21世纪 高等学校电子信息类专业规划教材·电子商务

电子商务中的信息安全

唐晓东 主 编
刘 辉 刘 宏 副主编

清华大学出版社·北京交通大学出版社

21世纪高等学校电子信息类专业规划教材·电子商务

电子商务中的信息安全

唐晓东　主　编
刘　辉　刘　宏　副主编

清华大学出版社
北京交通大学出版社
·北京·

内 容 简 介

作为商务活动一种新的模式，电子商务的发展前景十分诱人。但其安全问题也变得越来越突出，如何建立一个安全、便捷的电子商务应用环境，对信息提供足够的保护，已经成为商家和用户都十分关心的话题。本书全面阐述了目前电子商务中所使用的安全技术，内容包括：电子商务中所使用的典型密码算法、数字签名技术、密钥管理技术、身份认证技术、网络安全技术、公钥基础设施、数字证书、安全套接层（SSL）协议、安全电子交易（SET）、数字水印、安全电子支付系统、移动电子商务安全，以及电子商务安全所涉及的法律问题等。本书内容丰富，深入浅出，可读性和操作性强。对电子商务中当前中的热点和新应用方面所存在的安全问题，本书也做了详细的介绍。

本书适合作为电子商务、网络金融和网络营销等专业的教材，也可作为对电子商务及其安全和网络安全感兴趣读者的参考书。

图书在版编目（CIP）数据

电子商务中的信息安全／唐晓东主编. —北京：清华大学出版社；北京交通大学出版社，2006.8
（21世纪高等学校电子信息类专业规划教材·电子商务）
ISBN 7－81082－865－7

Ⅰ.电…　Ⅱ.唐…　Ⅲ.电子商务－信息系统－安全技术－高等学校－教材　Ⅳ.F713.36

中国版本图书馆CIP数据核字（2006）第102444号

责任编辑：杨祎　　特邀编辑：刘标
出版发行：清华大学出版社　　邮编：100084　　电话：010－62776969　　http://www.tup.com.cn
　　北京交通大学出版社　　邮编：100044　　电话：010－51686414　　http://press.bjtu.edu.cn
印 刷 者：北京鑫海金澳胶印有限公司
经　　销：全国新华书店
开　　本：185×260　　印张：21.25　　字数：516千字
版　　次：2006年9月第1版　　2006年9月第1次印刷
书　　号：ISBN 7－81082－865－7/F·188
印　　数：1～4 000册　　定价：30.00元

前　言

通信网络技术的快速发展使得 Internet 进入了千家万户，它极大地影响了人们的思想观念和消费方式。人们越来越希望利用网络进行采购和交易，电子商务（Electronic Commerce）便应运而生，并在世界范围内掀起了一阵阵热潮。作为商务活动中一种全新的模式，电子商务的发展前景十分诱人。随着新的购物方式——网上购物开始深入人们的生活，并被越来越多的人所喜爱，但问题也开始频频出现：一些传统的商务方式应用于 Internet 时，带来了许多安全问题，如使用银行卡进行网上支付时该如何保护卡号和密码等关键信息，如何在不安全的网络上建立一个安全信道来传送需要保护的商业信息等。因此，如何建立一个安全、快捷的电子商务应用环境，对信息提供足够的保护，已经成为商家和用户都十分关心而又迫在眉睫的问题。

由于电子商务系统是通过 Internet 把商家、客户和银行三方连接起来的，因此，电子商务安全不仅涉及银行、商家，还包括用户本身。而 Internet 又是非常脆弱的，极易受到黑客的攻击或入侵。任何个人、企业、商业机构及银行都不会愿意通过一个不安全的网络进行商务交易，因为这意味着商业机密和个人隐私的泄漏，会导致巨大的经济损失。因此，从事电子商务的相关人员都有必要了解在 Internet 上如何安全地进行电子商务活动。这些安全技术和知识能帮助大家在进行电子交易时规避风险，享受快捷。

全书共分 9 章，内容涉及电子商务中所使用的典型密码算法、数字签名技术、密钥管理技术及身份认证技术、防火墙技术、安全电子邮件协议、虚拟专用网 VPN 技术、网络入侵检测技术、公钥基础设施（PKI）与数字证书在电子商务中的应用、安全套接层（SSL）协议及应用、保证网上银行卡支付安全的安全电子交易（SET）协议、用于知识产权保护和信息安全的数字水印技术、银行互联网支付系统 BIPS、小额支付的微支付系统、移动电子商务所采用的安全技术如 WAP 协议等。

