浩强创作室
HAO QIANG STUDIO

电子商务教育丛书

谭浩强 吴功宜 主编

电子商务安全

DIANZI SHANGWU ANQUAN

程龙 杨海兰 编著

经济科学出版社

浩强创作室
HAO QIANG STUDIO

电子商务教育丛书

谭浩强　吴功宜　主编

电子商务安全

程　龙　杨海兰　编著

经济科学出版社

责任编辑：余建春
责任校对：王肖楠
版式设计：代小卫
技术编辑：刘　军　袁　雷

电子商务安全
程　龙　杨海兰　编著
经济科学出版社出版、发行　新华书店经销
社址：北京海淀区阜成路甲28号　邮编：100036
总编室电话：88191217　发行部电话：88191540
网址：www.esp.com.cn
电子邮件：esp@esp.com.cn
北京新丰印刷厂印刷
河北三佳装订厂装订
850×1168　16开　21.5印张　530000字
2002年11月第一版　2002年11月第一次印刷
印数：0001—5000册
ISBN 7-5058-2872-X／F·2240　定价：43.00元
（图书出现印装问题，本社负责调换）

序　言

我国正面临着高技术产业化形成知识经济的时代变革。经济全球化意味着生产的全球化、竞争的全球化。经济全球化的实质，是将全世界经济作为一个整体进行结构调整，这一过程会影响到每一个参与者。中国加入 WTO 就意味着我们已经选择了参与经济全球化的战略。世界各个国家都在大力发展信息技术和信息产业，都在加快建设国家信息基础设施；很多国家的信息产业都对本国国民经济的发展产生着重要的作用，并将会成为国民经济的支柱产业；信息化建设成果已经广泛渗透到教育、科研、国防、金融、商业与信息服务业，并且日益发挥重要作用。

随着 Internet 技术的迅速发展与应用的日益广泛，人类进入信息化社会的步伐在深度与广度上都大大加快。电子商务是在信息时代中产生与发展起来的新生事物，同时它也是信息技术与各国信息化建设的必然的产物。在全球范围内，基于 Internet 的电子商务正在以前所未有的速度迅猛发展，它不仅改变着传统的社会生产方式，而且对经济结构的调整产生了极其深刻的影响，成为世界经济新的增长点。电子商务通过 Internet，加快了全球物流、资金流与信息流的交流，极大地降低了经济与社会活动的成本，提高了社会运行效率和企业经济效益。电子商务一出现就显示出巨大的生命力。她不仅在全球呈现出竞相发展的趋势，而且对世界经济格局和贸易体制的变化产生了重大的影响，有力地促进了全球经济一体化的进程。1998 年 11 月的亚太经合组织非正式领导人会议上，江泽民主席明确地表示了中国政府对电子商务的重视。电子商务代表着未来贸易方式的发展方向，大力发展电子商务是推动国民经济信息化的重要内容。

我国的电子商务目前正处在起步阶段，机遇与挑战并存。接受 NASDAQ 网络泡沫破灭的教训，人们在如何发展我国电子商务的认识更加成熟。人们认识到，发展中国电子商务必须遵循社会主义市场经济体制的要求，充分运用市场机制，发挥企业的积极性。政府的宏观规划与指导，为电子商务的发展创造健康的法律环境。同时，培养大批掌握电子商务技术的人才也是至关重要的。为了配合我国电子商务教育工作的开展，由浩强创作室组织编写了这套《电子商务丛书》。根据我国当前的需要，先组织编写出版以下 5 本：

1.《电子商务干部培训教程》，是向广大干部和初学者普及电子商务基本知识的培训教材。

2.《电子商务导论》，从 Internet 技术发展的角度，帮助读者了解电子商务的

产生、发展、运行环境与应用技术。

3.《电子商务关键技术》，介绍了电子商务系统的规划、设计方法，以及所涉及的一些重要和基本的技术。

4.《电子商务网站建设》，介绍了电子商务网站建设的基本方法，以及实际建设的实例。

5.《电子商务安全》，从理论到实践，对电子商务系统运行的关键问题——安全技术，进行了系统的介绍。

丛书的作者都是从事计算机网络与电子商务应用技术研究与开发的大学教师和专业技术人员，其中多数是年轻的、有实际工作经验的博士。他们希望结合自己的工作经验，能够使理论与实际相结合，深入浅出地讲述电子商务的基本概念、设计方法与实现技术，帮助读者系统地掌握电子商务的基本知识与关键技术。通过丛书的学习，希望读者能够结合企业或本单位的工作实际，逐步掌握实际电子商务系统运行和管理技术，以及设计和开发实际的电子商务系统的初步能力。

