高等院校信息技术规划教材

电子商务安全

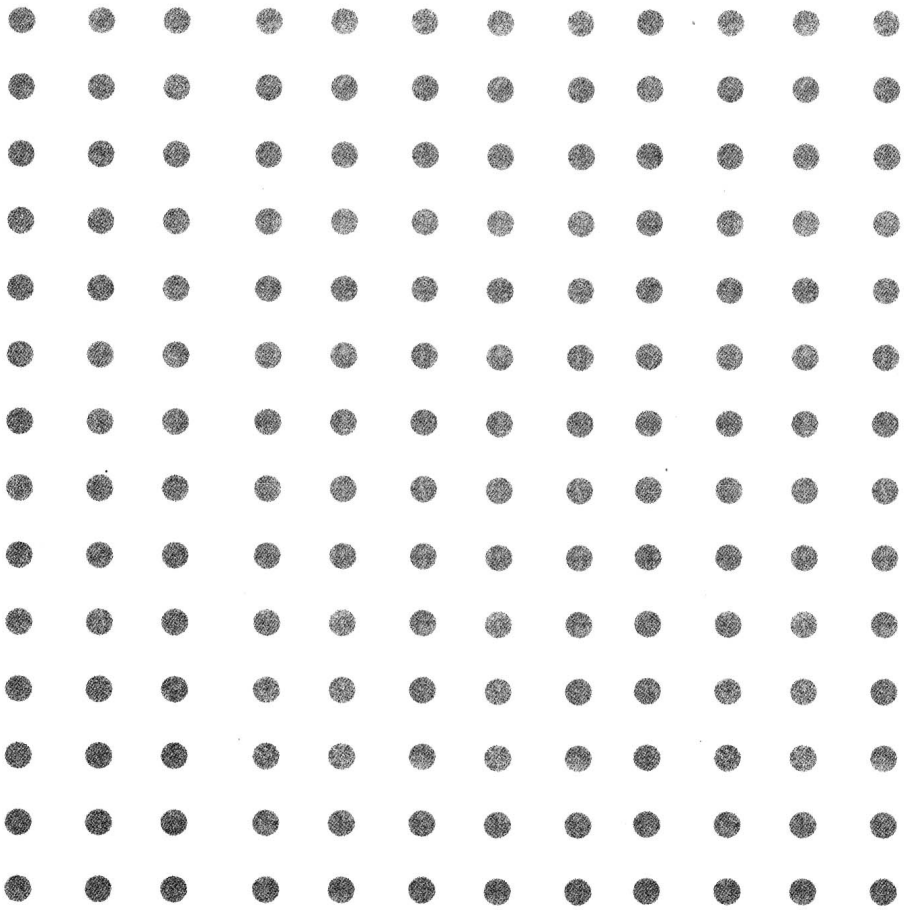
唐四薪　主编

清华大学出版社

高等院校信息技术规划教材

电子商务安全

唐四薪　主编



清华大学出版社
北京

内 容 简 介

本书按照电子商务安全的体系结构，全面介绍了电子商务安全有关技术和管理方面的问题，采用问题启发式的叙述模式，对电子商务安全的基本原理和核心技术做了详细通俗且符合认知逻辑的阐述。本书分为11章，包括电子商务安全概论、密码学基础、认证技术、数字证书和PKI、网络安全基础、防火墙和IDS、电子商务安全协议、电子支付及其安全、电子商务网站的安全、移动电子商务安全和电子商务安全管理的内容。

本书可作为高等院校电子商务、信息安全、信息系统与信息管理、国际贸易等专业本科生的教材，也可作为从事电子商务教学、科研和管理工作相关人员的参考用书。

本书封面贴有清华大学出版社防伪标签，无标签者不得销售。
版权所有，侵权必究。侵权举报电话：010-62782989　13701121933

图书在版编目（CIP）数据

电子商务安全/唐四薪主编. --北京：清华大学出版社，2013.5
高等院校信息技术规划教材
ISBN 978-7-302-31234-5

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(2013)第001726号

责任编辑：张　民　薛　阳
封面设计：常雪影
责任校对：时翠兰
责任印制：李红英

出版发行：清华大学出版社
网　　址：http://www.tup.com.cn，http://www.wqbook.com
地　　址：北京清华大学学研大厦A座　　**邮　　编**：100084
社 总 机：010-62770175　　**邮　　购**：010-62786544
投稿与读者服务：010-62776969，c-service@tup.tsinghua.edu.cn
质量反馈：010-62772015，zhiliang@tup.tsinghua.edu.cn
课件下载：http://www.tup.com.cn，010-62795954
印 刷 者：北京四季青印刷厂
装 订 者：三河市兴旺装订有限公司
经　　销：全国新华书店
开　　本：185mm×260mm　　**印　　张**：24　　**字　　数**：556千字
版　　次：2013年5月第1版　　**印　　次**：2013年5月第1次印刷
印　　数：1～2500
定　　价：39.00元

