E-COMMERCE SECURITY
THEORY AND TECHNOLOGY

电子商务安全
理论与技术

刘义春　梁英宏　编著

中国工信出版集团
電子工業出版社
PUBLISHING HOUSE OF ELECTRONICS INDUSTRY
http://www.phei.com.cn

电子商务安全理论与技术

刘义春　梁英宏　编著

電子工業出版社
Publishing House of Electronics Industry
北京 · BEIJING

内 容 简 介

本书系统介绍了电子商务研究和应用中有关的安全理论及实现技术，主要包括：密码学理论及技术、电子支付系统理论及技术、电子商务交易协议及形式化分析技术、信息系统安全理论及技术、电子商务信任管理技术等。本书力图在有限篇幅内包含必要的电子商务安全算法、协议、模型和方法，尽可能呈现一个完整的电子商务安全技术体系。

本书可作为电子商务、信息安全等专业本科生和研究生的教学参考书，也可供电子商务、信息安全、计算机应用等领域的研究人员和技术人员参考。

图书在版编目(CIP)数据

电子商务安全理论与技术 / 刘义春，梁英宏编著. —北京：电子工业出版社, 2015.5

ISBN 978-7-121-24747-7

I. ①电… II. ①刘… ②梁… III. ①电子商务－安全技术－高等学校－教材 IV. ①F713.36

中国版本图书馆 CIP 数据核字(2014)第 268565 号

策划编辑：张小乐
责任编辑：张小乐　　特约编辑：胡　雯
印　　刷：三河市鑫金马印装有限公司
装　　订：三河市鑫金马印装有限公司
出版发行：电子工业出版社
　　北京市海淀区万寿路 173 信箱　　邮编：100036
开　　本：787×1092　1/16　　印张：17.75　　字数：455 千字
版　　次：2015 年 5 月第 1 版
印　　次：2015 年 5 月第 1 次印刷
定　　价：49.00 元

凡所购买电子工业出版社图书有缺损问题，请向购买书店调换。若书店售缺，请与本社发行部联系，联系及邮购电话：(010)88254888。

质量投诉请发邮件至 zlts@phei.com.cn，盗版侵权举报请发邮件至 dbqq@phei.com.cn。

服务热线：(010)88258888。

前　言

随着互联网的广泛应用和迅速发展，电子商务交易和网络支付已经成为商业活动的重要组成部分。在电子商务系统中，客户、商家和金融机构之间使用电子支付手段（如电子现金、信用卡、微支付等）进行交易。客户把支付信息通过 Internet 安全地传送到商家、银行或相应的处理机构，并获得定购的商品或应得的服务。

由于交互环境为 Internet 等开放式网络，电子商务交易和网上支付必然面临非授权的网络分析、入侵攻击和恶意行为。为抵抗来自各方面的攻击和欺诈，必须确保电子商务交易和支付系统的安全性、健壮性和完善性。电子商务系统中的数据是最宝贵的资源，交易数据的机密性、完整性和真实性是电子商务系统成功应用的关键。密码学技术是确保交易数据机密性、完整性和真实性的最有效、最可靠的方法，也是保障电子商务安全的核心和关键技术。

作为互联网交易的流通手段，电子货币和网络支付系统必须具备独立性、安全性、匿名性、离线支付等一系列属性，必须防范伪造、复制、重复花费电子货币等欺诈行为。常见的电子支付工具，如电子现金、微支付、电子信用卡、电子支票等，皆使用专门的密码学技术来实现特定的功能属性。电子现金系统设计使用盲签名技术来实现匿名性，微支付系统使用 Hash 链、多路 Hash 或电子彩票技术来减轻计算负荷，电子支票系统则使用数字水印技术隐藏支付信息。