电子商务是一个涉及信息科学与技术、管理学、经济学与法学等多个学科的综合性交叉学科。本丛书的编写希望能在技术与管理、技术学科与人文学科的交叉方面，探索出自己的道路，形成自己的特色。

电子商务与相关的技术发展是非常迅速的，我们自己也在不断学习之中，因此本丛书一定会有不足之处，敬请读者批评指正。

谭浩强　吴功宜

2002 年 1 月

前　言

Internet 的迅猛发展和广泛应用给人类生活带来了根本性的影响，电子商务就是 Internet 对人类社会产生巨大影响的一个重要表现。电子商务作为一种崭新的商业运作模式，在现代经济生活中具有举足轻重的地位。它作为联系商家、企业、政府及顾客等实体的纽带，在信息传递、加工、综合利用等方面发挥着越来越重要的作用。它极大地改变了企业的运作方式。它不仅是现代企业参与竞争、提高经济效益的重要手段，而且也直接关系到整个国家未来的经济竞争力与综合国力。

基于 Internet 开展电子商务虽然前景诱人，但是其上的安全问题却令人担忧。Internet 之所以能够迅速发展成为今天的全球性网络，主要依赖于它的开放性；但也正是这种当初设计上的缺陷使得网络安全具有很大的脆弱性，正可谓“水能载舟，亦能覆舟”。与一般的信息交流相比，电子商务对网络安全提出了更高的要求。如何建立一个安全可靠便捷的电子商务应用环境，保证整个商务过程中的信息的安全性、完整性，使基于 Internet 的电子交易方式与传统交易方式一样安全可靠，已经成为人们关心的热门话题。

本书围绕电子商务活动中所涉及的各方面安全问题，全面深入地讲述了电子商务安全相关的信息安全技术与网络安全解决方案。作者希望本书能够为学习电子商务安全和支付系统的有关人员提供一定的帮助。在写作风格上，作者突出的是实用性和技术性相结合，希望能够使本书达到理论和实用的统一。

本书一共十章，各章的内容如下：

第一章介绍电子商务安全的基本知识，包括网络安全和商品交易安全。

第二章介绍电子商务安全的加密技术，包括对称密钥密码体制、非对称密钥密码体制、密钥管理和数字信封技术。

第三章介绍电子商务安全的认证技术，包括数字签名、数字时间戳、数字摘要、身份认证、报文认证等。

第四章主要介绍电子商务安全认证体系，包括 PKI 安全体系和 SET 安全体系，并介绍了我国的 CA 认证中心的建设情况。

第五章主要介绍电子商务网络安全。首先介绍了网络安全的基本概念、黑客常用的攻击技术，着重突出实用性。然后介绍了防范攻击的防火墙技术、入侵检测技术、网络安全漏洞扫描技术等，以及网络病毒的防范。

第六章介绍操作系统的安全，包括 Unix 系统和 Windows 系统。

第七章从 TCP/IP 的体系结构上入手，介绍了如何从网络层、传输层和应用层来保护电子商务传输通道上的信息安全，并给出了各层的安全解决方案。

第八章针对电子商务服务器的安全做了详细阐述，包括对服务器的安全威胁、服务器的访问控制，并结合实际详细介绍了常用的企业级防火墙及使用方法，然后介绍了常见的企业入侵检测系统（IDS）系统。本章突出的是实用性。

作为服务器—电子商务传输通道—客户机的电子商务链上的最后一个环节，客户机的安全同样不可忽视。第九章就详细介绍了对客户机的安全威胁以及解决的方案，讨论了电子邮件的安全，给出了几种常见的个人防火墙的使用方法，并介绍了几种常见的反病毒软件。