本书第 1、2、5、6、9 章由唐晓东编写，第 3、7 章由刘辉编写，第 4、8 章由刘宏编写，全书最后由唐晓东审阅定稿。

由于作者水平和能力有限，书中不足之处在所难免，敬请读者批评指正，不胜感谢！

编　者

2006 年 6 月

目　录

第 1 章　电子商务安全概论

电子商务是指交易双方利用简单、快捷、低成本的电子通信手段以不谋面的方式进行的各种商贸活动。从贸易活动角度来说，可以将电子商务分为低层次的电子商务和高级的电子商务两类。低层次的电子商务包括电子商情、电子贸易、电子合同等；高级的电子商务是指利用 Internet 进行的全部贸易活动，在 Internet 上完整地实现信息流、商流、资金流和部分物流，即从寻找客户开始，到洽谈、订货、在线付（收）款、开具电子发票以至电子报关、电子纳税等都通过 Internet 来完成。电子商务涉及到买家、卖家、银行或金融机构、政府机构、认证机构、配送中心机构，由于参与电子商务中的各方是互不谋面的，因此，保证整个电子商务过程中各个环节信息的安全是十分重要的。

1.1　电子商务安全概述

20 世纪 70 年代，支票和现金逐渐地被信用卡的支付方式所替代，同时高新技术的发展使得“现金流动”和“票据流动”逐渐地被先进的以计算机网络为媒体的“电子计算机数据流动”所淘汰，大量的资金在银行的计算机网络中以电子数据形式在各行之间进行着转账、划拨。这种以电子数据形式存储在计算机中，并通过银行计算机网络来流动的资金，以及赖以生存的银行计算机网络系统被称为“电子资金转账系统”（Eletronic Funds Transfer System，EFT）。EFT 的诞生不仅改进了传统银行的工作方式，还抛弃了旧的银行体系所存在的弊端，建立了一种全新的概念和工作制度。以光、电的速度在世界各国之间通过银行计算机网络传递着货币，办理着银行的各种业务，取得了不可估量的经济和社会的双重效益。

由于 EFT 技术的要求和费用都很高，一般小公司很难享受到 EFT 技术带来的好处，因此有了电子数据交换（Electronic Data Interchange，EDI）技术的兴起。EDI 是电子商务的雏形，这种想法最初来自于美国运输业。1968 年，美国运输业的许多公司联合成立了一个运输数据协调委员会（Transportation Data Coordinating Committee，TDCC），研究开发电子通信标准的可行性。1970 年，美国银行家协会（American Bankers Association）的一个研究委员会开发了无纸金融信息传递的美国全国结算系统，并提出了行业标准。1972 年，美国第一个自动票据交换所系统成立。1975 年，TDCC 发表了第一个 EDI 标准。1978 年，美国全国性 EDI 委员会——X12 委员会成立。1981 年，该委员会出版了第一套 EDI 标准。1989 年，美国重新进行了修订，规范了电子商务中的资金划拨问题，从而使得 EDI 的应用逐渐成为现实。1987 年，联合国公布了 EDI 运作标准 UN/EDIFACT（United Nations Rules for Electronic Data Interchange for Administation，Commerce and Transport），并且每年进行修订。1990 年 3 月正式推出了 UN/EDIFACT 标准，并被国际标准化组织正式接受为国际标准 ISO9735。联合国为此成立了联合国贸易网络组织。随着这一系列的 EDI 标准的推出，人们开始通过网络进行诸如产品交换、订购等活动，EDI 也得到广泛地使用和认可。1996 年 12 月 18 日，联合国贸易网络组织中国发展中心（CNTPDC）在北京成立，同年 12 月 24 日，北京海关与中国

银行北京分行在我国首次开通 EDI 通关电子划款业务，并成为联合国贸易网络组织的成员。

不过，EDI 始终是一种为满足企业需要而发展起来的先进技术手段，必须执行统一标准，与普通老百姓一直无缘。而且由于网络在那时仍没有得到充分发展，这使很多商务活动的电子化，仅仅处于一种想象阶段。到 20 世纪 90 年代，随着基于 WWW 的 Internet 技术的飞速发展，这些想法逐步成熟，Internet 网络开始真正应用于商业交易，这时电子商务才日益蓬勃起来，并成为 20 世纪 90 年代初期美国、加拿大等发达国家的一种崭新的企业经营方式。

