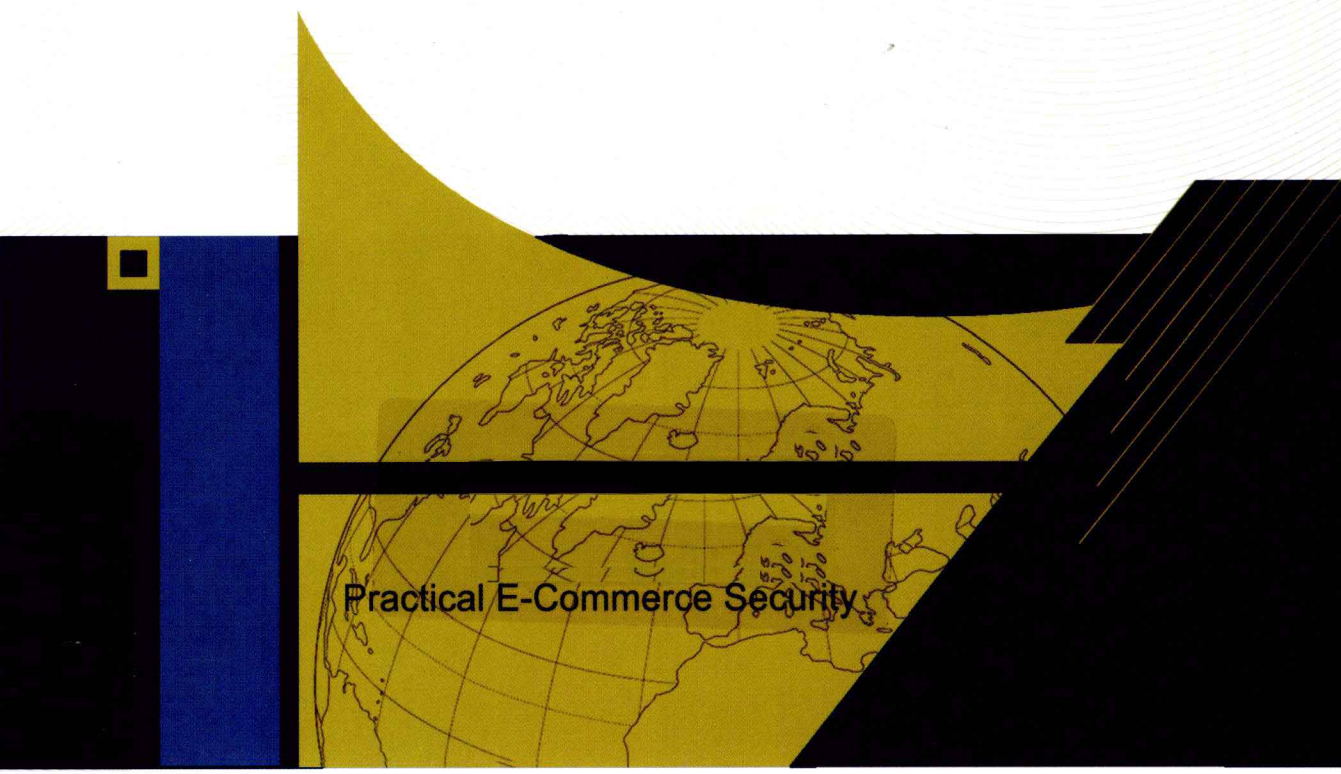
面向“十二五”高等院校应用型人才培养规划教材

电子商务安全实用教程

唐四薪 ◎主　编
邓明亮 何青 谭晓兰 ◎副主编
陈溪辉 刘艳波



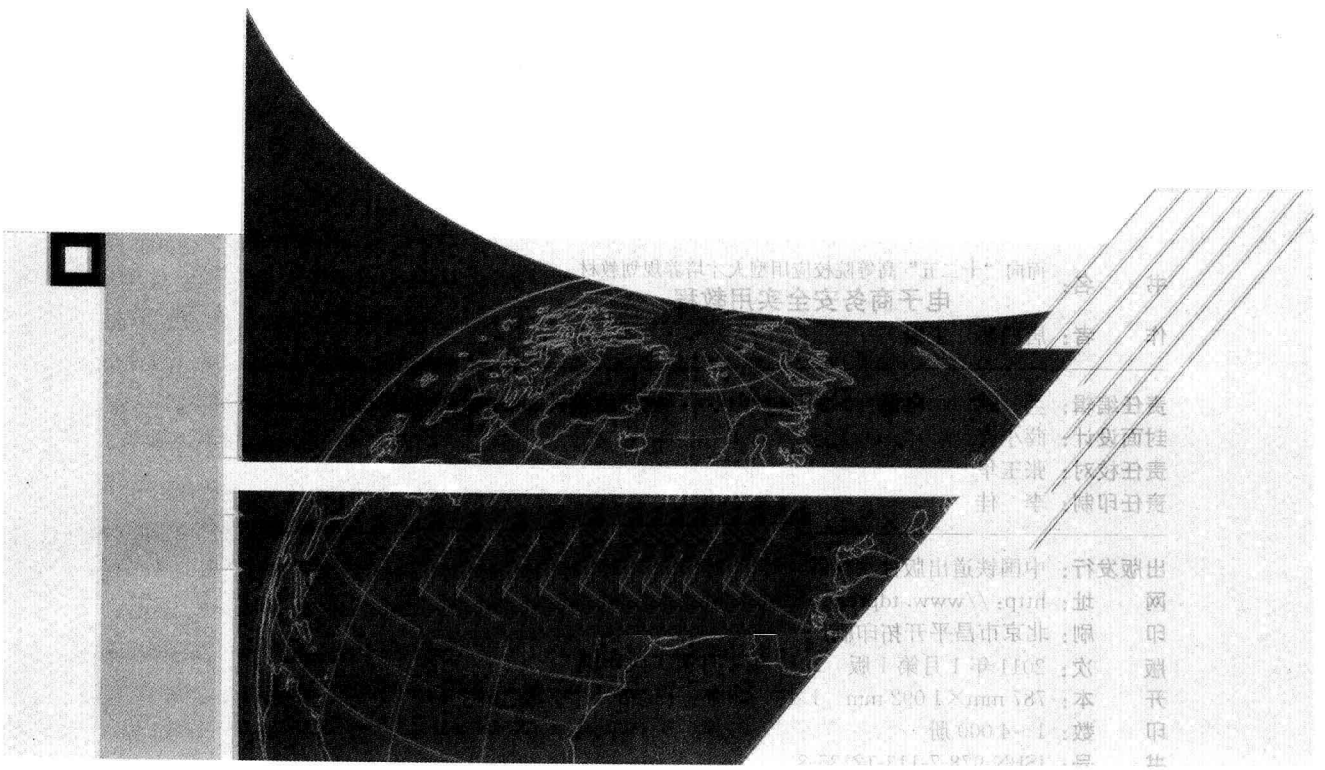
中国铁道出版社
CHINA RAILWAY PUBLISHING HOUSE

面向“十二五”高等院校应用型人才培养规划教材

电子商务安全实用教程

Practical E-Commerce Security

唐四薪◎主　编
邓明亮　何青　谭晓兰　陈溪辉　刘艳波◎副主编
邢容　屈瑜君　戴小新　徐雨明　黄大足　邹赛　唐亮◎参　编



中国铁道出版社
CHINA RAILWAY PUBLISHING HOUSE

图书在版编目（CIP）数据

电子商务安全实用教程 / 唐四薪主编. —北京：铁道出版社，2011.1

面向“十二五”高等院校应用型人才培养规划教材

ISBN 978-7-113-12135-8

Ⅰ.①电… Ⅱ.①唐… 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（2010）第 221846 号

书　　名： 面向“十二五”高等院校应用型人才培养规划教材
电子商务安全实用教程

作　　者： 唐四薪　主编

责任编辑： 兰　鹏　　**电话：** 010-51873014　　**电子信箱：** lanpengtd@126.com

封面设计： 薛小卉

责任校对： 张玉华

责任印制： 李　佳

出版发行： 中国铁道出版社（100054，北京市宣武区右安门西街 8 号）

网　　址： http://www.tdpress.com

印　　刷： 北京市昌平开拓印刷厂

版　　次： 2011 年 1 月第 1 版　2011 年 1 月第 1 次印刷

开　　本： 787 mm×1 092 mm　1/16　**印张：** 15.25　　**字数：** 373 千

印　　数： 1～4 000 册

