Security and Payment of E-commerce

高等院校经济与管理专业教材

电子商务安全与支付

□ 李飒　刘春　主编
□ 潘亚楠　毕浅雨　副主编

ECONOMICS & MANAGEMENT

- 理论与实务并重
- 校园与企业相连
- 教学与实践相关
- 学习与工作无间

人民邮电出版社
POSTS & TELECOM PRESS

Security and Payment of E-commerce

高等院校经济与管理专业教材

电子商务安全与支付

□ 李飒　刘春　主编
□ 潘亚楠　毕浅雨　副主编

人民邮电出版社
北京

图书在版编目（CIP）数据

电子商务安全与支付 / 李飒，刘春主编. -- 北京 : 人民邮电出版社，2014.8
高等院校经济与管理专业教材
ISBN 978-7-115-34145-7

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

中国版本图书馆CIP数据核字(2014)第099382号

内 容 提 要

电子商务安全与支付是电子商务业务流程的重要环节，服务于电子商务资金流的电子支付与结算及其安全性已经成为商务各方关注的焦点。本书从电子商务系统的安全角度出发，详细叙述了技术层面的加密与解密、网络安全技术、防火墙与VPN、安全协议与认证以及安全电子商务应用的内容，并对网上支付的安全使用做了介绍。在此基础上，以电子交易与支付为核心，系统介绍了电子支付工具、网上金融、网上银行等知识及应用。本书每章配有操作性很强的技能训练，学生学习完理论知识后便可以动手操作，有利于学生掌握安全与支付的原理、方法和应用。

本书可作为高等院校各层次电子商务、信息管理、工商管理等专业学生的教材，也可作为其他从事电子商务活动、网络金融等技术人员的参考用书。

◆ 主　　编　李　飒　刘　春
副 主 编　潘亚楠　毕浅雨
责任编辑　韩旭光
责任印制　张佳莹　焦志炜

◆ 人民邮电出版社出版发行　　北京市丰台区成寿寺路 11 号
邮编　100164　　电子邮件　315@ptpress.com.cn
网址　http://www.ptpress.com.cn
三河市潮河印业有限公司印刷

◆ 开本：787×1092　1/16
印张：16　　2014 年 8 月第 1 版
字数：393 千字　　2014 年 8 月河北第 1 次印刷

定价：34.00 元

读者服务热线：(010)81055256　印装质量热线：(010)81055316
反盗版热线：(010)81055315

前　言

随着 Internet 和信息技术的发展与普及，电子商务已逐步进入人们的日常生活。然而，电子商务是在国际化、社会化、开放化和个性化的 Internet 环境中运作的，它的应用可能会出现诸如各种商业信息的泄露、客户的银行账户信息被盗、金融欺诈以及缺乏可信性而导致的商业丢失等各种安全与信任问题。因此，要成功地进行电子交易，必须有效解决交易网络平台的安全问题，以及提供对电子支付过程的保护。电子商务环境下的安全与支付是目前困扰和影响电子商务推广的两个重要问题，这也引发市场对这方面人才的迫切需求。因此，电子商务安全与支付已经成为电子商务及相关专业学生学习的一门重要课程，也是从事电子商务、网络营销等人员应该掌握的重要知识之一。

本书在认真总结国内外电子商务安全与支付管理经验的基础上，从电子商务系统安全角度出发，全面阐述了电子商务交易安全综合防范的思路，从技术、管理和法律三方面着手，介绍了电子商务安全的途径和发展思路，并以电子交易与支付为核心，对电子支付问题进行了深入的研究，提出了电子支付的具体措施。

全书按照“任务引导→技能训练”的思路编写，在任务引导部分介绍基本概念与基本知识，在技能训练部分理论联系实际，培养学生实践能力。本教材创新之处有以下几点。

1. 强化创新理念。结合电子商务安全与支付应用性和创新性强的特点，根据实际应用需要，设计教学内容和实践体系，突出学生创新能力的培养。

2. 科学性与系统性。电子商务安全与支付技术涉及多学科知识领域的交叉，本书在做好学科体系和理论知识前导性工作的同时，正确处理好科学性与系统性、科学性与创新性、系统性与交叉性之间的关系。