英国《经济学家》杂志 2004 年 4 月份的一项调查显示，在世界十大电子商务国家或地区中，丹麦排名第一，英国第二，美国第六。英国互动媒介零售集团说，英国已有 1/3 的人在网上购物，且消费额不断扩大。2003 年，英国网上销售已占全国零售总额的 10%，预计到 2009 年，仅个人网上购物的金额就将达到 800 亿英镑。

由于资本市场对中国电子商务的青睐，伴随着国内物流、支付、信用体系的逐步建立和完善，信息基础设施的发展，以及企业和用户上网需求的不断开发和培养，中国电子商务市场已经进入到务实发展阶段。

全球的电子商务发展状况是极不平衡的。根据联合国贸易和发展会议(UNCTAD)发表的题为《2004 年电子商务及其发展状况》的报告显示，在发展中国家，已有越来越多的企业开始使用国际互联网。但时至今日，他们的电子商务依然处在一个较低的水平。对于中小型企业而言，如果将互联网作为一种商业工具，将在很大程度上提高企业的生产力。但目前的状况是，这些企业因为安全、资金和技术等方面的原因而对此望而却步。

根据 Verisign 在 2005 年上半年发布的互联网安全报告，2005 年一季度域名需求强劲，新注册的. com 域名增长了 29%，. net 增长了 24%。Verisign 在过去一年中通过对 13.5 万名在线消费者的跟踪发现，电子商务交易增长了 31%。2004 年 4 季度平均每笔电子商务交易额为 144 美元，2005 年 1 季度上升至 150 美元。通过 Verisign 的支付服务占北美电子商务市场的 37%，2005 年 1 季度交易量达 7 129 万笔，金额 106.9 亿美元。2005 年 1 季度，84.9% 的欺诈交易企图来自美国的计算机，加拿大占 5.2%，英国为 1.1%，澳大利亚与德国为 0.9%，日本为 0.7%。报告还指出，诱骗与域欺骗成为互联网面临的新威胁。网络罪犯正在采用更加复杂的技术应对反诱骗措施。最危险的手段是域欺骗，这是一种间接的攻击，通过安装间谍软件或破坏互联网连接中的一部分，如 DNS，以截取用户与企业网站之间的数据通信。尽管存在安全威胁，但全球范围的用户仍将互联网作为商务与个人使用的基本工具。Verisign加密标识自 2004 年 5 月以来增长了 225%，这意味着网站安全需求的增长，购物者更加倾向于在有可信安全标识的网站进行交易。在我国，根据金山反病毒中心 2005 年 4 月对外公布的《电子商务与网络安全分析报告》，目前对网络安全、电子商务除了计算机病毒造成的破坏之外，危害最大的是网络钓鱼式攻击。该数据来源于金山毒霸全球反病毒监测网，以及毒霸运营部门和线上反病毒部门的联合统计，它是对2003 年 12 月份至2005 年 4 月份以来的所有网络安全攻击事件进行综合分析得出的。网络钓鱼攻击是一种主要以骗取用户各种在线交易的账户、密码而造成严重经济损失的攻击方式。目前国内上网用户突破 9 000 万，宽带用户达 4 000 万以上，随着宽带网络的进一步普及，用户将面临更多的在线交易安全风险。目前威胁最大的 3 种网络钓鱼攻击方式是假冒网站、邮件欺骗和木马病

毒等。随着家庭数字化、网络宽带化的普及，加上各种银行在线支付、拍卖网站、网络游戏等新型消费方式的出现，病毒与钓鱼式攻击事件频繁发生，已经对国民生活与经济发展构成了巨大威胁。我国面临的网络仿冒威胁正在逐渐加大。2004 年，国家计算机网络应急技术处理协调中心共接到网络仿冒报告 223 起，仿冒对象主要是金融网站和电子商务网站。而在 2002 年和 2003 年，每年只有一起，同比增加了上百倍。

1.2　电子商务面临的安全威胁

目前，尽管网络、企业和用户要面临已有的和新出现的安全威胁，但是，互联网使用以及电子商务仍继续保持高速增长势头。许多人认为电子商务就是建立一个网站，事实上，电子商务所涉及的面要大得多。