书　　号： ISBN 978-7-113-12135-8

定　　价： 30.00 元

前言

电子商务安全实用教程 Practical E-Commerce Security Preface

随着电子商务在我国的迅速普及，人们意识到影响电子商务发展的最大障碍就是安全问题。由此《电子商务安全》成为电子商务专业及国贸专业、信息管理和信息系统专业的一门重要的专业基础课程。应该说，《电子商务安全》这门课程起源于《密码学与网络安全》，因为没有密码学（特别是公钥密码学）理论和网络安全技术，当今的电子商务就失去了技术基础而不可能存在。直到目前，电子商务安全的基础内容还是以密码学与网络安全为主，只是将这些知识放在电子商务的环境中进行介绍。《电子商务安全》和《密码学与网络安全》这两门课程相互促进，相互发展。《密码学与网络安全》的教材中也出现了越来越多关于电子商务安全方面的知识。

但《电子商务安全》要想成为一门成熟和独立的课程，必须和《密码学与网络安全》有所区别，要有其明显的特色才能促进该门课程的进一步完善，本书在写作过程中力求突出电子商务安全的特色，这主要表现在以下几方面。

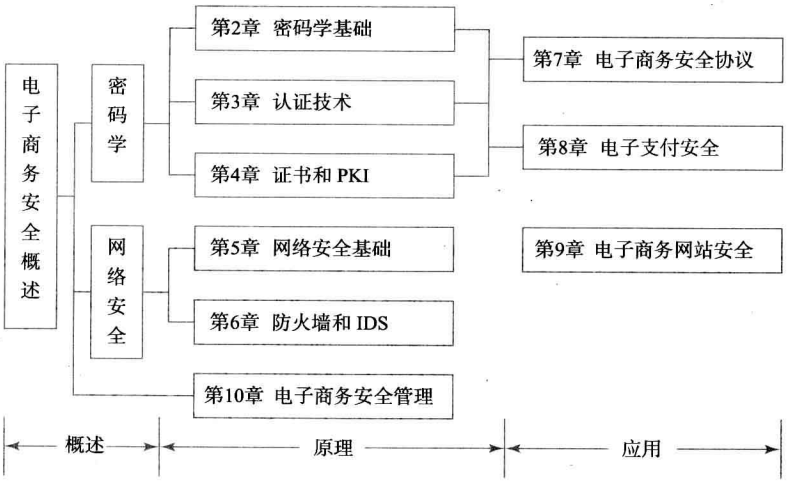
（1）将密码学与网络安全中涉及较深数学知识及较复杂的密码算法的部分删除掉，但保留一些基本的密码学原理和一些必要的数学知识。例如，在公钥密码算法方面，主要介绍 RSA 和 DH 两种算法，因为这两种算法比较简单，但又能使学生明白公钥密码体制的原理，而且在目前仍然是使用最广泛的密码算法。这是考虑到电子商务专业学生学习基础而定的。

（2）处理好电子商务安全原理和应用之间的关系。原理是基础，对电子商务安全的基础问题加密技术和认证技术做了较详细通俗且符合认知逻辑的阐述，使读者能更深刻的理解电子商务安全问题的产生原因。同时增加了单点登录技术、电子现金与微支付的安全机制和电子商务网站安全这些极具实用性和富有特色的内容。在编写形式上，叙述详细，重点突出。在阐述基本原理时大量的结合实例来分析，做到通俗生动。采用问题启发式教学，一步步引出各种加密、认证技术的用途。