3. 理论与实践相结合。将概念、理论框架和技能融合在一起，从理论和方法上对电子商务安全与支付技术做了介绍，使学生能够了解其理论和操作方法。实现学以致用，用以促学。

4. 案例引导教学。书中引入了许多实际案例，帮助学生更好地理解理论知识。

全书共分 10 章：

第 1 章，电子商务安全与支付概述。主要介绍电子商务的基本概念、电子商务的安全问题、安全要素、安全体系结构和网上支付与结算的基础知识，并对其发展现状进行了分析。

第 2 章，加密与解密。介绍了加密与解密基本知识以及对称加密学与非对称加密学。

第 3 章，认证技术。介绍了报文鉴别与身份认证、证书与 CA 相关知识。

第 4 章，网络安全协议。介绍了几种网络安全协议及无线网的安全。

第 5 章，网络安全应用。介绍了防火墙、入侵检测技术以及计算机病毒相关知识。

第 6 章，网络支付基础知识。介绍了网络支付与结算的过程、原理及网络支付工具相关内容。

第 7 章，网上银行。介绍了网上银行的相关知识、网上银行的金融业务、网上银行的业务申请以及中国网络银行的发展状况。

第 8 章，第三方支付。介绍了第三方支付的相关知识、业务功能并分析了第三方支付发展现状及存在的问题。

第 9 章，其他支付结算方式。对移动支付、虚拟货币的支付及电话支付进行了介绍。

第 10 章，网上金融。介绍了网上证券交易及网上保险服务。

每章均配有相关的技能训练。

本书由李飒（辽宁石油化工大学）起草大纲，撰写前言、第 1 章～第 4 章；刘春（武汉铁路职业技术学院）撰写第 5 章及第 6 章；潘亚楠（辽宁石油化工大学）撰写第 7 章、第 9 章和第 10 章；毕浅雨（辽宁石油化工大学）撰写第 8 章；李飒对全书进行了统稿。

本书在撰写工作中参考了众多文献和著作，得到了社会各界同仁和许多同事的指导和帮助，谨在此对他们表示衷心的感谢。

编者

2014 年 2 月

目　录

第 1 章　电子商务安全与支付概述

电子商务，作为一种新兴的交易方式，受到社会各行各业的高度重视，在国民经济的发展中发挥着越来越重要的作用。截至 2013 年 12 月底，我国网络购物用户规模达到 3.14 亿人，网络购物使用率提升至 37.8%。与 2013 年相比，网购用户增长 6 000 万人，增长率为 24%。网购交易促进的衍生企业繁荣发展，在线交易的商品和服务类型更加丰富，带动了用户网络购物频次和金额的显著提升。然而，随之而来的安全问题也越来越突出并已成为电子商务的核心问题。

第一部分　任务学习引导

1.1　电子商务的基本概念

1．电子商务的概念

电子商务源于英文 Electronic Commerce，简写为 EC。欧洲委员会 1997 年把电子商务定义为“以电子方式进行商务交易”。其内容包含两个方面，一是电子方式，二是商贸活动。电子商务以数据（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）。

随着计算机和计算机网络的应用普及，电子商务不断被赋予新的含义。

（1）从通信的角度看，电子商务是通过电话线、计算机网络或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，电子商务通常是指是在全球各地广泛的商业贸易活动中，在互联网开放的网络环境下，基于浏览器/服务器应用方式，买卖双方不谋面地进行各种商贸活动，实现消费者的网上购物、商户之间的网上交易和在线电子支付以及各种商务活动、交易活动、金融活动和相关的综合服务活动的一种新型的商业运营模式。

2. 电子商务的内容

电子商务可以分为 3 个方面：信息服务、交易和支付。其主要内容包括：电子商情广告；电子选购和交易、电子交易凭证的交换；电子支付与结算以及售后的网上服务等。主要交易类型有企业与个人的交易（B to C 方式）和企业之间的交易（B to B 方式）两种。 参与电子商务的实体有 4 类：顾客（个人消费者或企业集团）、商户（包括销售商、制造商、储运商）、银行（包括发卡行、收单行）及认证中心。