1.2.1　电子商务的一般框架

电子商务的主要参与者是制造商、广告商、中间商、服务商与消费者，主要的应用领域是销售、支付、税务、生产、保险、运输等，采用的主要技术涉及计算机软硬件、通信、网络、安全、数据库、运筹学、数据挖掘及人工智能等。大家通常在网上看到的网上购物、网上银行、网上拍卖、网上广告等，只是电子商务直接面向用户的层面，称为电子商务应用。为了使这些应用顺利运作，需要有人、公共政策、技术标准和组织四大支柱。这四大支柱是建立在公共商业服务、信息传播技术、多媒体技术、网络技术和各类接口等基础设施之上。管理是整个电子商务体系的基础（如图 1-1 所示）。电子商务与传统经营体制有很大的不同，它有自己特殊的运行环境、企业战略、管理模式（库存、调度）及组织形式，它将极大地改变人们的消费方式与行为。电子商务能降低流通成本，提高企业竞争力及效益。完整的电子商务体系由信息流、商流、物流、资金流几大部分组成。电子商务的优势在于能够简化流程、降低成本、提高效益。

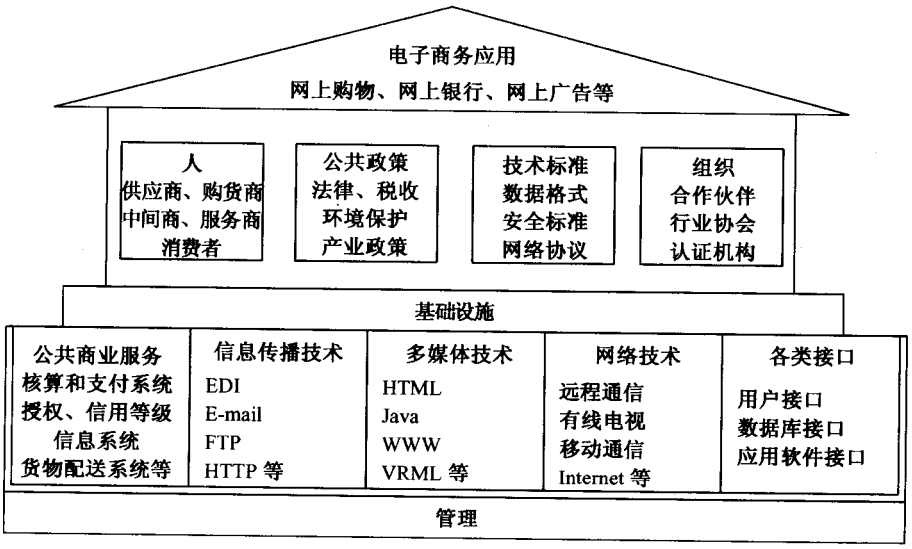

图 1-1　电子商务结构体系

1.2.2　电子商务面临的安全威胁

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网络安全和商务交易安全两大部分。网络安全的内容包括网络设备安全、网络系统安全和数据库安全等。其特征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，以保证计算机网络的自身安全性。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。

根据2005年上半年赛门铁克公司发布的《互联网安全威胁报告》，网上对机密信息的攻击有所上升。2004年7月1日至12月31日，为暴露机密信息而生成的恶意代码占赛门铁克收到的排名前50位恶意代码实例的54%，高出当年上半年的44%和2003年下半年的36%。这部分是由于特洛伊木马的扩散而导致的，在2003年7月至12月期间，特洛伊木马占前50位恶意代码的33%。网页仿冒欺骗攻击也不断上升。网页仿冒欺骗是一种盗取密码、信用卡号和其他金融信息等机密信息的方法。截至2004年12月底，赛门铁克防欺骗过滤器阻塞网页仿冒欺骗企图的次数从2004年7月每周平均900万次上升到每周平均3 300万次。赛门铁克认为，网页仿冒欺骗在2005年仍将是一个非常严重的问题。对Web应用程序的攻击不断增加。Web应用程序使用广泛，攻击者可避开防火墙等传统边界安全措施，不必危及各个服务器的安全即可访问到机密信息。在2004年7月至12月期间记载的所有漏洞中，有近48%是网络应用程序漏洞。这比当年1月至6月记载的39%有了大幅度的上升。企业每天受到攻击的次数从前6个月的10.6次上升到13.6次。金融行业受到的严重攻击率最高，其中在每1万个安全事件中就有16个是严重事件。美国仍是最大的攻击来源国，其次是中国和德国。