（3）辩证地看待电子商务安全在技术和管理方面的教学需要。虽然说电子商务安全是“三分技术、七分管理”。但毋庸置疑的事实是，目前绝大多数电子商务安全教材在篇幅安排上都是“七分技术、三分管理”，这样安排是有道理的。因为大学教育的主要目是为学生打基础，对于技术知识，学生要自学掌握是比较困难的，因此，教师必须重点阐述使学生能理解这部分知识，而管理知识学生可以通过

以后自学并在工作实践中掌握，只有有了一定的实践经验才能更有效地学习安全管理方面的知识。

本书的知识结构分为概述、原理、应用三大块，知识结构图如下：



目前，电子商务安全的课程在很多开设电子商务专业的高校还没受到足够的重视，认为该课程的实用性不如其他课程强。本人认为，学生通过学习该课程有利于把电子商务中的一些底层的、基础的问题理解透彻，可以为将来深入学习、研究电子商务打下坚实的基础。

作为教材，本书注重教材立体化建设。本书每章后都提供具有丰富题型的大量习题，并能为教师朋友提供如下配套资料(PPT 课件、习题答案、考试试卷、教学大纲和案例集)，可登录本书配套网络教学平台(http://ec.hynu.cn)或在出版社网站免费下载，也可和作者联系(tangsix@163.com)。

本书由唐四薪担任主编，邓明亮、何青、谭晓兰、陈溪辉、刘艳波担任副主编。其中，唐四薪编写了第 1～8 章和第 9 章的部分内容；邓明亮、何青、谭晓兰、陈溪辉、刘艳波编写了第 10 章的内容；邢容、屈瑜君、戴小新、徐雨明、黄大足、邹赛、唐亮等参与编写了第 9 章的部分内容。

本书是作者多年从事网络安全工作及电子商务安全教学工作的经验总结，在编写过程中，我的学生肖高云、眭艳凤、苏丽、陈小勤、黄亚运、欧阳双飞、赵丹、喻缘、吴雨桃、袁建君、林友滨等提出了一些有创意的想法和建议，为本书的编写提供了帮助。特别感谢中国铁道出版社的兰鹏编辑，他为本书的出版给予了非常热心的帮助。

本书在编写过程中参考了大量专家学者的图书和论文资料，作者已尽可能地在参考文献中列出，谨在此表示感谢，若有疏漏，也在此表示歉意。由于本人水平和教学经验有限，加之该书中有部分内容比较前沿，书中错误和把握不当之处在所难免，敬请广大读者和同行批评指正。

编　者

2010 年 10 月

目录 Contents

电子商务安全实用教程
Practical E-Commerce Security

第 1 章　电子商务安全概述

随着信息技术的迅速发展，尤其是 Internet 带宽的提高，为人们开辟了一种全新的商业交易方式，即在 Internet 上从事网上交易。人们可以足不出户地在网上购买商品，这种网上交易方式就是电子商务(E-commerce)带给人们最直观的好处。

一般认为，电子商务中的“电子”指的是以 Internet 为主要工具，同时包括其他计算机网络(如移动通信网、物联网、EDI)等通信手段，而“商务”是指各种形式的商业交易活动，因此说，电子商务就是利用一切电子手段进行的所有商业活动。它是一种以 Internet 为媒介，以商品交易双方为主体，以银行电子支付结算为手段，以客户数据为依托的全新商务模式。由此可知，电子商务的参与者包括企业、消费者和中介机构(如银行)等。

电子商务已经逐渐成为人们进行商务活动的新模式，电子商务作为一种新的经济形式正改变着社会生活的方方面面，也为人们带来了无限商机。但安全问题成为电子商务发展的瓶颈，这表现在：一些个人和商业机构对是否采用电子商务仍持观望态度，因为他们担心自己的银行卡是否会被盗用，或自己的个人信息会被窃取。

这些担心不是没有道理的。相对于传统商务，电子商务对管理水平、信息传输技术等都提出了更高的要求，其中安全体系的构建尤为重要，电子商务迫切需要有效的安全保障机制和措施。可以说，在运用电子商务模式进行交易的过程中，电子商务安全问题成为了电子商务最核心的问题，也是电子商务得以顺利推行的保障。

1.1　电子商务的现状及其实现方式

电子商务从字面上理解是以电子形式开展商务活动，表明电子商务的实质是“商务”，而从事商务活动的手段是“电子”的方式。

电子商务是以 Internet 为基础的商务活动，客户机、通信网络、WWW 服务器和各种服务器构成了电子商务活动的基本载体。简单地说，电子商务是买方、卖方(还可能有提供交易平台的第三方)，通过 Internet 进行交易信息交换的过程。由于商务活动的各个环节和信息交换都通过 Internet 完成，因此买卖双方不需要面对面就能够进行商务活动，从而实现商务活动的高效、便捷和廉价，实现利润的最大化。

1.1.1 电子商务在我国的发展现状

据商务部发布的《中国电子商务报告(2008～2009)》指出，我国电子商务交易额2008年达到3.1万亿元，同比增长44.8%，2009年达到3.8万亿元，同比增长21.7%，连续两年创新高。

报告指出，网络购物成为金融危机时期网络经济各个行业中，所受负面影响最小而成长性最佳的热点行业之一。2009年我国网络零售业实现了三个里程碑式的突破。即网络购物用户规模达1.08亿人，年增长45.9%，网络购物使用率继续上升，达28.1%；网络购物交易额达到2 586亿元，较2008年的1 257亿元，增长105.8%，已占社会消费品零售总额的2.06%；此外，网络经商人数规模持续快速增长，截至2009年9月底，人数达6 300万。展望2010年及未来几年的发展，中国电子商务研究中心认为，网络购物市场依然会维持相对较快的成长，相比国外同行及国内传统商务市场，中国电子商务可以有所作为的空间还很大。