在电子商务中，交易双方往往互不信任，交易中的一方总担心另一方比自己更加处于优势，从而可能使自己蒙受损失。由于各交易方之间非现场当面交易，因此如何保证商务交易公平合理，避免在交易中出现欺诈行为，或消除因欺诈导致交易风险的可能性，成为电子商务研究的一个重要方面。必须对电子商务交易系统进行协议分析，分析交易协议的安全性、公平性和不可否认性。相关研究主要包括：安全电子商务协议设计，电子商务协议分析，尤其是形式化分析，等等。

电子商务系统运行于计算机软硬件平台和网络环境，电子商务的安全依赖于所运行的信息平台的安全。必须保障电子商务信息在采集、传递、存储和应用等过程中的完整性、机密性、可用性、可控性和可审计性，以实现对商务数据安全保护、信息系统运行监控、异常检测与故障恢复等功能。信息系统安全技术包括访问控制、安全审计、数据库安全、防火墙、入侵检测、VPN、容错与恢复、病毒防治、容侵、容灾等。

在电子商务应用中，真实性不是衡量用户可信与否的唯一指标，用户身份的真实性并不能蕴含交易行为的可信性。电子商务的信任可分为身份信任和行为信任两类。身份信任一般使用数据加密、身份认证、访问控制、安全协议等机制实现，而行为信任主要采用信任评价和管理技术来建模分析。行为信任研究主要体现在基于策略和凭证的信任、基于声誉的信任、信任全局模型等方面，研究方法涉及机器学习、概率论、模糊数学和粗糙集、主观逻辑，以及其他不确定数学理论。

本书在国内外现有研究成果的基础上，针对电子商务系统安全体系的各个层面、各个环节进行分析，从算法处理、协议分析、评价模型、系统实现等方面着手，论述电子商务安全的解决理论及应用技术。

本书第 1 章简要介绍电子商务的安全概况、安全体系和安全技术；第 2 章详细介绍电子商务研究和应用中相关的密码学理论与实现技术；第 3 章介绍国内外电子支付技术的一些代表性研究和应用成果，包括电子现金系统、微支付系统中使用的密码算法和协议；第 4 章主要介绍安全协议设计技术，分析几类电子商务交易协议的结构和组成，介绍安全协议的形式化分析技术；第 5 章主要论述信息系统的安全体系架构，介绍访问控制、安全审计、数据库安全、防火墙、入侵检测、VPN、容错与恢复、病毒防治、容侵、容灾等系统安全保障技术；第 6 章重点探析电子商务信任的表达、处理、推理和协商技术，介绍了几个著名的信任评估和信任管理模型。

本书由刘义春、梁英宏编写，刘义春负责全书的组织、审校和统稿。本书编写工作得到了广东省电子商务市场应用技术重点实验室的同仁们给予的大力支持，在此致以诚挚的感谢。

本书的相关研究得到教育部人文社会科学研究规划基金项目“电子商务信任评价模型研究（编号：12YJAZH079）”、广东省高科技发展专项资金项目“结合数字签名和二维条码的高安全性电子消费券技术研发（编号：2013B01040103）”的资助。

由于作者水平有限，书中难免存在疏漏和不妥之处，敬请读者批评指正。

作　者

目　录

第1章 导 引

1.1 电子商务安全概况

当今世界，网络、通信和信息技术快速发展和日益融合，Internet 在全球迅速普及，促使电子商务蓬勃发展。所谓电子商务，是指商务活动的电子化实现，即通过电子化手段来实现传统的商务活动，如网上购物、网上订票、网上缴费等。电子商务可降低商家的运营成本，提高其利润率；可以扩大商品销路，建立企业与企业之间的联系渠道，为客户提供不间断的产品信息查询和定单处理等服务。

随着电子商务时代的到来，作为电子商务重要组成部分的支付问题就显得越来越突出。电子商务的巨大潜力为多种类型的电子支付方式提供了市场需求。Internet 将全世界的付款者和收款者联系在一起，他们可能来自不同的国家、不同的商业机构或社会组织、不同的法律制度，并且习惯于不同的支付方式。消费者选用何种支付工具进行支付，买卖双方之间按照什么工作流程进行支付是电子商务的核心工程。安全的电子支付是实现电子商务的关键环节。事实上，缺乏有效的电子支付的电子商务活动将是十分有限的，而不安全的电子支付不能真正实现电子商务。