一般来说，最完整、最高级的电子商务指的是利用互联网能够进行全部的贸易活动，包括 4 个部分：①信息流：包括商品信息、信息提供、促销、直销等；②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；③配送的物流（指商品的配送）；④支付的资金流：交易双方涉及的资金的转账支付，如付款，与金融机构交互等。由于参与电子商务中的各方在物理上是互不谋面的，因此，整个电子商务过程并不是物理世界商务活动的翻版。网上银行、在线电子支付等条件和数据加密、电子签名等技术在电子商务中发挥着不可或缺的作用。与传统的商业系统相比，电子商务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。

3. 电子商务系统的结构

电子商务系统是保证以电子商务为基础的网上交易实现的体系，它是一个相当复杂和庞大的系统。该系统整体上可分为 3 个层次和两个支柱，如图 1.1 所示。自下向上，从最基础的技术层到电子应用层依次为：网络层，消息/信息发布、传输层，一般业务服务层；两个支柱分别是技术标准和政策、法规，3 个层次之上是各种特定的电子商务应用。3 个层次依次代表电子商务顺利实施的各级技术及应用层次，而两边的支柱则是电子商务顺利应用的坚实基础。

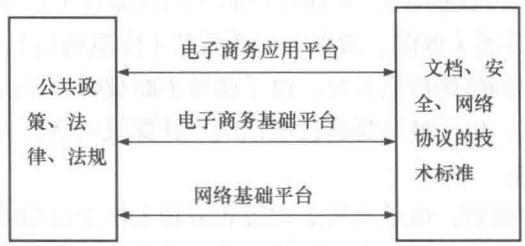

图 1.1　电子商务系统

（1）网络基础平台

网络基础平台是电子商务的硬件基础设施，是信息传送的载体和用户接入的手段。它包

括各种各样的物理传送平台和传送方式。如远程通信网（Telecom）、有线电视网（Cable TV）、无线通信网（Wireless）和互联网（Internet）。远程通信包括电话、电报，无线通信网包括移动通信和卫星网，互联网是计算机网络。

这些不同的网络都提供了电子商务信息传输线路，但是，当前大部分的电子商务应用还是基于 Internet。互联网络上包括的主要硬件有：基于计算机的电话设备、集线器（Hub）、数字交换机、路由器（Routers）、调制解调器、有线电视的机顶盒（Set-Top Box）、电缆调制解调器（Cable Modem）。

（2）电子商务基础平台

网络层提供了信息传输的线路，线路上传输的最复杂的信息就是多媒体信息，它是文本、声音、图像的综合。最常用的多媒体信息发布应用是万维网（World Wide Web，WWW），即用 HTML 或 JAVA 将多媒体内容发布在 Web 服务器上，然后通过一些传输协议将发布的信息传送到接收者。

（3）一般业务服务层

这一层实现标准的网上商务活动服务，以方便交易，如标准的商品目录/价目表建立、电子支付工具的开发、保证商业信息安全传送的方法、认证买卖双方的合法性方法。

（4）公共政策、法规和安全标准、技术标准

① 公共政策

公共政策包括围绕电子商务的税收制度、信息的定价（信息定价则围绕谁花钱来进行信息高速公路建设）、信息访问的收费、信息传输成本、隐私问题等，需要政府制定的政策。其中，税收制度如何制定是一个至关重要的问题。例如，对于咨询信息、电子书籍、软件等无形商品是否征税，如何征税；对于汽车、服装等有形商品如何通过海关，如何征税；税收制度是否应与国际惯例接轨，如何接轨；关贸总协定是否应把电子商务部分纳入其中。这些问题不妥善解决，则阻碍着电子商务的发展。