报告指出，我国电子商务目前已步入务实发展阶段，呈现七个方面特点：一是大型企业电子商务应用开始进入协同商务阶段；二是中小企业电子商务应用意识普遍提高；三是网络购物规模迅速扩大；四是电子商务专业化服务体系正在形成；五是电子商务在社会经济生活各领域中应用日趋广泛；六是电子商务在应对金融危机、举办北京奥运、抗击自然灾害中的作用日益凸显；七是电子商务渐成资本市场上的投资新宠，中国电子商务行业的高速增长，已引发新一轮资本热潮。据China Venture投资集团数据显示，2010年前6个月，国内电子商务行业企业已完成23笔融资交易，总融资规模达3.31亿美元。

商务部称，我国将从三方面着手，着力推动电子商务发展。第一，制定、完善相关政策，为电子商务的发展创造环境。第二，用“示范”促应用，如农村电子商务示范工程，“新农村商网”每日点击超300万次，有效地扩大了农村公共商务信息服务的覆盖范围，使更多农民从中受益。同时，商务部开始了城市电子商务、国际贸易电子商务的示范应用，这将使电子商务在传统产业结构的转型与升级中发挥更大引导作用。第三，加大电子商务应用的宣传力度，引导电子商务向纵深发展。

今天，以信息技术为手段的电子商务，作为一种新的经济形式已经成为不争的事实。它已经成为主要发达国家增强经济竞争实力，赢得全球资源配置优势的有效手段。各国政府和组织都在积极推进电子商务，以促进经济的繁荣和增长。

1.1.2 电子商务的主要类型

电子商务交易是指在网络平台基础上直接进行的在线交易(trade on line)，它利用数字化技术将企业与企业、企业与消费者或消费者之间有机地连接起来，实现从浏览、洽谈、签约、交货到付款等全部或部分业务的自动化处理。按照参与交易的主体和交易的产品类型，可以将电子商务交易分为不同的模式。

1. 按照参与交易的主体来划分

(1)企业对企业B2B(business to business)模式，是指商业企业之间进行的电子商务活动，这是最早出现的电子商务模式。企业通过互联网来与供应商联系订货、接收发票和付款。这种模式的特点是买家购买商品不是用来消费，而是用来生产加工或再出售，而且每次购买的量比较大。通过这种B2B的模式，企业之间可以实现协同作业，资源管理及信息共享，以推动分销商、经销商和中心企业之间的供应链重组，提高业务的有效性并降低成本。例如，国内的阿里巴巴网站(http://china.alibaba.com)就为企业之间搭建了一个B2B的平台。

(2)企业对消费者B2C(business to customer)模式，是指商业企业与消费者个人之间进行

的电子商务活动。随着网上商店的出现，产生了这种电子商务模式。这种模式既包括网上购物，也包括针对个人的网上订票、网上订餐及网上银行等服务型的业务。例如，企业在 Internet 上开设购物网站（网上商店），陈列商品、标示价格、说明服务，向消费者直接提供从图书、鲜花、数码产品到订票、旅游、订酒店等众多商品和服务。这种模式由于直接针对消费者，开创了一个前景广阔的庞大市场，由于个人的商业行为和商家的商业行为之间有着较大的差异，因此 B2B 和 B2C 之间也有着较大差异。国内的当当网、卓越网都是 B2C 模式的优秀代表。

（3）消费者对消费者 C2C（customer to customer）模式，是指消费者之间通过 Internet 来交换需求信息。一般情况是，在专门的个人交易平台网站上，消费者将自己需要出售的商品信息公示，其他消费者看到后协商购买，买卖双方达成协议后，一桩交易就通过网络初步实现了。在这里，网络中介的作用得到了充分的体现。国内的淘宝、易趣、百度有啊和腾讯拍拍都是主要为消费者提供 C2C 交易中介平台的网站。值得注意的是，以 C2C 模式来交易的一般是单件商品或件数很少的商品，如一本书、一台数码相机等。如果卖家希望出售的商品很多，则卖家就可看成是商业企业，该模式也就转换成 B2C 了。

另外，还有企业与政府之间（B2G）、个人与政府之间（C2G）等交易模式，但从实现技术上来看，B2G 可以归类到 B2B，C2C 和 C2G 可归类到 B2C。因此，在技术上看主要有 B2B 和 B2C 两种类型的电子商务。目前，B2B 在交易额和交易量方面仍远远大于 B2C，说明 B2C 还有很大的发展潜力。

2. 按照交易的产品类型划分

根据电子商务用于交易的产品类型不同，可以将电子商务分为以下两种运行模式。

（1）有形产品的电子商务。适合通过 Internet 直接向消费者销售的有形产品有：图书、音像制品、数码产品、电脑及电脑配件、化妆品、服装、体育用品、办公用品等。这些商品往往具有以下特点中的一项或几项：①体积小、便于运输；②价值不是特别大；③主要购买群体是年轻人或网民。

（2）无形产品的电子商务。目前，电子商务中交易的无形产品有两大类。一类是以数据形式存在的数字产品，如软件、可以下载的在线音像品或电子书籍。另一类是无形产品或服务，如架设网站所需的域名、主机空间，网上订票和网上学校等。无形产品电子商务交易的最大优点是所交易的商品可通过 Internet 直接传送，不需要考虑物流的问题，其物流、资金流、信息流均通过 Internet 完成，因此特别适合在 Internet 上交易，是一种“纯粹”的电子商务。目前，无形产品电子商务已成为电子商务发展中的一个重要方向。