电子商务支付系统是电子商务系统的重要组成部分，它指的是消费者、商家和金融机构之间使用安全的电子手段交换商品或服务，即利用新型支付手段（包括电子现金、信用卡、智能卡等）把支付信息通过网络安全地传送到商家、银行或相应的处理机构，来实现电子支付，并获得定购的商品或应有的服务。

电子商务支付的关键问题是电子支付活动中的安全问题。常见的安全问题主要有：

① 以非法手段窃取客户订单信息、订单确认信息及银行账户、密码、个人银行识别码等客户个人信息，或对通信数据进行译码分析，使机密数据泄露给未经授权者；

② 恶意破坏、篡改或删节通信信息中的数据，取消用户订单，生成虚假信息，以破坏交易信息和支付信息的完整性；

③ 由于系统故障、网络故障等造成的电子商务交易过程中出现的通信中断或数据丢失，阻碍支付过程的正常进行；

④ 伪造身份冒充合法的交易者参与交易，以对电子商务协议进行攻击；

⑤ 协议参与者利用过时的、失效的信息重新参与电子商务交易，对电子商务协议进行重放攻击；

⑥ 协议参与者利用电子商务交易协议的漏洞让自己处于优势，而使其他参与方蒙受损失；

⑦ 协议参与方对交易行为进行抵赖，否认交易结果；

⑧ 交易方在多次交易中表现不诚信，交易能力低下，服务满意度低劣，甚至进行低价诱骗、不按约支付交货等欺诈活动。

为抵抗来自各方面的攻击和欺诈，必须确保电子商务系统的安全性、健壮性、可行性和完善性。主要措施包括：

① 保护机要数据不被非授权者泄露或窃取（数据机密性）；

② 保护机要数据不被篡改、删除（数据完整性）；

③ 保护协议参与者身份、机要数据的可鉴别性及不可伪造性（数据真实性）；

④ 使协议中一些特定信息仅在一定时间内有效，避免被日后用于攻击协议（时效性）；

⑤ 协议参与方不能否认已发送或已接受的数据（不可否认性）；

⑥ 保护诚实的协议参与方在协议执行的任何阶段都不较其他方处于劣势（公平性）；

⑦ 保护系统和网络的稳定性与可靠性，以及系统的可恢复性；

⑧ 建立较为精准的交易信任评估、监测体系，对交易方的声誉和可信任程度进行客观评测；

⑨ 建立完善、可行的安全管理体制，加强制度化安全管理和安全监管。

1.2 电子商务安全体系

1.2.1 电子商务安全体系的组成

从技术上看，电子商务安全体系分为物理安全、网络安全、主机安全、应用安全、数据安全及备份恢复 5 个组成部分。

（1）物理安全

电子商务系统的物理安全（简称物理安全）是指，为了保证电子商务系统安全可靠地运行，确保其在对交易信息进行采集、处理、传输过程中不致受到人为或自然因素的危害，使信息丢失、泄露或破坏，而对计算机、网络设备、设施、环境、人员等所采取的安全措施。

物理安全保护的目的主要是使存放计算机、网络设备的机房，电子商务系统的设备和存储数据的介质等免受物理环境、自然灾难及人为操作失误和恶意操作等各种威胁所产生的攻击。物理安全是防护电子商务系统安全的最底层，缺乏物理安全，其他任何安全措施都是毫无意义的。

物理安全主要涉及环境安全（防火、防水、防雷击等），设备和介质的防盗窃、防破坏等方面。具体包括：物理位置的选择、物理访问控制、防盗窃和防破坏、防雷击、防火、防水和防潮、防静电、温湿度控制、电力供应和电磁防护等。