② 法规

法规维系着商务活动的正常运作，违规活动必须受到法律制裁。网上商务活动有其独特性，买卖双方很可能存在地域的差别，他们之间的纠纷如何解决？如果没有一个成熟的、统一的法律系统进行仲裁，纠纷就不可能解决。那么，这个法律系统究竟应该如何制定？应遵循什么样的原则？其效力如何保证？如何保证授权商品交易的顺利进行，如何有效遏制侵权商品或仿冒产品的销售，如何有力打击侵权行为，这些都是制定电子商务法规时应该考虑的问题。法规制定的成功与否直接关系到电子商务活动能否顺利开展。

③ 安全标准

安全问题可以说是电子商务的中心问题。如何保障电子商务活动的安全，一直是电子商务能否正常开展的核心问题。作为一个安全的电子商务系统，首先，必须具有一个安全、可靠的通信网络，以保证交易信息安全、迅速地传递；其次，必须保证数据库服务器的绝对安全，防止网络黑客闯入盗取信息。目前，电子签名和认证是网上比较成熟的安全手段。同时，人们还制定了一些安全标准，如安全套接层（Secure Sockets Layer）、安全 HTTP 协议（Secure-HTTP）、安全电子交易（Secure Electronic Transaction）等。

④ 技术标准

技术标准是信息发布、传递的基础，是网络上信息一致性的保证。如果没有统一的技术标准，这就像不同的国家使用不同的电压传输电流，用不同的制式传输视频信号，限制了许多产品在世界范围的使用。EDI 标准的建立就是电子商务技术标准的一个例子。

1.2 电子商务的安全问题

随着互联网的发展，电子商务已经逐渐成为一种全新的商务模式，越来越多的人通过 Internet 进行商务活动，随之而来的安全问题也越来越突出并已成为电子商务的核心问题。电子商务是基于计算机网络的商务活动，因此，电子商务安全问题从整体上可分为两大部分：计算机网络安全问题和电子商务交易安全问题。

1. 计算机网络安全

网络安全问题是计算机系统本身存在的漏洞和其他人为因素构成的计算机网络的潜在威胁。概括来说，计算机网络安全的内容包括物理安全、网络安全、数据库安全。

（1）物理安全

物理安全问题是指计算机网络设备、设施以及其他媒体遭到地震、水灾、火灾等环境事故以及人为操作失误或错误及各种计算机犯罪行为导致的破坏。主要有以下几种问题。

① 设备安全问题

任何一种设备都不是万无一失的，设备的机能失常、设备被盗被毁、计算机硬件如计算机所用的芯片、板卡及输入、输出等设备的故障都会对系统安全构成威胁。

② 电源故障

由于意外的原因，网络设备的供电电源可能会突然中断或者产生较大的波动，从而会突然中断计算机系统的工作，引起数据的丢失甚至对系统硬件设备产生不良后果。

电磁信息泄露：计算机和其他一些网络设备大多数是电子设备，当它工作时会产生电磁泄漏，另外，电子通信线路同样也有辐射。辐射的电磁波可以被截收，解译以后能将信息复现。有资料表明，普通计算机显示终端辐射的带信息电磁波可以在几百米甚至一千米外被接收和复现。这种电磁泄露信息的接收和还原技术可以被不法之徒用来窃取网络机密。

③ 搭线窃听

将导线搭到无人值守的网络传输线路上进行监听，通过解调和正确的协议即可以完全掌握通信的全部内容甚至改变通信内容——这是另一种窃取计算机信息的手段，特别对于跨国计算机网络，很难控制和检查境外是否有搭线窃听。美欧银行均遇到过搭线窃听并改变电子汇兑目的地址的主动式窃听，经向国际刑警组织申请协查，才在第三国查出了窃听设备。

保证计算机信息系统各种设备的物理安全是整个计算机信息系统安全的前提，也是整个组织安全策略的基本元素。对于足够敏感的数据和一些关键的网络基础设施，可以在物理上和多数公司用户分开，并采用增加的身份验证技术（如智能卡登录、生物验证技术

等）控制。

（2）网络安全

① 未进行操作系统相关安全配置

不论采用什么操作系统，在缺省安装的条件下都会存在一些安全问题，网络软件的漏洞和“后门”是进行网络攻击的首选目标。只有专门针对操作系统安全性进行相关的和严格的安全配置，才能达到一定的安全程度；即使如此，系统仍然不能被认为是绝对安全的，漏洞和缺陷会不断被攻击者发现。