1.1.3 电子商务系统的组成

电子商务系统的总体框架结构可分为三层，其底层是电子商务网络平台，中间层是电子商务基础平台，顶层是各种电子商务应用系统。

（1）电子商务网络平台，是指支持电子商务系统运行的企业内部网和 Internet。它是信息传递的载体和用户接入的手段，其结构一般包括软件和硬件两方面。对于商家来说，建立电子商务系统，首先应建立其企业的内部网（Intranet），然后再利用网络互联设备与 Internet 相连，这才能提供与 Internet 上的客户进行交易的接口，同时应提供与银行支付服务的接口，以完成整个电子商务服务。

（2）电子商务基础平台，是为各种电子商务应用系统提供服务的基础设施。包括 CA（certificate authority）认证机构、支付网关（payment gateway）以及企业自己建设的统一身份认证

系统等。对于电子商务来说，认证对方的身份是开展一切安全电子商务活动的前提。要建立起安全的电子商务系统，需要第三方的电子商务认证中心 CA 提供网上安全电子交易认证服务、签发数字证书、并确认用户身份的服务。支付网关的角色是信息网与金融内网连接的中介，它承担双方的支付信息转换的工作。

(3)电子商务应用系统，是指企业提供电子商务服务的软件系统。它的基本功能包括：商品的信息展示、购物车功能和交易处理功能，以及企业根据实际需要，提供为用户服务和企业内部管理服务的功能(如客户关系管理系统 CRM、企业资源计划 ERP 等)。

1.1.4 电子商务基础平台

电子商务基础平台是企业用于向电子商务转型的完整 IT 基础设施和完善的电子商务服务。它为企业提供了信息集成、应用整合、流程再造、业务创新的基础和能力。建设成熟、可管理的电子商务基础平台，使企业的每一项核心业务如 SCM、ERP、CRM、商业自动化、电子交易等，都可以借助该平台的支持获得最佳的效果。

电子商务基础平台的主要性能指标有安全性、可扩展性和灵活性。

(1)安全性。一个良好的电子商务基础平台应该能保证业务流程运作的安全性和连续性，以及电子商务服务对最终用户的可用性。

(2)可扩展性。企业一旦连接到网络上，将面临迅速增长的海量数据，以及极有可能因此导致的不可预知的客户需求和用户工作量的激增。因此，电子商务基础平台应有良好的可扩展性。

(3)灵活性。统计表明平均每个企业在一年中对电子商务系统应用的更改超过 3 000 次，许多企业内部存在着不同厂商提供的服务器、操作系统、数据库和各类应用软件。同时，企业还需要解决与客户、商业合作伙伴和供应商的系统之间进行沟通和整合的问题。这样才能促进电子商务模式的迅速扩展。

电子商务基础平台的作用贯穿于企业运营的每个环节。规划和建设电子商务基础平台不仅仅只是技术问题，应当同时考虑到业务流程、管理方式、与合作伙伴的协作关系等。需要有全局的远见、充足的时间、强大的资金实力和良好的资源作为保证。

1.2 电子商务安全的内涵

安全(security)是指主体没有危险的客观状态。安全涉及主体的方方面面，就像人的吃、住、行等各方面都可能存在安全隐患一样，电子商务安全也是一个系统而广泛的概念。凡是与电子商务相关的各方面都涉及安全问题，它不仅包含着计算机系统、网络通信技术、电子商务应用环境、人员素质等方面的安全，而且还与管理风险、交易风险等密切相关。

电子商务系统的安全性涉及很多方面，诸如计算机主机系统的安全、操作系统安全、数据存储安全、网络安全、电子商务交易安全等。但从整体上看，电子商务安全可分为两个层次，一是计算机网络的安全，二是电子交易安全。两者相辅相成，密不可分。没有计算机网络安全作为基础，电子交易安全无从谈起；没有电子交易安全，即使计算机网络本身很安全，也无法满足电子商务特有的安全需求，电子商务安全就无法实现。

1.2.1 计算机网络的安全

所谓计算机网络的安全是指保障电子商务系统的计算机设备、系统软件平台和网络环境

能够无故障运行，并且不受外部入侵和破坏。这个层次主要针对电子商务信息基础设施，它与计算机、网络等系统环境的关系更为密切，与企业的商务活动的联系较少。

电子商务系统是通过计算机和网络实现的，需要利用 Internet 的各种基础设施和标准，因此构成电子商务安全系统结构的底层是计算机网络服务层。网络服务层是各种电子商务应用系统的基础，提供信息传输功能、用户接入方式和安全通信服务，并保证网络运行安全。

计算机网络安全主要包括系统实体安全、运行安全和系统软件安全，如图 1.1 所示。其特征是针对计算机网络本身可能存在的安全问题，实施强大的网络安全监控方案，以保证计算机网络自身的安全性。

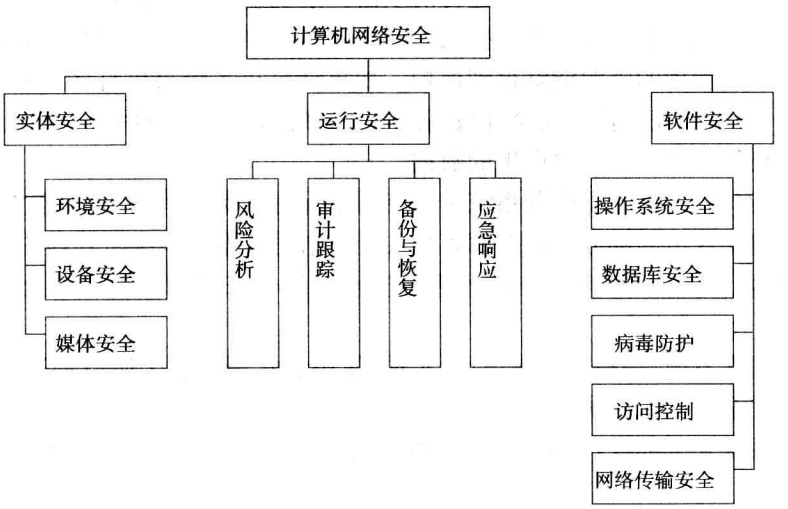


图 1.1 计算机网络安全的组成

1. 系统实体安全

所谓系统实体安全（又称物理安全），是指保护计算机设备、设施（含网络）以及其他媒体免遭自然灾害、人为破坏和环境威胁的措施或过程。实体安全是整个电子商务系统安全的前提，它是由环境安全、设备安全和媒体安全三部分组成。