（2）网络安全

网络安全为电子商务系统在网络环境下的安全运行提供支持。一方面，确保网络设备的安全运行，提供有效的网络服务；另一方面，确保在网上传输数据的保密性、完整性和可用性等。由于网络环境是抵御外部攻击的第一道防线，因此必须进行各方面的防护。对网络安全的保护，主要关注两个方面：共享和安全。开放的网络环境便利了各种资源之间的流动和共享，但同时也打开了“罪恶”的大门。因此，必须在二者之间寻找恰当的平衡点，使得在尽可能安全的情况下实现最大程度的资源共享，这是实现网络安全的理想目标。

网络安全主要关注的方面包括：网络结构、网络边界及网络设备自身安全等。具体技术内容包括：结构安全、访问控制、安全审计、边界完整性检查、入侵防范、恶意代码防范、网络设备防护等。

重要信息系统的网络安全要求对网络边界的访问控制做出更为严格的要求，禁止远程拨号访问，不允许数据带通用协议通过。网络安全审计应着眼于系统全局，做到集中审计分析，以便得到更多的综合信息。主要网络设备应对同一用户选择两种或两种以上组合的鉴别技术来进行身份认证，并且用户身份鉴别信息至少应有一种是不可伪造的，以加强对网络设备的防护。

（3）主机安全

主机系统安全是包括服务器、终端/工作站等在内的计算机设备在操作系统及数据库系统层面的安全。终端/工作站是带外设的台式机与笔记本计算机，服务器则包括应用程序、网络、Web、文件与通信等服务器。主机系统是构成电子商务系统的主要部分，其上承载着各种应用。因此，主机系统安全是保护电子商务系统安全的中坚力量。

保障主机系统安全的措施包括：身份鉴别、安全标记、访问控制、可信路径、安全审计、剩余信息保护、入侵防范、恶意代码防范和资源控制等。

（4）应用安全

通过网络、主机系统的安全防护，最终应用安全成为电子商务系统整体防御的最后一道防线。在应用层面运行着电子商务系统的基于网络的应用以及特定业务应用。基于网络的应用是形成其他应用的基础，包括消息发送、Web浏览等，可以说是基本的应用。业务应用采纳基本应用的功能以满足特定业务的要求，如电子商务、电子政务等。由于各种基本应用最终是为业务应用服务的，因此对应用系统的安全保护最终就是如何保护系统的各种业务应用程序安全运行。

应用安全主要涉及的技术包括：身份鉴别、安全标记、访问控制、可信路径、安全审计、剩余信息保护、通信完整性、通信保密性、抗抵赖、软件容错、资源控制等。

（5）数据安全及备份恢复

电子商务系统处理的各种数据（用户数据、系统数据、业务数据等）在维持系统正常运行中起着至关重要的作用。一旦数据遭到破坏（泄露、修改、毁坏），都会在不同程度上造成影响，从而危害到系统的正常运行。由于电子商务系统的各个层面（网络、主机、应用等）都对各类数据进行传输、存储和处理等，因此，对数据的保护需要物理环境、网络、数据库和操作系统、应用程序等提供支持。各个“关口”把好了，数据本身再具有一些防御和修复手段，必然将对数据造成的损害降至最小。

另外，数据备份也是防止数据被破坏后无法恢复的重要手段，而硬件备份等更是保证系统可用的重要内容，在电子商务系统中采用异地适时备份会有效地防治灾难发生时可能造成的系统危害。

保证数据安全和备份恢复主要从数据完整性、数据保密性、备份和恢复等方面考虑。

1.2.2 安全管理

安全管理是确保电子商务系统安全运行的重要组成部分。安全管理主要包括两方面：

制度和教育。其中，安全管理制度包括信息系统安全管理制度和信息系统使用单位安全管理制度。

安全管理制度包括信息安全工作的总体方针、策略、规范，各种安全管理活动的管理制度，以及管理人员或操作人员日常操作的操作规程。

安全管理制度主要包括信息安全管理制度的制定、发布、评审、修订四个方面。

电子商务系统安全管理制度涉及以下内容。

① 安全等级保护制度。包括确定各类信息的安全等级，不同人员的安全等级，以及信息系统、分系统和单个计算机及其物理环境的安全等级，并将其作为电子商务系统安全管理的基本依据。