第十章是本书的最后一章，讨论了几种大公司的电子商务解决方案和它们的安全措施。

本书的读者对象主要包括：希望了解和学习电子商务安全与支付理论以及相关技术的人员；从事电子商务系统设计和开发的工程技术人员；电子商务网站的管理人员和安全人员；适合于从事电子商务及研究的网络安全研究人员以及高等院校相关专业的学生。本书材料丰富翔实、图文并茂，既有一定的理论深度，又有实际的案例分析，有较强的实用性。

本书在编写过程中，参考了很多网上的资料，在此谨向有关的作者表示感谢。

由于电子商务安全涉及的内容很广，加上电子商务安全又是一个较新的领域，且本书编写的时间有限，作者自身的水平也有限，所以书中难免有不足之处，敬请读者批评指教。

作者

2002 年 10 月

目　录

第一章 电子商务安全概述

电子商务（EC，Electronic Commerce）是以开放的Internet网络环境为基础，在计算机系统支持下进行的商务活动。电子商务的一个重要技术特征是利用IT技术来传输和处理商业信息。因此，电子商务安全从整体上可分为两大部分：计算机网络安全和商务交易安全。计算机网络安全是针对计算机网络本身可能存在的安全问题，实施网络安全增强方案，以保证计算机网络自身的安全性为目标；商务交易安全则紧紧围绕传统商务在互联网络上应用时产生的各种安全问题，在计算机网络安全的基础上，保障电子商务过程的顺利进行，即实现电子商务的保密性、完整性、可鉴别性、不可伪造性和不可抵赖性。计算机网络安全与商务交易安全密不可分，两者相辅相成，缺一不可。没有计算机网络安全作为基础，商务交易安全就犹如空中楼阁，无从谈起。没有商务交易安全保障，即使计算机网络本身再安全，仍然无法达到电子商务所特有的安全要求。

1.1 电子商务的基本概念

随着Internet的发展，Internet已经成为目前全世界规模最大、信息资源最多的计算机网络。同时，利用Internet组建企业专用的企业内部网（Intranet）和企业之间使用的外联网（Extranet）也开始得到广泛应用。电子商务是Internet技术应用的全新发展方向，由Internet所引发的电子商务应用发展迅猛，给社会带来了难得的、巨大的发展机遇。Internet本身所具有的开放性、全球性、低成本、高效率的特点，也成为电子商务的内在特征，并使得电子商务大大超越了作为一种新的贸易形式所具有的价值。它不仅会改变企业本身的生产、经营、管理活动，而且将影响到整个社会的经济运行结构。那么，什么是电子商务呢？对很多人来说，电子商务就是在互联网上的购物，但是电子商务并不局限于网上购物，它包括很多商业活动。欧洲委员会（1997年）对电子商务的定义是：

“电子商务就是以电子方式进行商务交易。它以数据（包括文本、声音和图像）的电子处理和传输为基础，包含了许多不同的活动（如商品服务的电子贸易、数字内容的在线传输、电子转账、商品拍卖、协作、在线资源利用、消费品营销和售后服务）。它涉及产品（消费品和工业品）和服务（信息服务、财务与法律服务）；传统活动（保健、教育）与新活动（虚拟商场）。”

这一定义简明的阐述了电子商务的含义。从不同的角度来看：

（1）从通信角度看，电子商务是通过电话线、计算机网络和其他方式实现的信息、产品、服务或结算款项的传送。

（2）从业务流程的角度看，电子商务是实现业务和工作流自动化的技术应用。

（3）从服务的角度看，电子商务是要满足企业、消费者和管理者的愿望（如降低服务成本），同时改进商品的质量并提高服务实现的速度。

（4）从在线的角度看，电子商务是指提供在互联网和其他联机服务上购买和销售产品的能力。

总之，电子商务就是借助于公共网络，如 Internet 或开放式计算机网络（Open Computer Network）进行网上交易，快速而又有效地实现各种商务活动过程的电子化、网络化、直接化。这种商务过程包括商品和服务交易的各个环节，如广告、商品购买、产品推销、信息咨询、商务洽谈、金融服务、商品的支付等商业交易活动。电子商务应用范围相当广泛，以消费者对企业方面来讲包括：电子购物——电子商场、商品展示、线上订购；网络拍卖；电子钱包——电子现金（Electronic Cash）、电子支票（Electronic Cheque）；网络银行——网络转账、账单查询、服务申请、开户、金融产品介绍、网络广告。而企业与企业之间则有商品资料库、电子资料交换、生产供求、商务洽谈、账目清算、技术合作、资金拆借等应用。在企业内部则可利用相关的安全技术建立数字签名、电子公文传送等系统，真正达到安全、迅速的无纸办公以提高管理效率、改善经营质量。