（1）环境安全：是指保护电子商务系统免受水、火、有害气体、地震、雷击、高温、潮湿和静电等灾害的危害。这要求在建设机房和架设线路时全面考虑有可能对系统造成破坏的各种因素，并设计可行的防范措施。

（2）设备安全：是指对电子商务系统的设备进行安全保护，主要包括设备防盗、设备防毁、抗电磁干扰、电源保护、防电磁信息泄露及防止线路截获等方面。设备防盗可通过加强门禁管理、安装监控报警装置实现；设备防毁包括防止设备跌落、防止鼠害和防止人为破坏等；电源保护一般通过加装不间断电源（UPS）实现。

（3）媒体安全：是指对媒体数据和媒体本身实施安全保护。如防止保存有重要信息的光盘或软盘起霉、损坏或被盗；防止重要数据被非法拷贝；对不再需要的媒体数据要进行销毁，防止媒体数据删除或丢弃后被他人恢复而泄露信息。

2. 系统运行安全

系统运行安全是指为了保障系统功能的安全实现，提供一套安全措施来保护信息处理过程的安全。电子商务系统的运行安全具体由四方面组成。

(1)风险分析:旨在发现系统潜在的安全隐患,并在系统运行过程中测试、跟踪并记录其活动,发现系统运行期间的安全漏洞;最后在系统运行后进行分析,提供相应的系统脆弱性分析报告。

(2)审计跟踪:对系统进行人工或自动的审计跟踪,保存审计记录和维护详尽的审计日志。

(3)备份与恢复:提供对系统设备和系统数据的备份与恢复。

(4)应急措施:是指在紧急事件或安全事故发生时,保证电子商务系统继续运行或紧急恢复所需要的策略。

3. 系统软件安全

与硬件安全相比,电子商务系统的软件安全显得更为重要,因为电子商务系统面临的主要威胁是来自网上的黑客针对系统软件进行的攻击。系统软件安全包括如下几部分。

(1)操作系统安全:通过建立用户授权访问机制、审计等措施,控制系统资源的访问权限,保障操作系统及其管理的资源能够得到保护。如果计算机系统可供许多人使用,操作系统必须能区分用户,以防相互干扰。安全性较高的操作系统应给每一位用户分配独立的账户,并不允许一个用户获得由另一个用户产生的数据。

(2)数据库安全:由于电子商务系统中的资料都保存在数据库中,因此数据库是系统中非常重要又容易遭受攻击的部分。数据库系统安全是指对数据库系统所管理的数据和资源提供安全保护,一般采用多种安全机制与操作系统安全相结合来保护数据库安全。这可从以下两方面着手。

①安全数据库系统:是指从系统设计、实现、使用和管理的各个阶段都遵循一套完整的系统安全策略的安全数据库系统。

②数据库系统安全部件:是指以现有数据库系统所提供的功能为基础构建安全模块,以增强安全性。

此外,病毒防护、访问控制、网络传输安全(如加密)也是系统软件安全的重要组成。

1.2.2 交易安全

电子交易的安全则是指通过一系列的措施保证交易过程的真实可靠、完整、不可否认和机密,目的是在计算机网络安全的基础上确保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、可靠性、真实性和不可否认性等。它侧重于交易过程的安全。

电子交易安全的内容包括:如何确定通信中贸易伙伴的真实性,保证身份的可认证性;如何保证电子单证的机密性,防范电子单证的内容被第三方读取;如何保证被传输的业务单证不会丢失,或者发送方可以察觉所发单证的丢失;如何保证电子单证内容的真实性、准确性和完整性;如何保证存储信息的安全性;如何对交易数据信息进行审查并将审查的结果进行记录。

电子交易安全是计算机网络与信息安全的延伸,它是在传统密码学、计算机网络安全基础上,针对电子交易过程特有的要求,通过加密技术层、安全认证层和交易协议层一起来实现的。当然,计算机网络安全和交易安全并不是完全独立的,两种安全的实现有时依赖于一些共同的技术(如加密)。

1.2.3 电子商务安全的特点

电子商务安全具有系统性、相对性、有代价性和动态性这四个特点。

(1)系统性。电子商务安全不仅是一个技术性的问题,同时也是管理问题,而且它还与社会道德、法律法规、行业管理以及人们的行为模式等紧密联系在一起。

(2)相对性。任何安全都是相对的,没有绝对的安全。同样,对于电子商务安全来说,不能

也不必追求一个永远绝对攻不破的系统，安全与管理是联系在一起的。希望网站永远不受攻击，不出任何安全问题是不可能的。

(3)有代价性。任何电子商务系统，都应考虑到安全的代价和成本问题。如果只注重速度和便捷性，就必定要以牺牲安全来作为代价；如果一味只注重安全，便捷性就会大打折扣。例如，如果不牵涉支付问题，对安全的要求就可以低一些；如果牵涉支付问题，对安全的要求就要高一些，所有安全是有成本和代价的。作为一个管理者，应该综合考虑这两方面因素，作为安全技术的提供者，在研发技术时也要考虑到这些因素。

(4)动态性。因为网络技术的攻防是此消彼涨。尤其是安全技术，它的敏感性、竞争性和对抗性都是很强的，这就需要不断检查、评估和调整相应的安全策略。没有一劳永逸的安全，也没有一蹴而就的安全。