② 有害数据防治管理制度。从制度上对包括计算机病毒在内的有害数据采取有效措施，防止其入侵和传播。

③ 安全管理规章制度。包括进入机房管理、上机人员管理、运行管理、口令管理、特殊程序管理、启动程序管理、重要数据管理、密钥管理、网络及通信设备的安全管理、为各种突然事件采取的应急技术措施的管理。

电子商务系统使用的单位安全管理制度包括如下内容。

① 建立、健全工作机制和各类人员的责任制。

② 人员的安全管理。根据电子商务系统及其所包含的信息的安全等级，确定有关人员的安全等级。

③ 运行的安全管理。包括机房、场地、操作使用、审计跟踪等方面的管理。

④ 安全技术管理。包括设备管理、备份管理、应急措施以及常备工具的安全管理等。

安全教育的目的是使从领导到技术人员，直至一般用户都能了解有关法规、制度，并掌握一定的安全基础知识。一般可以通过普法教育、定期培训、基础教育等不同形式，对不同人员进行计算机安全方面的教育。

1.3 电子商务安全技术

国际标准化组织在其《信息处理系统开放系统互连基本参考模型第 2 部分：安全体系结构》中规定了五项基本的安全服务内容：认证（Authentication）、访问控制（Access Control）、数据机密性（Confidentiality）、数据完整性（Integrative）、不可否认性（Non-Reputation）。为了保障电子商务系统的基本安全，下面一系列安全技术用于保障电子商务系统和电子商务活动的安全、可信。

（1）数据加密技术

加密技术是解决网络信息安全问题的技术核心，通过数据加密技术，可以在很大程度上提高数据传输的安全性，保证传输数据的完整性。

数据加密技术主要分为对称密码加密和公钥密码加密。数据加密按不同应用分为数据传输加密和数据存储加密。

常用的数据加密算法有很多种。古典密码算法有替代加密、置换加密，常用的对称加密算法包括 DES 和 AES，常用的非对称加密算法包括 RSA、ECC 等。目前在数据通信中使用最普遍的算法有 AES 算法、RSA 算法和 ECC 算法等。

公钥密码加密技术也可用于对消息进行数字签名。数字签名广泛用于电子商务、电子政务和其他应用信息系统中对实体身份和数据真实性的认证。

（2）数据完整性技术

数据的完整性就是防止非法篡改信息，如修改、复制、插入、删除等。在交易过程中，要确保通信双方接收到的数据和从数据源发出的数据完全一致，数据在传输和存储的过程中不能被篡改。

保障数据完整性最常用的技术是通过采用散列函数（也称密码杂凑函数）和数字签名技术实现数据完整性保护。（散列函数对所要处理的数据计算其消息摘要或称消息认证码（MAC）。而且消息摘要的长度都是固定的，无论所处理的数据有多大。）任何原始数据的改变都会在相同的计算条件下产生不同的 MAC。这样，在传输或存储数据时，附带上该消息的 MAC，通过验证该消息的 MAC 是否改变，来高效、准确地判断原始数据是否改变，从而保证数据的完整性。目前国际上广泛采用的标准散列算法有 SHA-l、MD-5。2012 年 10 月 2 日，Keccak 被选为 NIST 竞赛的胜利者，成为新一代的散列算法标准 SHA-3。

（3）认证技术

常见的认证包括 2 类：对实体身份的认证和对数据来源真实性的认证。

进行身份认证的方法主要有 2 类：基于口令的身份认证；基于公钥密码学技术的身份认证。

而对数据来源真实性的认证主要采用基于公钥密码学技术的身份认证。

信息系统中应确保口令信息在通信通道传输中和在存储期间的安全，避免被入侵者从磁盘数据文件中窃取或从通信信道截获。最常用的办法是使用加“盐”的单向散列函数对口令进行处理。