② 未进行 CGI 程序代码审计

通用网关接口（Common Gateway Interface，CGI），在物理上是一段程序，运行在浏览器可以请求的服务器上，提供同客户端 HTML 页面的接口。CGI 应用程序运行在浏览器可以请求的服务器系统上，因此，不完善的 CGI 应用程序可能成为别入非法进入服务器系统的通道，有可能导致重要的资料被删除或外泄。对于电子商务站点来说，会出现恶意攻击者冒用他人账号进行网上购物等严重后果。

③ 黑客的恶意攻击

黑客最早源自英文 hacker，早期在美国的计算机界是带有褒义的，原指热心于计算机技术，水平高超的计算机专家，尤其是程序设计人员。但到了今天，“黑客”一词已被用于泛指那些专门利用计算机网络搞破坏或恶作剧的人。以前的黑客事件大多数是想显示自己的能力，攻击规模也较小。但现在越来越多的网络攻击开始利用由远程控制程序非法控制他人计算机，获取被控制计算机或服务器上的信息。无论是个人、企业，还是政府机构，只要进入计算机网络，都会感受到黑客带来的网络安全威胁。自 2006 年年底开始，来自于黑客的大规模的网络攻击越来越多，网络攻击表现出的商业目的也越来越明显。这种以网络瘫痪为目标的袭击效果比任何传统的恐怖主义和战争方式都来得更强烈，破坏性更大，造成危害的速度更快，范围也更广，而袭击者本身的风险却非常小，甚至可以在袭击开始前就已经消失得无影无踪，使对方很难追踪。

④ 计算机病毒攻击

计算机病毒是指编制或者在计算机程序中插入的破坏计算机功能或者毁坏数据、影响计算机使用，并且能自我复制的一组计算机指令或程序代码。计算机病毒作为一种具有破坏性的程序，往往想尽一切办法将自身隐藏起来，保护自己，但是病毒最根本的目的还是达到其破坏目的。在某些特定条件被满足的前提下，病毒就会发作，这也就是病毒的破坏性。有些病毒只是显示一些图片、放一段音乐或和你开个玩笑，这类病毒属于良性病毒；而有些病毒则含有明确的目的性，像破坏数据、删除文件、格式化磁盘等，这类病毒属于恶性病毒。计算机病毒的破坏行为体现了病毒的杀伤能力，病毒破坏行为的激烈程度取决于病毒作者的主观愿望和他所具备的技术含量。

⑤ 安全产品使用不当

虽然不少网站采用了一些网络安全设备，但由于安全产品本身的问题或使用问题，这些产品并没有起到应有的作用。很多安全厂商的产品对配置人员的技术背景要求很高，超出对普通网管人员的技术要求，就算是厂家在最初给用户做了正确的安装、配置，但一旦系统改动，需要改动相关安全产品的设置时，很容易产生许多安全问题。

⑥ 缺少严格的网络安全管理制度

安全和管理是分不开的，即便有好的安全设备和系统，也应该有一套好的安全管理贯彻实施。事实上，很多企业、机构及用户的网站或系统都疏于对网络安全方面的管理。调查显示，美国 90%的 IT 企业对黑客攻击准备不足，75%～85%的网站都抵挡不住黑客的攻击。此外，管理的缺陷还可能出现系统内部人员泄露机密或外部人员通过非法手段截获而导致机密信息的泄露，从而为一些不法分子制造了可乘之机。没有安全管理机制，那么安全就是空谈。

（3）数据库安全

网络中的信息数据是存放在计算机数据库中的，供不同的用户来共享。数据库存在着不安全性和危险性，因为在数据系统中存放着大量重要的信息资源，在用户共享资源时可能会出现以下现象：授权用户超出了他们的访问权限进行更改活动；非法用户绕过安全内核，窃取信息资源。数据库数据的安全主要是指针对数据的安全性、完整性和并发控制 3 个方面。