1.3 电子商务安全的基本需求

电子商务活动是通过 Internet 进行的，因此 Internet 所面临的安全威胁，也同样是电子商务所面临的威胁。

1.3.1 电子商务面临的安全威胁

在 Internet 发展的初期，其各种协议的设计都是以连通和数据传输为目的的，安全性并没有放在重要的位置来考虑。资源共享、快速、便捷是 Internet 迅速发展的原因，而这种开放性决定了基于 Internet 的电子商务在安全方面存在先天不足。

例如：在 Internet 上的信息是以数据包的形式传送的，这些数据包好比是一封封的平信，它们按照目的地址寄往某个地方，如果不知道目的地址具体对应哪台主机，就只发送到其所在的局域网，再由局域网将该数据包广播发送(通常采用的以太网或令牌网技术的局域网都是广播式的局域网)。这样局域网中的所有主机都能收到这个数据包。在一般情况下，如果其他主机发现这个数据包不是发送给它的就直接将其丢弃，但是对于别有用心的人来说，他可能会设置他的主机能接收所有数据包，无论是不是发给他的，并查看这些数据包中的内容，甚至对其中的内容进行篡改再发送出去。

如果把 Internet 系统的运转看成是一种信息的流动，则在正常情况下，信息是从信息源流向信息目的，这种正常的信息流动如图 1.2(a)所示。而攻击者可以破坏这种正常的信息流动，攻击者对网络系统的威胁可归纳为四种类型：中断、截获、篡改和伪造。

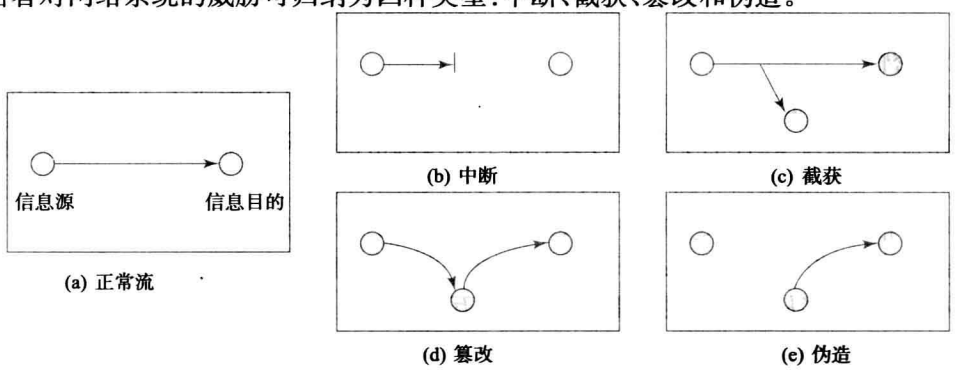


图 1.2 安全威胁的类型

1. 中断(interruption)

中断是指信息接收方无法收到发送方发来的信息。这通常是攻击者对服务提供者进行攻击,使其无法提供服务,这是对可用性进行攻击,如图 1.2(b)所示。

2. 截获(interception)

截获是被动攻击,它是指攻击者从网络上窃听他人的通信消息内容,破坏信息的机密性。如图 1.2(c)所示。

3. 篡改(modification)

篡改是指攻击者故意篡改线路上传输的报文,这是对完整性的攻击。如图 1.2(d)所示。

4. 伪造(fabrication)

伪造是指攻击者伪造信息在网络上传送,这是对报文真实性或身份认证机制的攻击。如图 1.2(e)所示。伪造分为两种情况,一是伪造消息(如伪造电子邮件),骗取用户汇款或输入账号密码到伪造者的网站等;二是伪造身份,如发送一条消息声称自己是某人,由此可见,伪造身份是通过伪造认证消息实现的。

5. 抵赖(repudiation)

当交易的一方发现交易行为对自己不利时,或当利益刺激到一定程度时,就有可能否认电子交易行为。交易抵赖包括发送方的抵赖和接收方的抵赖两种情况。如发送方发了某个订货消息后又声称自己没发过,或接收方收到某个订货消息后声称自己没收到。

1.3.2 电子商务安全要素

为了防御以上电子商务面临的各种安全威胁,一个安全的电子商务系统,应该实现的安全要素有以下几点,见表 1.1。

表 1.1 电子商务安全的要素

要素	含义
机密性	信息不被泄露给非授权用户
完整性	信息是未被篡改的
不可抵赖性	信息的收、发双方不能否认曾经收发过信息
即时性	在规定的时间内完成服务
真实性	确保对方的身份和信息的来源是真实的
访问控制	对访问者访问资源时的权限控制
可用性	访问者需要的时候,资源是可用的

1. 机密性

在电子商务系统中,交易中产生、传递的信息可能涉及商业机密或个人隐私,因此这些信息均有保密的要求。这种电子商务的安全需求称为机密性需求。机密性要求做到只有发送方和接收方才能访问消息内容,而不允许非授权人员访问消息内容。机密性一般是通过密码技术对传输的信息进行加密来实现的。在上节中的"截获"就是对机密性的攻击。

攻击机密性的一个例子是:CDNow 是美国一家网上销售音像制品的电子商务企业,2000 年,俄罗斯一名黑客从该公司网站上窃取了 30 万条信用卡记录,并向其敲诈 10 万美元。遭到 CDNow 公司拒绝后,黑客开始逐条公布所有信用卡的内容。导致 CDNow 公司不得不要求银行更换所有被公布的信用卡,所承担的更换信用卡的损失就达数百万美元,而这些机密信息被

窃取给公司带来的信誉损失和间接经济损失更是无法估量。

2. 完整性

完整性是指保证只有被授权的各方能够修改计算机中存储的或网络上传输的信息，修改包括对信息的写、改变状态、时延或重放。电子商务系统应防止对交易信息未授权的生成、修改和删除，同时防止交易信息在传输过程中的丢失或重复，并保证信息传递次序的统一。

