信息安全系列丛书

Security of Electronic Commerce

电子商务安全

肖德琴　周权　等

高等教育出版社

信息安全系列丛书

Security of Electronic Commerce

电子商务安全

高等教育出版社

内容提要

本书全面介绍了电子商务安全保密技术的基础理论、应用安全和实际的解决方案。基础理论包括电子商务所涉及的加密、数字签名、认证技术和安全协议;应用安全包括网络安全、管理安全、公钥基础设施、移动商务安全和典型行业商务安全;实际的解决方案贯穿于应用安全的相关章节。此外,还介绍了电子商务涉及的安全标准与法规等方面的许多热点问题。

本书可作为信息安全、电子商务、计算机、金融和信息管理等专业的高年级本科生和研究生教材,也可作为上述领域的研究人员和工程技术人员的参考书。

图书在版编目(CIP)数据

电子商务安全/肖德琴等.—北京:高等教育出版社,2009.9
(信息安全系列丛书)
ISBN 978-7-04-027459-2

Ⅰ.电… Ⅱ.肖… Ⅲ.电子商务-安全技术
Ⅳ.F713.36

中国版本图书馆 CIP 数据核字(2009)第 121819 号

策划编辑 陈红英 **责任编辑** 萧 潇 **封面设计** 刘晓翔
责任绘图 尹 莉 **版式设计** 张 岚 **责任校对** 俞声佳
责任印制 陈伟光

出版发行	高等教育出版社	**购书热线**	010-58581118
社 址	北京市西城区德外大街 4 号	**咨询电话**	800-810-0598
邮政编码	100120	**网 址**	http://www.hep.edu.cn
总 机	010-58581000		http://www.hep.com.cn
		网上订购	http://www.landraco.com
经 销	蓝色畅想图书发行有限公司		http://www.landraco.com.cn
印 刷	北京印刷一厂	**畅想教育**	http://www.widedu.com
开 本	787×1092 1/16	**版 次**	2009 年 9 月第 1 版
印 张	20.25	**印 次**	2009 年 9 月第 1 次印刷
字 数	410 000	**定 价**	30.00 元

物料号 27459-00

前　言

随着信息网络技术的飞速发展，电子商务，特别是通过 Internet 进行的电子商务成为越来越多人关注的焦点。但由于 Internet 的开放性和其他各种因素的影响，在进行电子商务时，特别是在网络支付的时候，需要在 Internet 上传输一些消费者和商家的机密信息，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和黑客的攻击目标。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抵赖性等，已经成为电子商务发展的瓶颈。

纵观各种安全事故的产生，越来越多的人意识到，电子商务安全意识的普遍薄弱和安全人才的奇缺是导致安全漏洞出现的非常重要的原因。因此出现了一批与电子商务安全相关的新兴职业，例如电子保安、电子商务律师、电子商务安全策划、电子商务法官、电子商务安全警察、电子商务安全员等。毫无疑问，电子商务安全已经成为普及率极高的知识和应用技术，成为从事与电子商务有关行业的人员所必须了解和掌握的知识，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。

除第 1 章概述外，本书其余部分可分为三个层次。第一层次包括第 2～5 章，是电子商务安全基础理论篇，主要概述电子商务所涉及的典型加密算法、数字签名、认证技术和电子商务安全协议；第二层次包括第 6～11 章，是电子商务安全应用篇，主要介绍网络安全技术、管理安全、公钥基础设施、移动商务安全和典型行业安全，以及电子商务应用所涉及的安全标准与法规等方面的内容；第三层次是电子商务安全解决方案，主要介绍国内外大公司的种种实际的安全解决方案和各种安全产品的采购策略，这部分内容没有独立成章，而是贯穿于应用安全篇的各个章节，为每一个应用环节提供针对性的解决方案，具有可操作性。

本书观点新颖、内容丰富，可读性和实践性强，论述深入浅出，特别适合作为信息安全、电子商务、计算机应用、金融和信息管理等专业的教学参考书，也可作为上述相关领域的研究人员和工程技术人员的参考书。本书具有如下特点：

① 内容新颖，跟踪了当前电子商务发展的许多热点。如公钥基础设施、安全电子支付、安全管理、移动商务安全、电子政务安全、企业信息化安全和电子商务安全标准法规等。

② 知识系统全面，但避免冗杂。既有密码基础知识、网络基础知识，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概念。但是，系统性强而不复杂，对基础技术点到为止，既避免涉及复杂的密码和网络理论，又较完整地介绍了基础知识，使读者对电子商务安全有一个深层次的理解。

③ 图例丰富，对较复杂的概念、过程、原理配有图解，便于讲解和自学。

④ 章末附有讨论题，让读者回味和思考。

⑤ 实用性和可操作性强，对照书中的应用方案和方法，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。

本书由肖德琴、周权、冯健昭、罗穗萍共同编写。其中第1、7、8、9、10、11章由华南农业大学肖德琴教授编写，第2、3、4、5章由广州大学周权老师编写，第6章由华南农业大学冯健昭老师编写，第6～11章的解决方案由冯健昭和罗穗萍老师共同提供。

