	106
5.4.2 SSL 协议的加密认证算法	108
5.4.3 SSL 协议与 SET 协议的比较	108
【本章小结】	110
【思考与练习】	110
第6章 网络支付系统及其安全	112
【本章要点】	112
6.1 网络支付内涵及其安全	112
6.1.1 网络支付的定义	112



6.1.2	网络支付的基本功能	112
6.1.3	网络支付的安全问题与需求	113
6.2	网络支付系统安全体系	115
6.2.1	网络支付系统构成	115
6.2.2	网络支付的相关安全技术及应用	117
6.2.3	安全网络支付的 SSL 与 SET 协议机制	123
6.3	安全电子商务支付工具	126
6.3.1	信用卡支付	126
6.3.2	电子支票支付	127
6.3.3	电子现金支付	129
6.3.4	微支付	131
6.3.5	目前流行的第三方网络支付工具	131
6.4	网络银行系统的安全	135
6.4.1	网络银行体系结构和安全需求	136
6.4.2	网络银行通信安全和客户认证	139
6.4.3	网络银行系统的其他安全问题	140
	【本章小结】	141
	【思考与练习】	142
第7章 移动商务安全		143
	【本章要点】	143
7.1	移动商务安全概述	143
7.1.1	移动商务的安全基础	144
7.1.2	移动网络的安全性能分析	148
7.1.3	移动商务安全的技术要素	153
7.2	移动商务安全的技术标准	154
7.2.1	移动商务安全的技术(协议)	155
7.2.2	无线应用协议(WAP)	156
7.2.3	Bluetooth 技术	159
7.2.4	3G 系统的安全体系	166
7.3	移动商务应用及其安全	170
7.3.1	802.11b 无线应用和安全	170
7.3.2	移动商务应用和服务现状	173
7.3.3	移动商务应用:移动钱包	176
7.4	移动商务安全的发展趋势	179
7.4.1	3G/4G 无线网络	179
7.4.2	移动服务与移动交易	182
7.4.3	移动商务的发展趋势	183
	【本章小结】	184
	【思考与练习】	184



第8章 电子商务安全防范与对策	186
【本章要点】	186
8.1 安全防范策略概述	186
8.1.1 安全防范策略	186
8.1.2 安全防范策略的实施	188
8.1.3 安全防范的关键支撑技术	189
8.1.4 存取访问控制的管理与实现	190
8.2 系统物理安全防范	191
8.2.1 机房环境安全	191
8.2.2 静电危害与电磁防护安全	193
8.2.3 硬件设施防护	195
8.2.4 系统平台安全	196
8.3 黑客防范策略	197
8.3.1 黑客起源	197
8.3.2 黑客攻击的原理和方法	197
8.3.3 黑客攻击的常用工具	200
8.3.4 黑客的防范措施	202
8.4 交易风险与系统灾难管理	204
8.4.1 风险评估与风险管理	204
8.4.2 交易风险管理对策	206
8.4.3 系统灾难恢复策略	207
8.4.4 系统安全防范与对策	208
【本章小结】	209
【思考与练习】	209
第9章 电子商务信息安全解决方案	211
【本章要点】	211
9.1 国内外公司在电子商务安全上的解决方案	211
9.1.1 CA公司的eTrust企业管理安全解决方案	211
9.1.2 3Com公司无线网络安全解决方案	215
9.1.3 美国联邦PKI解决方案	222
9.2 典型电子商务系统安全解决方案	225
9.2.1 XXB2B电子商务系统安全解决方案	225
9.2.2 中国××银行网上银行安全建设解决方案	231
9.2.3 ××网络银行安全接入解决方案	232
9.2.4 网上证券交易CA安全解决方案	235
【本章小结】	237
【思考与练习】	237



附 录.....	239
电子银行安全评估指引.....	239
中华人民共和国电子签名法.....	244
电子认证服务密码管理办法.....	248
电子认证服务管理办法.....	249
参考文献.....	254



第1章 绪 论

【本章要点】

- ◇ 电子商务面临的主要安全威胁
- ◇ 电子商务对安全的基本需求
- ◇ 电子商务安全概念
- ◇ 电子商务安全技术基础
- ◇ 电子商务安全架构
- ◇ 电子商务安全与其他领域的关系

1.1 电子商务安全概况

随着信息技术日新月异的发展,人类正在进入以网络为主的信息时代,基于 Internet 开展的电子商务已逐渐成为人们进行商务活动的新模式。越来越多的人通过 Internet 进行商务活动,电子商务的发展前景十分诱人,但随之而来的是其安全问题也变得越来越突出。如何建立一个安全、便捷的电子商务应用环境,保证整个商务过程中信息的安全性,使基于 Internet 的电子交易方式与传统交易方式一样安全可靠,已经成为在电子商务应用中所关注的重要技术问题。本章首先分析了电子商务面临的各种安全性威胁,然后讨论基于 Internet 进行的电子商务活动提出的安全需求,在此基础上,我们系统地介绍电子商务安全架构,让读者对本书所讨论的电子商务安全技术有一个总体概要的认识,最后,对电子商务安全与其他领域交融的有关情况进行了探讨。

1.1.1 电子商务安全现状

随着电子商务在全球范围内的迅猛发展,电子商务中的安全问题日渐突出,安全事故经常出现。例如,从 2000 年 2 月 7~9 日,短短三天时间内,美国几大主要网的站点遭受不明黑客攻击,其中包括著名的电子商务网站电子港湾(eBay)和亚马逊(Amazon)。在黑客开始所谓“拒绝服务(Denial of Service)”式的攻击后,亚马逊(Amazon)站点容纳顾客的能力急剧下降。数分钟后访客数量只有平时同一时段访客数量的 1.5%,大约一小时后亚马逊网站才恢复正常。据统计,三天来黑客袭击各大网站所造成的直接或间接的经济损失高达数十亿美元以上。又如,2004 年 4 月 30 日爆发的震荡电脑病毒“震荡波”横扫全世界,在中国香港的医院和政府部门,工作人员眼睁睁地看着自己的计算机不断崩溃、重启,或者速度奇慢无比;澳大利亚铁路网成千上万的旅客滞留站台;德国一些银行和邮局还被迫改用手写完成各种业务;英国海事和海岸警备局的计算机无法运转,工作人员不得不用纸条来记录事故;一家芬兰银行不得不把所有 120 家分行关闭了数个小时;德尔塔航空公司亚特兰大总部的计算机系统在近 7 小时内无法正常使用,大约 40 个航班被迫取消或延误……十多天就给全球带