① 数据的安全性

数据库被故意的破坏和非法的存取。

② 数据的完整性

数据库中存在不符合语义的数据，以及防止由于错误信息的输入、输出而造成无效操作和错误结果。

③ 并发控制

数据库是一个共享资源，在多个用户程序并行地存取数据时，就可能会产生多个用户程序并发地存取同一数据的情况，若不进行并发控制就会使取出和存入的数据不正确，破坏数据库的一致性。

2. 电子商务交易安全

当许多传统的商务方式应用在 Internet 上时，便会带来许多源于安全方面的问题。一般来说，商务安全中普遍存在着以下几种安全隐患。

（1）窃取信息

由于未采用加密措施，数据信息在网络上以明文形式传送，入侵者在数据包经过的网关或路由器上可以截获传送的信息。通过多次窃取和分析，可以找到信息的规律和格式，进而得到传输信息的内容，造成网上传输信息泄密。

（2）篡改信息

当入侵者掌握了信息的格式和规律后，通过各种技术手段和方法，将网络上传送的信息数据在中途修改，然后再发向目的地。这种方法并不新鲜，在路由器或网关上都可以操作。

（3）假冒

由于掌握了数据的格式，并可以篡改通过的信息，攻击者可以冒充合法用户发送假冒的信息或者主动获取信息，而远端用户通常很难分辨。

（4）恶意破坏

由于攻击者可以接入网络，则可能对网络中的信息进行修改，掌握网上的机要信息，甚至可以潜入网络内部，其后果是非常严重的。

电子商务交易安全紧紧围绕传统商务在互联网上应用时产生的各种安全问题，网上交易日益成为新的商务模式，基于网络资源的电子商务交易已为大众接受，人们在享受网上交易带来的便捷的同时，交易的安全性备受关注。在计算机网络安全的基础上，如何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。保证交易数据的安全是电子商务系统的关键。

1.3 电子商务安全要素

电子商务随时面临的安全问题导致了电子商务的安全需求。只有提供了以下 5 个方面的安全，才能满足电子商务安全的基本需求。这 5 个方面分别是真实性、机密性、有效性、完整性和不可否认性。

1. 真实性（认证性）

在传统的交易中，交易双方往往是面对面进行活动的。然而，在进行网上交易时，交易双方在整个交易过程中互不见面。如果不采取任何新的保护措施，就要比传统的商务活动更容易引起假冒、诈骗等违法活动。在进行网上购物时，对于客户来说，如何确信计算机屏幕上显示的那个有声誉的网上商店，而不是居心不良的假网站冒充的，怎样才能相信正在选购商品的客户不是一个骗子，而是一个担责任的客户。因此，在进行电子商务交易时首先要保证身份的可认证性。这就意味着，在双方进行交易前，首先必须明确对方的身份，交易双方的身份不能被假冒或伪装。

2. 机密性

在传统的交易活动中，都是通过面对面进行信息交换，或者通过邮寄封装的信件或可靠渠道发送商业报文，达到保守商业机密的目的。而电子商务是建立在一个开放的网络环境中，当交易双方通过互联网交换信息时，由于互联网是一个开放的互联网络，如果不采取适当的保密措施，那么其他人就有可能知道他们的通信内容；另外，存储在网络上的文件信息如果不加密，也有可能被黑客窃取。上述情况有可能造成敏感商业信息的泄露，导致商业上的巨大损失。因此，电子商务另一个重要的安全需求就是信息的机密性。要使信息发送和接收在安全的通道进行，保证通信双方的信息保密；交易的参与方在信息交换过程中没有被窃听的危险；非参与方不能获取交易的信息。

3. 有效性

有效性是指数据在确定的时刻、确定的地点是有效的。电子商务以电子形式取代了纸

张，那么保证这种电子形式的贸易信息的有效性是开展电子商务的前提。因此，要对网络故障、操作错误、应用程序错误、硬件故障、系统软件错误及计算机病毒所产生的潜在威胁加以控制和预防，以保证贸易数据在确定的时刻、确定的地点是有效的。

