DIANZI SHANGWU ANQUAN JISHU

电子商务安全技术

（第2版）

管有庆　王晓军　董小燕　李养群　编著

北京邮电大学出版社
www.buptpress.com

电子商务安全技术

（第 2 版）

管有庆　王晓军　董小燕　李养群　编著

北京邮电大学出版社
·北京·

内容简介

本书介绍了电子商务安全概念与构建安全电子商务的实用技术与方法，通过实例具体说明电子商务安全技术的应用与实践。重点讨论电子商务安全体系结构，密码学基础知识，信息加解密技术，电子商务安全技术，身份认证方法，电子支付系统的安全技术，移动电子商务安全，万维网安全，万维网服务安全，安全电子交易协议 SET，安全套接层协议 SSL，3-D Secure 支付协议的组成、技术及流程。

本书可用作高等院校相关专业的本科生和研究生的电子商务安全课程教材，也可以作为相关专业科研和工程技术人员的参考书。

图书在版编目(CIP)数据

电子商务安全技术/管有庆等编著. —2 版. —北京：北京邮电大学出版社，2009

ISBN 978-7-5635-2080-0

Ⅰ. 电… Ⅱ. 管… 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 140674 号

书　　名：电子商务安全技术(第 2 版)

作　　者：管有庆　王晓军　董小燕　李养群

责任编辑：李欣一

出版发行：北京邮电大学出版社

社　　址：北京市海淀区西土城路 10 号(邮编：100876)

发 行 部：电话：010-62282185　传真：010-62283578

E-mail：publish@bupt.edu.cn

经　　销：各地新华书店

印　　刷：北京源海印刷有限责任公司

开　　本：787 mm×960 mm　1/16

印　　张：17.5

字　　数：379 千字

印　　数：1—3 000 册

版　　次：2005 年 12 月第 1 版　2009 年 10 月第 2 版　2009 年 10 月第 1 次印刷

ISBN 978-7-5635-2080-0　　定　价：29.00 元

前　言

随着计算机网络与因特网技术的发展与普及，电子商务已逐步进入人们的日常生活，电子商务活动已经演变成利用因特网进行经济活动的网络经济。网络银行和网络商城等的出现，正悄悄地改变人们的购物方式、消费方式和生活观念，更方便了人们的日常生活，真正实现了“24 小时、全天候、足不出户、送货上门”的理财与消费方式。

目前，影响电子商务发展的最大障碍之一是消费者担心他们的信用卡等信息的泄密。由于电子商务中交易双方互不见面，将会产生许多传统商务模式中不会出现的安全问题，如假冒、否认、欺诈、泄密、网络黑客、通信监听和木马病毒等。因此，安全是保证电子商务过程能够顺利进行的必要条件。

不少高等院校已开设了包括“电子商务安全技术”在内的电子商务系列课程，为了配合“电子商务安全技术”课程的教学，北京邮电大学出版社组织出版了此教材。

本书共分 8 章。第 1 章和第 7.1～7.6 节由管有庆编写，第 3 章和第 5 章由王晓军编写，第 2 章和第 4 章由董小燕编写，第 6 章、第 8 章和第 7.7 节由李养群编写。下面摘要介绍各章的主要内容。

第 1 章 电子商务安全概述：简要介绍电子商务的一般流程、基本分类、体系架构、电子商务面临的威胁、电子商务的安全需求、电子商务安全体系结构、网络安全和交易安全涉及的内容。

第 2 章 密码学基础：主要介绍现代密码学的基本知识，内容包括密码学的起源与发展、密码学的基本概念和分类；现代密码学的三大密码体制，即传统对称密码体制、公钥密码体制以及近几年来兴起的量子密码体制；各类密码体制的加解密原理，经典的算法以及各自应用的场合。

第 3 章 电子商务安全技术：描述计算机安全各方面的问题，内容涵盖了程序、操作系统、数据库管理系统以及网络的安全，其中重点介绍计算机程序安全漏洞的种类和影响；描述操作系统的访问控制；研究数据库管理系统的安全。此外还介绍了网络应用程序面临的威胁以及防止网络攻击的控制措施。