基于公钥密码学技术的数字证书认证体系又称为 PKI，PKI 系统中有一个或多个权威的 CA 机构进行数字证书签发和管理。由于数字证书上带有 CA 机构的签名，其真实性易于验证。此外，签名也可作为发送者发送信息和接收者接收信息的不可否认证据，防止实体对信息的抵赖。CA 认证机制既能实现单向认证，又能实现双向认证；既能用于实体身份的信任，又能用于通信数据的信任。

（4）防抵赖技术

不可否认性是电子商务、电子政务等系统中必须要解决的问题之一，不可抵赖服务就是防止通信中的任何一方试图对已发生的特定事件或行为的欺诈性抵赖，为此，不可抵赖服务提供不可抵赖证据的产生、收集和维护机制，用于对日后可能产生的法律纠纷进行仲裁。基本的不可抵赖服务包括：

① **发送方不可否认**（Non-Repudiation of Origin，NRO）：为消息接收方提供发送信息的证据，防止发送信息方试图否认曾经发送过消息。证据的提供者是信息发送方。

② **接收方不可否认**（Non-Repudiation of Receipt，NRR）：为发送信息方提供消息已接收的证据，防止接收方试图否认曾经收到消息。证据的提供者是信息接收方。

（5）访问控制技术

访问控制指按用户身份及其所归属的某组（域）来限制用户对信息项的访问，或限制对某些控制功能的使用。访问控制通常用于系统管理员控制用户对服务器、目录、文件等网络资源的访问。

访问控制的功能主要有：① 防止非法的主体进入受保护的系统资源；② 允许合法用户访问受保护的系统资源；③ 防止合法的用户对受保护的系统资源进行非授权的访问。

目前主要应用的访问控制类型有自主访问控制和强制访问控制两大类。

自主访问控制是指用户有权对自身所创建的访问对象（文件、数据表等）进行访问，并可将对这些对象的访问权授予其他用户和从授予权限的用户收回访问权限。

强制访问控制是指由系统（通过专门设置的系统安全员）对用户所创建的对象进行统一地强制性控制，按照规定的规则决定哪些用户可以对哪些对象进行什么操作系统类型的访问，即使是创建者用户，在创建一个对象后，也可能无权访问该对象。

（6）其他信息安全技术

除了以上几类最基本的信息安全技术以外，常用的安全技术还包括：

① 安全审计与取证技术；
② 安全扫描技术；
③ 反病毒反木马技术；
④ 入侵检测技术；
⑤ 防火墙技术；
⑥ 容错和数据备份技术；
⑦ 容灾技术；
⑧ VPN 技术；
⑨ 信息隐藏技术；
⑩ 电磁泄漏防范技术。

近几年来涌现的新技术有：

① 新一代密码学技术，包括基于格、基于特殊群运算的密码技术以及可证安全技术；
② 可信计算技术；
③ 基于 ID 的鉴别技术（IBE 认证和 CPK 认证等）；
④ 主动防御技术；
⑤ 容侵技术；
⑥ 移动 Agent 技术；
⑦ 量子密码技术；
⑧ DNA 安全技术。

1.4 电子商务系统的信任

信任是电子商务的基石，诚信机制是保障电子商务安全的重要手段。“信任”的英文单词是“Trust”，它包含了信赖、信用、责任等意义。

在大规模、开放的网络环境中，电子商务交易具有匿名性、随机性和动态性的特点。交易双方往往互不相识，仅仅通过网络来交换信息，这使得双方失去了传统商务环境下信任所依赖的基础。身份欺诈、虚假信息发布、拒绝或延期交货、质量和售后服务等问题已成为电子商务健康发展的瓶颈。电子商务信用问题已成为制约电子商务