4. 完整性

由于数据输入时的意外差错或欺诈行为，可能导致贸易各方信息的差异。此外，数据传输过程中信息的丢失、信息重复或信息传送的次序差异，也会导致贸易各方信息的不同。因此，要预防对信息的随意生成、修改和删除，同时，要防止数据传送过程中信息的丢失和重复，并保证信息传送次序的统一。

5. 不可否认性

交易抵赖行为在现实中屡屡发生，更何况在虚拟的网络世界。在传统的纸面贸易中，贸易双方通过在交易合同、契约或贸易单据等书面文件上手写签名或印章来鉴别贸易伙伴，确定合同、契约、单据的可靠性并预防抵赖行为的发生。在无纸化的电子商务方式下，通过手写签名和印章进行贸易方的鉴别已是不可能的了。因此，要在交易信息的传输过程中为参与交易的个人、企业或国家提供可靠的标识，以防止通信或交易双方对已发生的业务进行否认。

1.4 电子商务的安全体系结构

电子商务是活动在互联网平台上的一个涉及信息、资金和物资交易的综合交易系统，其安全对象不是一般的系统，而是一个开放的、人在其中频繁活动的、与社会系统紧密耦合的复杂巨系统（complex giant system）。因此，一个完整的电子商务安全体系，至少应包括 3 类措施，并且三者缺一不可：一是技术方面的措施，如防火墙技术、网络防毒、信息加密存储通信、身份认证、授权等；二是管理方面的措施，包括交易的安全制度、交易安全的实时监控、提供实时改变安全策略的能力、对现有安全系统漏洞的检查以及安全教育等；三是社会的法律政策与法律保障。只有从上述 3 个方面入手，才能真正实现电子商务的安全。

1. 技术措施

（1）加密技术

加密技术是电子商务采取的主要技术手段，是认证技术及其他许多安全技术的基础。通常信息加密的途径是通过密码技术实现的。采用密码技术可以对传输中的数据流进行加密，满足信息机密性的安全需求，避免敏感信息泄露的威胁。密码技术还可用于报文认证、数字签名等，是保护信息机密性、完整性、不可否认性的有效手段。随着电子商务及信息技术的进一步发展，非密码技术如信息隐藏、生物特征、量子密码技术也得到了快速发展。

（2）认证技术

认证技术可以直接满足身份认证、信息完整性、不可否认和不可修改等多项网上交易的安全需求，较好地避免了网上交易面临的假冒、篡改、抵赖、伪造等种种威胁。认证技术主要涉及身份认证和报文认证两个方面的内容。身份认证用于鉴别用户身份，报文认证用于保证通信双方的不可抵赖性和信息的完整性。

目前，在电子商务中广泛使用的认证方法和手段主要有数字签名、数字摘要、数字证书、CA 安全认证体系以及其他一些身份认证技术和提出报文认证技术。

① 数字签名

数字签名可以防止他人对传输的文件进行破坏以及确定发信人的身份。在电子商务安全技术中，数字签名技术有着特别重要的地位，在电子商务安全服务中的源鉴别、完整性服务和不可否认服务中，都要用到数字签名技术。目前的数字签名均建立在公共密钥体制基础上。其中，RSA 签名方法和 EIC amal 数字签名方法是两种基本的数字签名方法。

② 数字摘要

数字摘要技术就是单向哈希（HASH）函数技术。所谓单向哈希函数就是把任意长的输入串 x 变化成固定长的输出串 y 的一种函数，并满足：

已知哈希函数的输出，求解它的输入是困难的，即已知 y=Hash(x)，求 x 是困难的；

已知 x，计算 Hash（x）是容易的；

已知 y_1=Hash（x_1），构造 x_2 使 Hash（x_2）=y_1 是困难的；

y=Hash（x），y 的每一比特都与 x 的每一比特相关，并有高度敏感性。即每改变 x 的每一比特，都将对 y 产生明显影响。

数字摘要可用于数字签名应用，还可用于信息的完整性检验、各种协议的设计以及计算机科学等。

③ 数字证书

数字证书（digital certificate，digital ID）又称为数字凭证，即用电子手段来证实一个用户的身份和对网络资源的访问权限。数字证书是一种数字标识，也可以说是网络上的身份证，它提供的是网络上的身份证明。数字证书拥有者可以将其证书提供给其他人、Web 站点及网络资源，以证实他的合法身份，并且与对方建立加密的、可信的通信。