电子商务一般包括四个部分：（1）交易的商流：指接受订单、购买、开具发票等销售的工作，也包括维修等售后服务之类的工作；（2）配送的物流：指商品的配送；（3）转账支付的结算：交易双方必然涉及资金转移的过程，包括付款、与金融机构交互等（应包括资金转移、与资金转移之相关信息，例如所有权转移凭证等）；（4）信息流：包括商品信息、信息提供、促销、直销等。它和传统的商业系统相比，具有交易花费成本低、资金更安全、资金结算速度快、节省人力物力、方便等特点。

1.1.1 电子商务系统结构

从整体上看，电子商务系统是一个相当复杂和庞大的系统，不但涉及众多的计算机技术和网络技术，而且涉及金融、税收、法律、政治等方方面面。为了简化系统设计和实现过程，通常将庞大的电子商务系统看成几个小系统的组合。每个小系统实现某些特定的功能，小系统之间通过接口与其他小系统交换数据。这样就形成了电子商务的层次体系结构。

通常，电子商务的体系结构可以分为网络基础平台、安全结构、支付体系和业务系统四个层次。其系统结构如图 1-1 所示。

1. 电子商务的网络基础平台

电子商务是以计算机网络为基础的，计算机网络是电子商务的运行平台。所有的电子商务活动最终都需要在网络中进行信息传递，因此，网络基础的好坏直接影响电子商务系统的质量。目前，计算机的处理速度已基本满足商务处理要求，网络的带宽、网络的可靠性及稳定性成为影响电子商务系统整体性能的重要因素。Internet 是电子商务的主要载体，我国已建成的中国公用计算机互联网（CHINANET）、中国科学技术网（CSTNET）、中国教育和科研

计算机网（CERNET）、中国金桥信息网（CHINAGBN）以及各省市自己建立的内部互联网（如天津互联网等）将构成电子商务支柱网络。

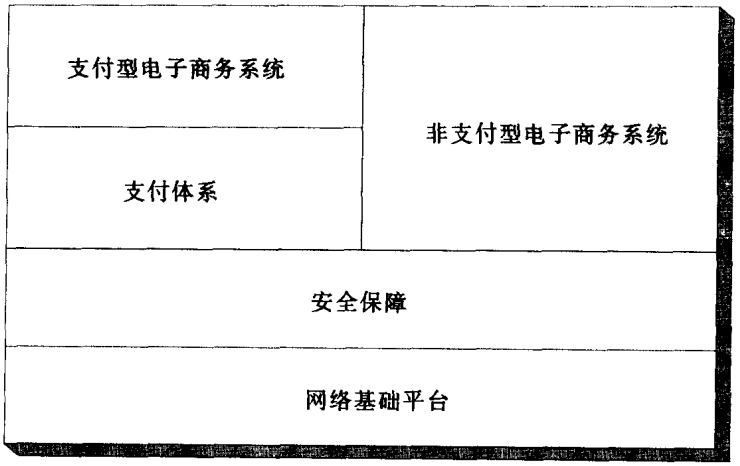

图 1-1　网络基础平台

2. 安全基础结构

电子商务活动不仅包括简单的广告宣传、信息浏览，而且也包括在线谈判、在线交易等各种复杂的商务活动。通常，电子商务活动需要有一个安全的环境基础，以保证数据在网络中传输的安全性和完整性，实现交易各方的身份认证，防止交易中抵赖的发生。电子商务安全基础结构层建立在网络基础层之上，包括 CA（Certificate Authority）安全认证体系和基本的安全技术。利用先进的安全技术，提供各种安全服务，保障电子商务活动安全、顺利进行，是安全基础结构层提供的功能。