对电子商务来说，网络安全是基础。但是，电子商务安全与网络安全又是有区别的。首先，网络不可能绝对安全，在这种情况下，还需要运行安全的电子商务。其次，即使网络绝对安全，也不能保障电子商务的安全。电子商务安全除了基础要求之外，还有特殊要求。从安全等级来说，从下至上有计算机密码安全、局域网安全、互联网安全和信息安全之分，而电子商务安全属于信息安全的范畴，涉及信息的机密性、完整性、认证性等方面。同时，电子商务安全有它自身的特殊性，即以电子交易安全和电子支付安全为核心，有更复杂的机密性概念、更严格的身份认证功能，对不可否认性有新的要求，需要有法律依据性和货币直接流通性特点，还要求网络设有的其他服务（如数字时间戳服务）等。

而在Internet设计之初，设计者们只考虑了方便性、开放性，他们忽视了安全性对网络的重要性，因为他们很难想象到Internet会在短短的几十年内发展得如此迅速和庞大。正是因为当初对安全性考虑太少，所以，今天的Internet非常脆弱，极易受到黑客的攻击或有组织的群体入侵，也会由于系统内部人员的不规范使用和恶意破坏而使网络信息系统遭到破坏，信息被泄露。由于Internet本身的开放性而使网上交易要面临各种危险，通常电子商务中的安全隐患可被分为如下几类。

1. 信息的截获和窃取

如果没有采用加密措施或加密强度不够，攻击者可能通过互联网、公共电话网在电磁波辐射范围内安装截获装置或在数据包通过的网关和路由器上截获数据，获取传输的机密信

息，或通过对信息流量和流向、通信频度和长度等参数的分析，推测出有用信息，如消费者的银行账号、密码以及企业的商业机密等。

2. 信息的篡改

当攻击者熟悉了网络信息格式以后，通过各种技术方法和手段对网络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。例如，改变信息流的次序，更改信息的内容，如购买商品的出货地址；删除某个消息或消息的某些部分；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等。

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。信息假冒主要有两种方式，一是伪造大量用户，发电子邮件，虚开网站和商店，给用户发电子邮件，收订货单，或者发送大量电子邮件，耗尽商家资源，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息等；另外一种为假冒他人身份，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、密钥等信息等。

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，购买者做了订货单不承认，商家卖出的商品因价格差而不承认原有的交易等。在电子商务活动中，消费者面临的威胁有如下几个。

（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。在要求客户付款后，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，此信息也可能会在传递的过程中被窃听。

（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。可能是物理破坏，或者被偷窃。这通常给用户带来不可挽回的损失。

除普通的安全威胁外，电子商务服务器通常还面临如下一些特殊的安全威胁。

（1）系统中心的安全性被破坏。入侵者假冒成合法用户来改变用户数据（如商品送达地址）、解除用户订单或生成虚假订单。

（2）竞争者的威胁。恶意竞争者以他人的名义来订购商品，从而了解有关商品的递送状况和货物的库存情况。

（3）商业机密的安全。客户资料被竞争者获悉。

（4）假冒的威胁。不诚实的人建立与销售者服务器名字相同的另一个WWW服务器来假冒销售者、虚假订单、获取他人的机密数据。比如，某人想要了解另一人在销售商处的信誉时，他以其名字向销售商订购昂贵的商品，然后观察销售商的行动，假如销售商认可该订单，则说明被观察者的信誉高，否则，说明被观察者的信誉不高。

（5）信用的威胁。买方提交订单后不付款。

1.2.3　电子商务的安全需求

电子商务所面临的安全威胁的出现，导致了对电子商务安全的需求。为真正实现一个安全的电子商务系统，保证交易的安全可靠性，要求电子商务具有机密性、完整性、认证性和不可抵赖性。

1. 机密性

电子商务作为贸易的一种手段，其信息直接代表着个人、企业或国家的商业机密。传统的纸面贸易都是通过邮寄封装的信件或通过可靠的通信渠道发送商业报文来达到保守机密的目的。电子商务是建立在一个较为开放的网络环境上的，维护商业机密是电子商务全面推广应用的重要保障。因此，要预防非法的信息存取和信息在传输过程中被非法窃取。机密性一般通过密码技术对传输的信息进行加密处理来保证。