本书的出版得到了国家自然科学基金(10871222)和广州市教育局科技计划(08C068)的支持。在本书编写过程中，得到了武汉大学张焕国教授和王丽娜教授、华南农业大学杨波教授、林丕源教授、张明武副教授的指导和帮助。厦门大学彭丽芳教授早年提供了部分参考解决方案，华南理工大学祁明教授多次与作者讨论书稿，提供了很多最新研究资料，提出不少切实有用的建议。在此，对所有关心、支持本书出版的领导和学界同仁表示衷心的感谢！

电子商务安全技术更新和发展迅速，限于作者的学术水平，书中难免有错误与不妥之处，诚恳地希望读者批评指正。为方便讨论和交流，欢迎选用本书作参考的教师、专家和学者发送电子邮件至 deqin.x@163.com 索要电子讲稿或提出对本书的意见和建议。

作 者

2009年7月

目 录

第1章　电子商务安全概述

本章首先介绍电子商务面临的各种安全威胁和主要攻击方法。对电子商务消费者来说，他们面临着虚假订单、付款后不能收到商品、机密性丧失、拒绝服务、电子货币丢失等安全威胁。对商家来说，他们面临着系统中心安全性被破坏、竞争者的威胁、商业机密的安全、假冒的威胁、虚假订单、信用的威胁等安全威胁。然后详细地分析电子商务的六大安全要素：机密性、完整性、认证性、不可抵赖性、不可拒绝性、访问控制性。所有的安全威胁都是针对这6项内容中的某一部分，所有的安全技术都是为了保证这6项内容，全书的内容都与这六大安全需求有关。最后，介绍电子商务安全所涉及的三大基础技术、电子商务安全系统的框架体系结构和电子商务所涉及的服务规范，以及电子商务安全涉及的基础环境，包括公共政策、法规和安全技术标准等。

1.1　电子商务面临的安全威胁

电子商务(electronic commerce)是指政府、企业和个人利用现代电子计算机与网络技术实现商业交换和行政管理的全过程，是一种基于Internet、以交易双方为主体、以银行电子支付和结算为手段、以客户数据为依托的全新商务模式。它的本质是建立一种全社会的“网络计算环境”或“数字化神经系统”，以实现信息资源在国民经济和大众生活中的全方位应用。

电子商务在Internet上实现了物流、信息流、资金流三者的统一，加速了财富(信息)的流动。由于金钱的利诱，大大刺激了黑客们去冒险。不管安全技术发展到何等完善的地步，对安全的威胁永远存在。因此，对电子商务的安全威胁应该时刻警惕，认识电子商务的安全威胁以及对其进行全面防范是富有挑战性的工作。

由于Internet的全球性、开放性、无缝连通性、共享性和动态性，使得任何人都可以自由接入。电子商务在这样的环境中，时时处处受到安全威胁，这些安全威胁可分为如下几类。

1. 信息截获和窃取

如果没有采用加密措施或加密强度不够，攻击者可能通过Internet、公共电话网、搭线、电磁波辐射范围内安装截收装置或在数据包通过的网关和路由器上截获

数据等方式，获取传输的机密信息；或通过对信息的流量、流向、通信频度和长度等参数的分析，推出有用信息，如消费者的银行账号、密码以及企业的商业机密等。

2. 信息篡改

当攻击者获得了网络信息格式以后，通过各种方法和手段对网络中传输的信息进行中途修改，并发往目的地，从而破坏信息的完整性。这种破坏手段主要有3个方面。

① 篡改。改变信息流的次序或更改信息的内容，如购买商品的出货地址。

② 删除。删除某个消息或消息的某些部分。

③ 插入。在消息中插入一些信息，让接收方读不懂或接收错误的信息。

3. 信息假冒

当攻击者掌握了网络信息数据规律或解密了商务信息以后，可以假冒合法用户或发送假冒信息来欺骗其他用户，主要有伪造电子邮件和假冒他人身份两种方式。

① 伪造电子邮件。如虚开网站和商店，给用户发电子邮件，收订货单；伪造大量用户，发电子邮件，穷尽商家资源，使合法用户不能正常访问网络资源，使有严格时间要求的服务不能及时得到响应，或窃取商家的商品信息和用户信用信息。

② 假冒他人身份。如冒充领导发布命令、调阅密件；冒充他人消费、栽赃；冒充主机欺骗合法主机及合法用户；冒充网络控制程序，套取或修改使用权限、通行字、密钥等信息；接管合法用户，欺骗系统，占用合法用户的资源。

4. 交易抵赖

交易抵赖包括多个方面，如发信者事后否认曾经发送过某条信息或内容；收信者事后否认曾经收到过某条消息或内容；购买者订货后不承认；商家因价格差而不承认原有的交易等。

1.1.1 电子商务消费者面临的安全威胁

在电子商务活动中，消费者面临的威胁有：

① 虚假订单。一个假冒者可能会以客户的名字来订购商品，而且有可能收到商品，而此时客户却被要求付款或返还商品。

② 付款后不能收到商品。在客户付款后，销售商中的内部人员不将订单和钱转发给执行部门，因而使客户不能收到商品。

③ 机密性丧失。客户有可能将秘密的个人数据或自己的身份数据（如PIN、口令等）发送给冒充销售商的机构，这些信息也可能会在传递过程中被窃听。

④ 拒绝服务。攻击者可能向销售商的服务器发送大量的虚假订单来挤占它的资源，从而使合法用户不能得到正常的服务。

⑤ 电子货币丢失。可能是由物理破坏或者被偷窃导致，这通常会给用户带来不可挽回的损失。