第 4 章 电子商务中的认证技术：主要讲述电子商务中的认证技术，内容包括安全认证在电子商务中的重要性及两类不同的认证——实体身份认证与报文认证的概念、功能和解决方法；在认证中起关键作用的报文摘要与数字签名技术的原理、算法及其在电子商务中的应用；电子商务认证中心(CA)、公钥基础设施(PKI)以及信任机制。

第 5 章 电子商务支付系统：介绍电子支付系统的特点、安全需求以及主要安全问题；描述三类电子支付系统——电子信用卡支付系统、电子现金支付系统和电子支票支付系统；重点介绍电子支付系统的安全技术。

第 6 章 移动电子商务安全：介绍移动电子商务概念、技术及其应用、面临的安全威胁与安全需求；重点分析 WTLS 协议和基于 WPKI 的移动电子商务安全技术；最后详细介绍移动支付的模型、安全需求与安全技术以及发展趋势。

第 7 章 安全电子交易协议：介绍 SET 支付系统的成员与目标、认证中心和认证中心业务流程、SET 协议中涉及的报文摘要、数字签名、数字信封和双重签名等相关技术、SET 协议流程、安全套接层协议(SSL)以及 SET 与 SSL 的特点及性能比较；最后介绍 3-D Secure 支付协议的安全模式、架构、支付协议内容和应用实例等。

第 8 章 万维网安全及万维网服务安全：介绍万维网安全以及万维网服务安全的概念、面临的安全问题以及安全需求、万维网服务中的关键技术、万维网服务安全协议栈、主要万维网服务安全标准；最后介绍 OASIS 万维网服务安全规范和万维网服务安全架构等。

本书第 2 版在第 1 版的基础上进行了适当修订，删除了网络银行等内容，增加了移动电子商务安全、万维网安全、万维网服务安全、3-D Secure 支付协议、电子商务信任机制、识别潜在的隐蔽通道和典型的微支付系统等内容。在本书的编写过程中，编者参阅了大量参考文献，力求做到概念准确，叙述简洁，并通过实例介绍具体应用。由于编者水平所限，书中的不当之处，恳请读者指正。编者 E-mail 地址：guanyouq@njupt.edu.cn。

最后，感谢南京邮电大学郑会颂教授和沈苏彬研究员在本书第 1 版编写过程中给予的指导和帮助。

作　者

目　　录

第1章　电子商务安全概述

电子商务(Electronic Commerce/Electronic Business/E-commerce/E-business/E-trade/EC)不是一个单纯的技术概念,也不是一个单纯的商业概念,而是运用现代通信技术、计算机和网络技术进行的一种社会经济形态,其目的是通过降低社会经营成本,提高社会生产效率,优化社会资源配置,从而实现社会财富的最大化利用。

电子商务是建立在因特网上的一种商业应用,因特网使得电子商务能够以比较低廉的成本从事较大经济规模的商业活动。而电子商务是否可以蓬勃发展,进而掌握未来的经济命脉,完全依赖于安全技术的研究与发展以及安全交易架构的建立。

1.1　电子商务的基本概念

电子商务是一种新的社会经济形态,或者说电子商务是以因特网为媒介、以商品交易双方为主体、以银行电子支付与结算为手段的全新商务模式。与传统商务相比,电子商务增加了卖方的销售机会,同时也给买方提供了更多的选择。

电子商务的好处可以惠及整个社会。例如,通过因特网可以安全、迅速、低成本地实现税收、退休金、社会福利金的支付和电子商务交易等。另外,比起支票或现金支付,网上支付在因特网上更容易审计和监督,可以有效地防止欺诈和盗窃。由于具有以上优势,电子商务受到了全球的关注。

网络是人类社会劳动、生活、学习的新工具。通过影响人类通信与交往方式,间接地对传统经济领域的生产、交换、分配和消费方式产生影响,直到渗透、改造、重塑传统经济的运行模式以及社会经济价值标准与增值方式。因此,电子商务是一个泛社会化的概念,电子商务的发展是一个从基础应用入手,循序渐进地推而广之,最终实现普遍应用的发展过程。

1.1.1 电子商务内容

目前电子商务大致包含以下3方面内容:

- 网上商业信息服务;
- 电子购物和交易;
- 电子银行与金融交易服务。

随着信息技术的不断发展,电子商务将会扩充新的内容和新的领域。通常,电子商务的基本流程如图1.1所示。

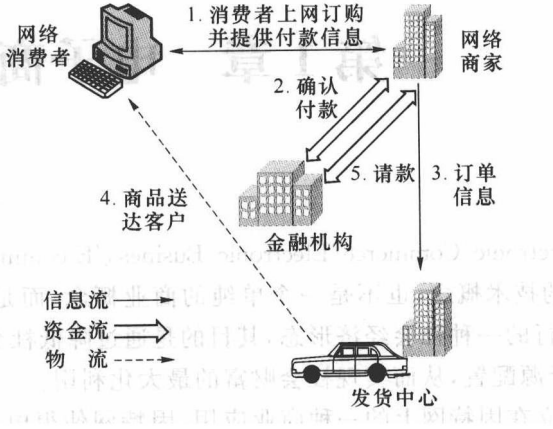

图1.1 电子商务流程图

首先消费者上网订购商品,并提供付款信息;然后网络商家根据消费者提供的付款信息到银行等金融机构确认付款信息;确认后,向发货中心下达订单信息;发货中心根据订单信息将商品送达客户;最后网络商家向银行等金融机构请款,将资金从消费者账户转到商家账户。图1.1描述的电子商务的基本流程中包含了信息流、资金流和物流,另外安全也是保证电子商务正常进行的基本条件。因此从技术上看,电子商务必须涉及和处理这4个方面的问题。

1. 信息流

信息流是电子商务最大的优势,也是电子商务的基础。传统商务中的信息沟通,要花费大量的时间和精力,所需的交易成本较高。电子商务中基于因特网,采用电子信息交换,将会使商务交易过程快速、公开、低廉和准确,而且可打破地域限制。因此,解决好信息流的问题,将是电子商务成功的关键。

2. 资金流

资金流是电子商务遇到的第一个挑战。信息流只是解决了参与商务各方的信息交流,而一个真正的商务过程的完成,最终要靠资金的转移来实现。因此如果不解决好这个问题,电子商务就无法实现。

资金流必须依靠电子货币、网络银行和安全交易协议等方式来解决。

3. 物流

电子商务的特点是加快了商务过程，减少了中间环节，并能提供全球化和个性化的服务。但是，物流过程是不可代替的，在某种程度上甚至还增加了物流的流量和难度。电子商务的巨大好处是否会因为这个问题而受到阻碍，关键在于商家如何解决。

4. 安全

安全是保证电子商务过程能够顺利完成的必要条件。由于电子商务中交易双方无法见面，将会产生许多传统商务模式中不会出现的安全问题，本质上就是网络安全和交易的安全。

如何将网络上传递的资料加密，即解决网络资料安全性的问题？

此外，对顾客来说，网上所看到的商品与实物是否一致？交钱以后对方是否一定会送货？何时送到？使用的电子货币是否安全？等等。对网络商家来说，对方的资金是否真能转到自己的账上？自己的网上账号是否安全？如果是货到付款，对方是否能履行交易合约？等等。

对双方来说，交易出现了争议，又该如何解决？

这些都是电子商务中的安全问题，必须靠技术手段和信用手段来解决。只有这个问题解决了，才能保证电子商务的顺利进行。本书主要介绍保障电子商务安全涉及的相关技术。

1.1.2　电子商务分类

电子商务改变了传统经济活动的运行方式。电子商务按照应用群体的角度进行分类，可以分为以下 4 个主要类别。

1. 企业间的电子商务(B2B)

即企业与企业之间，通过网络进行产品或服务的经营活动。例如，工商企业通过计算机网络向它的供应商进行采购，或通过计算机网络进行付款等商业活动。企业目前面临的激烈竞争也需要电子商务来改善竞争条件，建立竞争优势。商业机构对商业机构的电子商务从未来的发展看仍将是电子商务的主流。商业机构之间的交易和商业机构之间的商业合作是商业活动的主要方面。

2. 企业与消费者之间的电子商务(B2C)