产品编号：047287-01

前言 foreword

目前电子商务正在迅速普及，但安全问题一直是电子商务发展的最大障碍。电子商务在给人们的生活和工作带来便利的同时，安全问题也日渐突出。

为此，绝大多数高校的电子商务、信息安全等专业都开设了“电子商务安全”的课程。“电子商务安全”这门课程在电子商务专业的课程体系中具有承前启后的作用。电子商务安全的先修课程是“电子商务概论”和“计算机网络”，后继课程有“电子商务系统设计”等。学习电子商务安全一方面可以加深对电子商务概论和计算机网络中相关知识的理解，另一方面由于安全是电子商务系统设计中最重要的考虑因素，电子商务系统中很多实现技术都与安全有关，因此又能加深对电子商务系统和电子商务关键技术的理解。

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。直到现在，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”的书籍中也出现了越来越多关于电子商务安全方面的知识，体现了电子商务安全已越来越被人们所重视。

当然，“电子商务安全”和“密码学与网络安全”又是有所区别的，电子商务安全的目的是紧紧围绕保障电子商务的安全，因此，密码学中一些与保障电子商务安全关系不大的技术就不是电子商务安全的研究范围，同时，密码学研究的内容偏向于底层密码算法或密码协议的实现和安全证明，而电子商务安全研究的内容则偏向于上层应用(如密码技术的应用)。因此，电子商务安全在教学中应把握这一侧重点，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，这表现在以下几个方面。

(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部分从略，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如加密和认证技术做了较详细通俗且符合认知逻辑的阐述，使读者能更深刻地理解电子商务安全问题产生的根源。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富有特色和实用性的内容，并对一些特殊的数字签名和散列链进行了论述，因为这些技术在目前电子商务前沿领域应用很广泛。在编写形式上，叙述详细，重点突出。在阐述基本原理时大量地结合实例来分析，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的是为学生打基础，对于技术知识，学生要自学掌握是比较困难的，因此教师有必要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将来在实际工作中掌握，只有有了一定的实践经验才能更有效地学习和理解安全管理方面的内容。

本书的知识结构可分为概述、原理、应用 3 大块，知识结构如下：第 1 章为概述，第 2～4 章为密码学的内容，第 5～7 章为网络安全技术的内容，第 8～10 章为电子商务安全具体的应用方面的内容，第 11 章为安全管理的内容。

本书的理论教学课时以 54 课时为宜。对于目录中带“*”号的部分，可以根据需要选择性讲解。本门课程还可以适当安排实验课，但建议应以理论讲授为主，实验课时不超过总课时的 1/4，附录 A 中给出了 6 个实验项目的设计和安排。

作为教材，本书注重教材立体化建设。本书每章后都提供了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、教学大纲和实验指导)，可登录本书配套网络教学平台(http://ec.hynu.cn)免费下载，也可和作者联系(tangsix@163.com)。

本书由唐四薪担任主编，唐四薪编写了第 1～9 章和第 10 章的部分内容。由何青、唐琼、谭晓兰、屈瑜君担任副主编，编写了第 11 章的内容。参加编写的还有陈溪辉、邓明亮、邢容、邹飞、刘艳波、戴小新、尹军、康江林、黄大足、唐亮等，他们编写了第 10 章的部分内容。

与本书配套的网络课程及课件获得了湖南省 2012 年普通高校教师现代教育技术应用竞赛三等奖。本书的写作还得到了衡阳师范学院教学研究课题(jykt201247)的资助。

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

2012 年 8 月

试读结束，需要全本PDF请购买 www.ertongbook.com

目录 contents

试读结束，需要全本PDF请购买 www.ertongbook.com

第1章 chapter 1

电子商务安全概述

电子商务(E-Commerce),是指在Internet上按照一定的标准开展商务活动。它是一种以Internet为媒介,以商品交易双方为主体,以银行电子支付为结算手段的全新商务模式。人们可以足不出户地在网上购买或出售商品(或服务),这种网上交易方式就是电子商务带给人们最直观的便利。

但是,在Internet上从事电子商务活动的前提是要解决商务过程中各个环节的安全性和可靠性问题。任何电子商务系统都必须提供高度的安全性、可靠性和可用性,才能赢得客户和商家的信赖。安全问题始终是电子商务活动的参与实体最为关心的问题。如何保障电子商务的安全,是电子商务的核心研究领域之一。

本章首先介绍电子商务安全的内涵,然后指出电子商务面临的各种安全威胁,接下来详细分析了电子商务安全的6大要素,所有的安全威胁都是针对安全要素中某一部分的攻击,而所有的安全技术和管理措施都是为了保证这些安全要素的实现,因此本书所有的内容都与这些安全要素密切相关。最后,介绍了电子商务安全的体系结构,它是保证电子商务安全的一个完整的多层次的逻辑结构。