④ CA 安全认证中心

CA 认证中心（CA：Certification Authority，证书授权）是电子商务安全认证体系的核心机构。认证中心作为一个权威、公正、可信的第三方机构，需要承担网上安全电子交易的认证服务，主要负责产生、分配并管理用户的数字证书。它对电子商务活动中的数据加密、数字签名、防抵、数据完整性以及身份鉴别所需的密钥和认证实施统一的集中化管理，支持电子商务的参与者在网络环境下建立和维护平等的信任关系，保证网上在线交易的安全。CA 的建设是电子商务最重要的基础建设之一，也是电子商务大规模发展的根本保证。

（3）黑客防范技术

目前，人们已提出了许多有效的黑客防范技术，主要包括网络安全评估技术、防火墙技术、入侵检测技术等。

① 安全评估技术

安全评估黑客技术源于黑客入侵系统时采用的工具——扫描器。通过使用扫描器可以不留痕迹地发现远程或本地服务器的各种 TCP 端口的分配以及提供的服务和它们的软件版本，从而间接地或直观地了解到本地或远程机存在的问题，为网络安全漏洞的发现提供强大的支持。

② 防火墙技术

防火墙技术是防止非法用户入侵的有效措施。防火墙是指隔离在本地网络与外界网络之间的一道或一组执行策略的防御系统。所有的防火墙设计都要遵循两条基本原则，即未被允许的必禁止，未被禁止的均允许。作为最成熟的、最早产品化的网络安全机制，防火墙最初的设计就是防范外部攻击。改进的防火墙技术还可有效地控制内部和病毒的破坏。在选择防火墙时，要考虑诸多因素，包括网络结构、业务应用系统需求、用户及通信流量规模方面的需求，以及可靠性、可用性和易用性等方面的需求。

③ 入侵检测技术

入侵检测技术是一种主动保护自己免受黑客攻击的网络安全技术。入侵检测技术通过从计算机网络系统中的若干关键点收集信息并分析这些信息，看看网络中是否有违反安全策略的行为和遭到袭击的迹象。入侵检测被认为是防火墙之后的第二道安全闸门，它在不影响网络性能的情况下能对网络进行监测，从而提供对内部攻击、外部攻击和误操作的实时保护。入侵检测系统（IDS）被定义为对计算机和网络资源的恶意使用行为进行识别和相应处理的系统。它通过对计算机系统进行监视，提供实时的入侵监测，并采取相应的防护手段。目的在于监测可能存在的攻击行为，包括来自系统外部的入侵行为和来自内部用户的非授权行为。目前，国外的 IDS 商业产品已经多达一百多种。另外，还有几十个大型的国家级研究机构和大学正在进行 IDS 的研发工作。

（4）反病毒技术

长期以来，计算机病毒一直是计算机信息系统中的一个很大的不安全因素。反病毒技术主要包括预防病毒、检测病毒和消毒 3 种技术。

① 预防病毒技术

它通过自身常驻系统内存优先获得系统的控制权，监视和判断系统中是否有病毒存在，进而阻止计算机病毒进入计算机系统和对系统进行破坏。这类技术有加密可执行程序、引导区保护、系统监控与读写控制（如防病毒卡）等。

② 检测病毒技术

它是通过对计算机病毒的特征来进行判断的技术，如自身校验、关键字、文件长度的变化等。

③ 消毒技术

它通过对计算机病毒的分析，开发出具有删除病毒程序并恢复原文件的软件。随着网络的发展，病毒传播的国际化发展趋势日趋明显，反病毒工作也由本地化走向国际化。所以，有效的反病毒产品必须能够对全球最新出现的病毒具有最快速的反应能力。