即企业通过网络为消费者提供产品或者服务的经营活动。这类电子商务主要是借助于因特网所开展的网上销售活动。随着因特网的发展，这类电子商务的发展异军突起。例如，在因特网上目前已出现许多大型的网络商店，所出售的商品一应俱全，从服装、食品到计算机、汽车等，几乎包括了所有的消费品。网上交易通常只涉及信用卡或其他电子货币。因此实现企业与消费者之间的电子商务障碍较少，潜力巨大。就目前发展看，这类电子商务仍将持续发展，是推动其他类型电子商务活动的主要动力之一。

3. 政府与企业之间的电子商务(G2B)

这类商务活动包括企业与政府组织间的各项电子商务活动。例如，政府将采购的细节在因特网上公布，通过网上竞价方式进行招标，企业也要通过电子商务的方式进行投

标。目前这种方式仍处于初期的试验阶段。

4. 政府与消费者之间的电子商务(G2C)

政府与消费者之间的电子商务是指政府通过因特网进行社会福利金的支付、个人所得税的征收等。

不同类型的电子商务所包含的主要内容如图 1.2 所示。

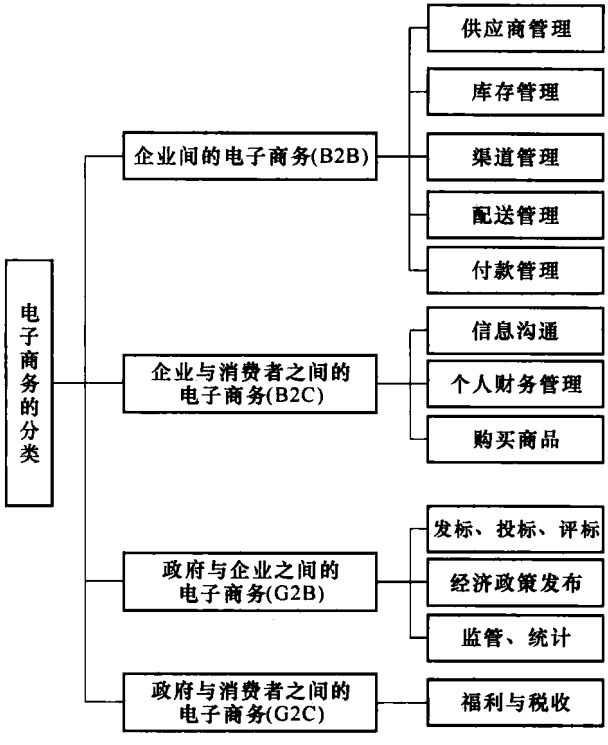

图 1.2 电子商务的分类

1.1.3 电子商务架构

由于电子商务的发展速度惊人,覆盖范围十分广泛,因此必须针对具体的应用才能描述清楚系统架构。目前电子商务的应用包括网上商店、网上银行、远程教育、网上订票、网上交税、股票交易和远程医疗等。

电子商务系统总体框架结构如图 1.3 所示。底层是网络基础平台,它是信息传送的载体和用户接入手段,它包括各种各样的物理传送平台和传送方式;中间是电子商务基础平台,包括 CA 认证和支付网关等,真正的核心是 CA 认证;而上层就是各种各样的电子商务应用系统。电子商务基础平台是各种电子商务应用系统的基础。

对电子商务应用及各种基础建设的发展而言,位于图 1.3 左右两侧的技术标准安全协议和相关政策法律法规则是两大重要支柱。

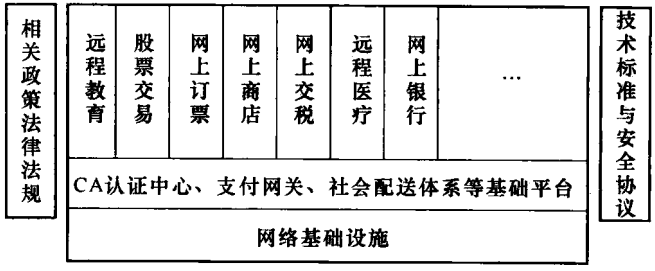

图 1.3　电子商务系统总体框架结构

技术标准与安全协议是指电子商务过程中涉及的标准和协议，包括“电子”与“商务”两部分的标准与协议。“电子”是基础，涉及信息技术方面的标准与协议；“商务”是核心，主要包括与电子商务活动有关的标准与协议，其中涉及信息流、资金流、物流等方面的标准。此外，还包括安全交易协议和服务标准等。综合各种体系结构，电子商务标准与协议应包含如下几个方面：通用基础标准、网络标准、安全协议、认证协议、交易支付标准、商务应用标准和其他标准等。