3. 支付体系

电子商务活动分为支付型业务和非支付型业务。支付型业务需要支付体系层完成。支付体系架构在安全基础结构之上，为支付型电子商务业务提供各种支付手段。其中包括基于 SET 标准的信用卡支付方式和符合其他标准的各种电子支付手段。

4. 电子商务业务系统

电子商务业务系统包括支付型业务和非支付型业务两类。支付型业务通常涉及资金的转移（如在线购物等）。支付型业务架构在支付体系之上，根据业务的需求使用相应的支付体系。而非支付型业务（如在线谈判、单据传递等）则直接架构在安全基础结构之上，使用安全基础层提供的各种认证手段和安全技术保证安全的电子商务服务。

1.1.2 电子商务应用系统

电子商务系统由各个子系统构成（如图 1-2 所示）。其中有些子系统（如 CA 安全认证系统、支付网关系统）在电子商务系统中是必不可少的，没有这些子系统就不能成为完整的电子商务系统。而有些子系统则可以根据企业用户或个人用户的需求来建立（如业务应用系统、用户终端系统等）。所有这些子系统都需要连接在 Internet 上，它们相互通信，协同工

作，构成完整的电子商务应用系统。

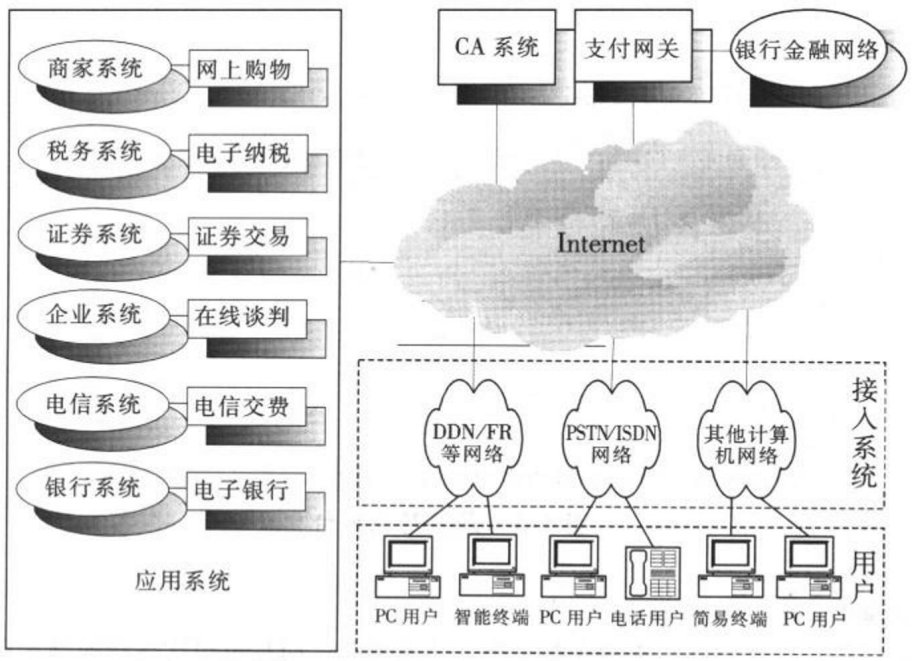

图 1-2　电子商务应用系统构成

1. CA 安全认证系统

在商务活动中，参与活动的双方需要确认对方的身份，以便保证交易活动安全顺利地进行。在一个电子商务系统中，所有参与交易活动的实体也必须使用某种方式或方法表明自己的身份。通过 CA 安全认证系统发放的证书以确认对方（或表明自身）的身份，是电子商务中最常用的方法之一。

证书经证书授权中心数字签名，它包含证书拥有者的基本信息和公开密钥。证书的作用可以归纳为两个方面：

（1）证书是由 CA 安全认证中心发放的，具有权威机构的签名，所以它可以用来向系统中的其他实体证明自己的身份。

（2）每份证书都携带着证书持有者的公开密钥，所以它可以向接收者证实某个实体对公开密钥的拥有，同时起着分发公开密钥的作用。

安全是电子商务的命脉。电子商务的安全是通过加密手段来达到的。公开密钥加密技术（非对称密钥加密技术）是电子商务系统中使用的主要加密技术之一，它主要用于秘密密钥的分发和数字签名，以实现身份认证、信息完整性检验和交易防抵赖等。CA 安全认证中心为用户的公开密钥签发证书，以实现公开密钥的分发并证明其有效性。证书证明了该用户拥有证书中列出的公开密钥。CA 机构的数字签名使得攻击者不能伪造和篡改证书。