2. 完整性

电子商务简化了贸易过程，减少了人为的干预，同时也带来维护贸易各方商业信息的完整、统一的问题。数据输入时的意外差错或欺诈行为可能会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、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。贸易各方信息的完整性将影响到贸易各方的交易和经营策略，保持贸易各方信息的完整性是电子商务应用的基础。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。因此，要预防对信息的随意改动，还要防止数据传输过程中信息的丢失和重复并保证信息传送次序的统一。所以，电子商务系统应该提供对数据进行完整性验证的手段，确保能够发现数据在传输过程中是否被改变了。完整性一般可通过提取信息的数据摘要方式来获得。

3. 可靠性

系统不能拒绝合法用户对网络系统中信息资源的使用。这就需要对网络故障、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。

4. 鉴别性

因为网络电子商务交易系统的特殊性，企业或个人的交易通常都是在虚拟的网络环境中进行的，所以对个人或企业实体进行身份确认成了电子商务中十分重要的一环。对人或实体的身份进行鉴别，为身份的真实性提供保证，即交易双方能够在相互不见面的情况下确认对方的身份。这意味着当某人或实体声称具有某个特定的身份时，鉴别服务将提供一种方法来验证其声明的正确性。电子商务系统应该提供通信双方进行身份鉴别的机制。一般可以通过数字签名和数字证书相结合的方式实现用户身份的鉴别。数字证书应该由可靠的证书认证机构签发，签发证书时应对申请用户提供的身份信息进行真实性验证。

5. 不可否认性

电子商务关系到贸易双方的商业交易，如何确定要进行交易的贸易方正是所期望的贸易伙伴这一问题是保证电子商务顺利进行的关键。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身份，确定合同、契约、单据的可靠性，并预防抵赖行为的发生。这也就是人们常说的“白纸黑字”。在无纸

化的电子商务方式下，通过手写签名和印章已是不可能的。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。不可否认性可通过对发送的消息进行数字签名来获取。

6. 有效性

电子商务以电子形式取代了纸张，因此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。电子商务作为贸易的一种形式，其信息的有效性将直接关系到个人、企业或国家的经济利益和声誉。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。

1.2.4　电子商务的安全体系结构

电子商务安全是制约电子商务发展的一个核心和关键问题。电子商务的安全性是由其安全体系结构和协议的安全性决定的，协议的安全性是建立在安全体系结构之上的，而协议的安全性又是由协议的关键技术决定的。

电子商务的安全体系结构是保证电子商务中的数据安全的一个完整的逻辑结构，由 5 个部分组成，具体结构如图 1-2 所示。

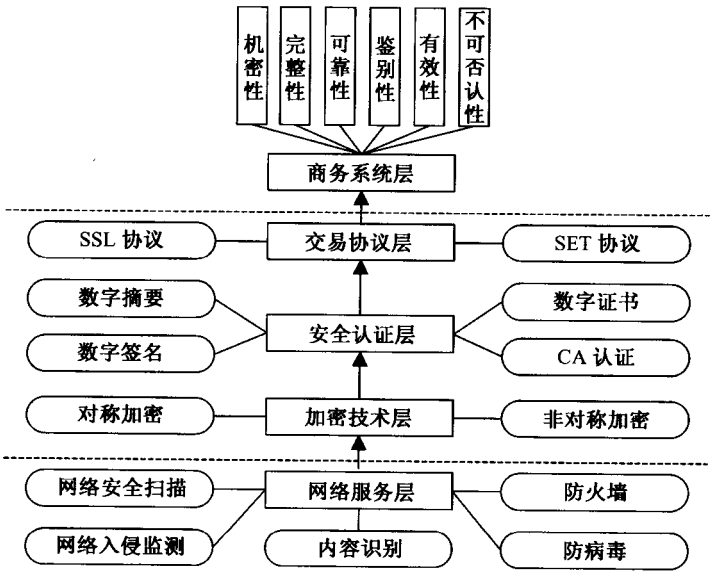

图 1-2　电子商务的安全体系结构

电子商务的安全体系总体上可看成是一个三层框架结构，底层是网络平台，也就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；中间层是电子商务基础平台，包括 CA（Certificate Authority）认证体系、支付网关（Payment Gateway）和客户服务中心 3 个部分，其核心是 CA 认证；第三层就是各种各样的电子商务应用系统。具体来说，电子商务安全体系由网络服务层、加密技术层、安全认证层、交易协议层、商务系统层组成。从图 1-2 中的层次结构可以看出，下层是上层的基础，为上层提供技术支持；上层是下