相关政策法律法规是指有关电子商务的政策、法律和法规等。例如，关于著作权、隐私权的保障、消费者的保护、非法交易的侦察、网络信息的监督，以及交易纠纷的仲裁等，都需要相关的公共政策及法律条文来配合。

一个完整的电子商务系统应该包括哪些部分，目前还没有统一的论述。通常电子商务系统的三层框架结构图如图 1.4 所示。

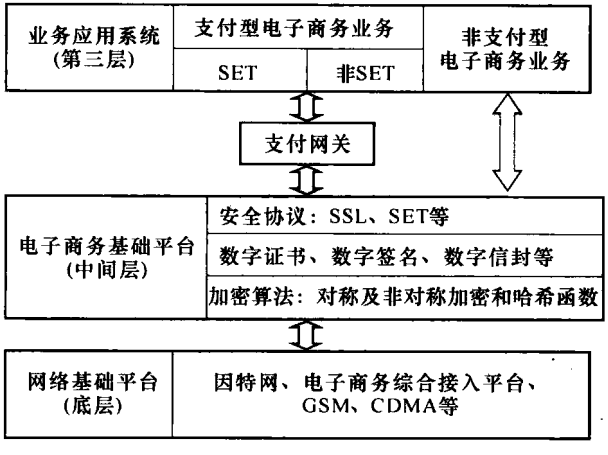

图 1.4　电子商务系统三层框架结构

1. 底层——网络基础平台

网络基础平台是信息传送的载体和用户接入手段，它包括各种各样的网络传输平台、网络传输设备和网络接入方式等。

2. 中间层——电子商务基础平台

电子商务基础平台包含以下3个方面的内容:

(1) 基本加密算法:包括各种对称和非对称加密算法,以及哈希(Hash)函数等。

(2) 基本安全技术:包括以基本加密算法为基础的认证中心(CA)体系以及数字信封、数字签名、报文摘要等安全技术。

(3) 安全协议:包括以基本加密算法、安全技术、认证中心体系为基础的各种安全协议,如SSL协议和SET协议等。

电子商务基础平台是整个电子商务体系的安全基础,它为电子商务提供所需要的各种安全技术,包括实现传输数据的保密性、完整性、不可否认性以及身份认证的各种技术。而认证中心安全认证系统是安全技术的核心。

3. 第三层——业务应用系统

电子商务业务系统包括支付型业务系统和非支付型业务系统。电子商务业务系统中主要是支付型业务系统,而支付型业务系统可分为SET和非SET两类。

支付系统通过支付网关架构在电子商务基础平台之上,以其提供的各种安全服务为前提,为支付型电子商务业务系统提供各种安全的支付手段。而非支付型电子商务系统直接架构在电子商务基础平台之上,使用这一层提供的各种证书技术、认证手段和安全技术为最终用户提供安全的电子商务服务。

电子商务系统中的各个组成部分,例如认证中心、支付网关、业务应用系统、用户终端等均连接在因特网上,并通过因特网实现完整的电子商务。认证中心通过因特网向终端用户、支付网关和电子商务业务应用系统提供证书发放和授权服务等业务。支付网关通过专线与银行的网络中心实现连接。一个支付网关可以实现对多个网络的连接。电子商务业务应用系统直接建立在因特网上,分布在世界各地,通过网络实现企业对消费者(B2C)、企业对企业(B2B)的电子商务应用。

1.2 电子商务安全需求

电子商务的安全与其他计算机应用系统的安全一样,是一个完整的安全体系结构,它包含了从物理硬件到人员管理的各个方面,任何一个方面的缺陷都将在一定程度上影响整个电子商务系统的安全性。此外,电子商务安全还具有其特有的安全需求,如交易安全。

1.2.1 安全威胁

目前电子商务发展面临的主要问题之一是如何保障电子商务交易过程中的安全性。交易安全是网上贸易的基础和保障,同时也是电子商务技术的难点,围绕电子商务安全的相关技术已经成为目前电子商务研究的重点之一。

在电子商务的交易过程中,必然涉及用户的一些机密信息和重要利益。例如,在交易过程