证书按照用户和应用范围可以分为个人证书、企业证书、服务器证书、业务受理点证书等等。需要使用证书的单位（或个人），可以以书面形式（或通过网络）向 CA 安全认证中心（或其代理机构）申请证书。CA 安全认证中心在审查用户的资料后，以磁盘或智能 IC 卡等

方式向用户发放证书。对安全性要求不太高的用户，可以利用浏览器通过 Internet 直接申请和下载证书。

在电子商务系统中，CA 安全认证中心负责所有实体证书的签名和分发。一个安全、完整的电子商务系统必须建立一个完整、合理的 CA 安全认证体系。通常，CA 安全认证体系由证书审批部门和证书操作部门组成。证书的审批部门负责对证书申请者进行资格审查，并决定是否同意给该申请者发放证书。而证书操作部门负责为已授权的申请者制作、发放和管理证书，负责证书的查询工作和黑名单库（作废、失效和过期的证书库）的管理工作。

2. 支付网关系统

支付网关系统处于公共 Internet 网络与银行内部网络之间，主要完成通信、协议转换和数据加密解密功能以及保护银行内部网络。当公共 Internet 网络传来信息请求时，支付网关系统将传来的数据包解密，并按照银行系统内部的通信协议将数据重新打包，送往银行内部网络；在接收到银行系统内部网络传回的响应信息时，支付网关将其转换为公共 Internet 网络的数据格式，并对其进行加密，发往公共 Internet 网络。支付网关系统的使用，不仅可以过滤 Internet 上发来的信息包，对防止黑客的攻击和不相关信息的流入大有好处，而且可以利用银行已经建立的内部网络，保护原有的投资。

支付网关系统既要连接公共 Internet 网络系统，又要连接银行内部的专用金融网络系统。通常，支付网关通过专线与公共 Internet 网络和银行内部网相连。当然，一个支付网关系统既可以连接一个银行网络系统，也可以同时连接多个银行网络系统。

3. 业务应用系统

每一个业务应用系统对应于一个特定的业务应用。在电子商务系统中，可以有各式各样的业务应用系统，如网上购物、电子纳税、证券交易、在线谈判、电信交费等等。这些业务应用系统通过接入 Internet，可以实现企业对用户（B to C，Business to Customer）和企业对企业（B to B，Business to Business）的电子商务应用。

支付型的业务应用系统必须配备具有支付服务功能的支付服务器（符合 SET 标准或其他支付标准），该服务器通过支付服务软件（有时也称为电子柜员机软件）系统接入 Internet，并通过支付网关系统与银行进行信息交换。此外，业务应用系统还需要处理用户的请求、发送和接收加密信息、申请和接收认证、处理订单、保存所有记录、与应用系统的后台数据库进行协作等。

在通常情况下，业务应用系统可以以常用的 Web 站点方式接入公共 Internet 网络。某些特殊的专用应用系统也可以采用专用业务软件接入公共 Internet 网络。

4. 用户及终端系统

电子商务用户包括企业用户、事业用户及个人用户等，他们通过 Internet 享受各种电子商务服务。用户使用的终端可以为计算机终端、智能终端、电话终端等。

目前，人们进行电子商务活动最常用的终端就是计算机终端。计算机终端不但性能可靠、安全，而且在使用浏览器（如 Microsoft 公司的 Internet Explorer 或 Netscape 公司的 Navigator）进行电子商务活动时，界面统一，简单易学，既可以包含文字信息，也可以包含图像、声音、动画等多媒体信息。

电话已经普及到千家万户，它具有使用方便、普及率高和使用范围广等特点。计算机技术（特别是 XML 等网络技术）的发展，已经使包括语音在内的各种多媒体业务接入 Internet