如果消息内容在发送方发出后和到达接收方之前发生了改变，就表明消息失去了完整性。失去完整性可分为两种情况。第一种情况例如：假设 A 发出的消息内容是“将 100 元转给 D”，而 B(银行方)收到的消息却变成了“将 1 000 元转给 C”，则表明该消息已经失去了完整性，这种情况通常是消息被第三方故意篡改了。第二种情况可能是数据传输线路不可靠，使数据在传输过程中发生了不可预知的改变，但这种改变一般是可以察觉到的。

3. 不可抵赖性

有时发送方发出某个消息后，又想否认发过这个消息，或接收方收到消息，却否认已收到信息。例如用户 A 通过 Internet 向商家要求购买某种商品，商家按 A 的请求发货之后，A 声称没有发过这个购买请求，拒绝向商家支付。不可抵赖性(non-repudiation)可防止这类抵赖现象。

由于抵赖通常是发生在交易双方之间的行为。因此有文献认为，不可抵赖性是电子商务安全比网络安全多出来的一种安全需求。

4. 即时性

即时性是指服务可被授权实体访问并在规定的时间内完成服务的特性。电子商务的即时性需求要求电子商务网站的打开速度在可接受的时间内，数据库系统的性能足够高，使响应查询的时间很短等。即时性对网络带宽、系统硬件配置和软件性能都有要求。

在易趣网进入中国初期，由于其网站访问速度明显比较慢，使其失去了大量的潜在客户。这就是即时性需求未能得到满足的例子。

5. 真实性(认证)

真实性是指确保对方的身份是真实的和信息的来源是真实的。在电子商务中，由于交易双方无法见面，经常会发生攻击者伪造网站、伪造电子邮件地址，给用户发假冒的支付请求等攻击行为。例如用户 C 冒充用户 A 发一个转账请求给银行 B，请求银行将资金从 A 账户转到 C 账户，银行从 A 账户转账到了 C 账户，以为这是用户 A 要求的，这就是针对真实性进行的攻击。为了防止这类攻击，必须认证对方身份的真实性并鉴别接收到的消息的真实来源。真实性通常需要可靠的认证机制(包括消息认证和身份认证)来保障。

2005 年，黑客模仿中国工商银行、中国银行等金融机构的网页，采用诱骗用户输入账号和密码信息的方式来盗取账号信息，并从中获取利益。这种欺骗性的网站被人们形象地称为“钓鱼网站”。它是针对身份真实性进行的攻击。

6. 可用性

可用性是指保证信息和信息系统能随时为授权者提供服务，而不会出现由于非授权者干扰而对授权者拒绝服务的情况发生。例如，由于某个非法用户 C 的故意操作，使授权方 A 无法与服务器计算机 B 联系，从而破坏了可用性原则。

在电子商务活动中，消费者准备在网站上购买商品，需要了解商品价格、性能、质量等信息，决定购买后，要提交订购信息，提供支付相关的信息，这些环节都要求电子商务系统能够随

时提供稳定的网络服务，这就是对电子商务系统可用性的要求。

在我国，如果像淘宝、卓越这类的大型电子商务网站，由于受到攻击或发生故障而停止服务几分钟，就会有上千万次交易无法进行，估计的经济损失将超过几千万。

［提示］ 理解上述几种电子商务安全要素非常重要，因为本书将介绍的所有技术手段、管理措施，其根本目的都是为了实现一种或多种电子商务安全要素。

1.4 电子商务安全技术

为了保障电子商务安全的基本需求，人们采用了很多种技术，这些技术主要可分为密码学技术、网络安全技术和电子交易安全技术，包括：加密技术、认证技术、公钥基础设施、访问控制技术、网络安全技术、电子商务安全协议等。

1. 加密技术

加密技术是电子商务安全采取的最基本安全措施，也是其他很多安全技术的实现基础。加密技术分为对称加密技术和公钥加密技术。

(1)对称加密。利用对称加密技术可对通信的双方传输的数据进行加密，这样，如果信息不幸被攻击者截获，只要攻击者没获取到密钥，攻击者就无法解读，也无法修改加密之前明文的内容，对信息的机密性和完整性可提供一定的保证。

(2)公钥加密。利用公钥加密技术，可解决对称密码体制遇到的很多难题，公钥加密技术常用来完成密钥的分发和数字签名这些特殊的功能。

2. 认证技术

在网上交易过程中，由于交易双方不能见面，为了保证不被欺骗，需要保证交易的另一方的身份信息和交易信息都是真实的。认证技术就是用来认证对方的身份是真实的或收到的信息是真实的而没有被伪造或篡改过，为电子商务安全的真实性需求提供保障。认证分为消息认证和身份认证。认证系统有以下两种认证模式。

(1)当事人自由约定的认证体系：当事人可以约定好采取何种认证方式，对对方的身份进行认证，不需要第三方的参与。

(2)依赖可信第三方的认证体系：由可信第三方提供通信各方的身份证明，被认证方将可信第三方提供的身份证明(数字证书)提交给认证方进行认证。

3. 公钥基础设施

公钥基础设置 PKI 提供了一个框架，在这一框架下能实施各种安全服务，是目前比较成熟和完善的电子商务安全解决方案。PKI 的核心功能是提供认证服务，包括数字签名、身份认证、时间戳和不可否认服务等。

4. 访问控制技术

访问控制是建立在身份认证基础之上的安全服务，它的目的是控制和管理合法用户访问资源的范围和访问方式，防止合法用户对资源的误用和滥用，因而能保证资源受控地、合理地使用。访问控制不仅保护了客体的安全，维护了资源所有者的利益，更重要的是建立了良好的电子商务秩序。

5. 网络安全技术

网络安全是一个复杂的、系统的工程，需要从系统的观点出发，从多个环节综合运用一系