1.1 电子商务安全的现状

电子商务已经逐渐成为人们进行商务活动的新模式,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。但安全问题却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会被盗用,或担心自己的客户信息会被窃取。

据中国互联网络信息中心(China Internet Network Information Center,CNNIC)2011年7月发布的《第28次中国互联网络发展状况统计报告》显示,中国网民规模已达4.85亿,网购用户规模达到了1.73亿,这意味着有1/7的中国人在进行网络购物。从这个意义上讲,电子商务与人们的生活已越来越密切,并已经渗透到各行各业。电子商务作为一种新的经济形式已经成为不争的事实,越来越多的企业开始重视电子商务的作用,搭建自己的电子商务网站和交易平台。

报告还指出,2011年上半年有85.7%的网民在网上查询过商品信息,但只有29%的网民实现了网上购物。这表明,网上购物的人群占网民总人数的比例还处于较低的水

平，可见目前大多数网民对电子商务还是持观望或不信任的态度。

许多网民不愿意网上购物固然与他们的购物习惯和上网熟练程度有关，但对于安全问题的担心也是一个不可忽视的重要因素。而且对于那些参与电子商务交易的网民来说，其购物也多集中在书籍、服饰、数码产品等价值较低的领域。表明我国电子商务发展的广度和深度均未达到其应有的水平，而解决安全问题是将电子商务向纵深推进的必要条件。

1.1.1 电子商务安全的重要性

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。总的来看，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。电子商务安全的重要性表现在以下两方面。

1. 安全问题是实施电子商务的关键因素

人类传统的交易是面对面进行的，可以当面识别对方身份，当面清点钱物，因而比较容易保障交易双方的信任关系和交易过程的安全性。而电子商务活动中的交易行为是通过网络进行的，买卖双方互不见面，因而缺乏传统交易中的信任感和安全感。

美国密执安大学一个调查机构通过对 23 000 名因特网用户的调查显示：

① 超过 60%的人由于电子商务的安全问题而不愿进行网上购物。

② 任何个人、企业或商业机构以及银行都不会通过一个不安全的网络进行商务交易，这样会导致商业机密信息或个人隐私的泄露，从而导致巨大的利益损失。

根据 CNNIC 发布的《中国互联网络发展状况统计报告》，在电子商务方面，52.26% 的用户最关心的是交易的安全可靠性。由此可见，电子商务中的网络安全和交易安全问题是实施电子商务的关键所在。

Internet 所具有的开放性是电子商务方便快捷、广泛接受的基础，而开放性本身又会使网上交易面临种种危险。例如，在开放的网络上处理交易，如何保证传输数据的安全成为电子商务能否普及的最重要的因素之一。

在电子商务安全程度还不能得到充分保障的情况下，我们怎么可以放心地把自己的银行账号放到网上？我们怎么知道网络另一端的交易对象不是一家骗子公司呢？在电子商务活动中，企业比以往任何时候都更需要知道其合作伙伴的真实身份，客户需要保证其保密信息不会被暴露。还有各种恶意的袭击会侵入电子商务网站，进行各种可能的破坏，如制造和传播破坏性病毒或让网站拒绝服务。这些攻击可能引起网站的服务崩溃，用户的保密信息泄露，从而最终导致公众信心的丧失，电子商务实施的瓦解。

从宏观上看，电子商务在我国各行各业逐步普及，应用不断深入，电子商务安全对国家安全的影响也在不断加深，这主要表现在两个方面：一是危及经济安全。随着电子商务活动的普及，越来越多的资金流在网络中流动，极大地诱惑不法分子犯罪，以网络为基础构建的银行、证券等金融系统成为现代社会运行的核心，一旦这些系统遭受攻击或者破坏而出现故障，便直接危及国家经济安全。例如采用网络攻击手段进行商业欺诈和勒

索，窃取、篡改和盗用信息，销售假货等类型的网络经济犯罪活动正急剧增加，这会对我国经济发展和金融秩序造成严重危害。二是影响社会稳定的银行、保险、税务、证券、民航、医疗等行业都开始实施电子商务，它们一旦出现比较严重的信息安全问题，则有可能会严重影响人民生活进而影响社会稳定。例如，铁道部的购票网站由于访问速度缓慢而饱受人们诟病，一度使春节购票成为广大人民群众关注的焦点问题。因此，安全建设工作必须贯穿电子商务建设的整个过程。

根据调查显示，目前电子商务安全主要存在的问题包括计算机网络安全、商品的品质、商家的诚信、货款的支付、商品的递送、买卖纠纷的处理、网站售后服务等 7 个方面。这 7 个方面的问题可以归结为两大部分：计算机网络安全和电子交易安全。

2. 安全是电子商务系统最重要的功能

一个真正的电子商务系统并非单纯意味着一个商家和用户之间开展交易的界面，而应该是利用各种技术手段向客户提供安全、可信的交易环境，并保障客户的隐私不被泄露，从而实现在 Internet 中安全地完成现实生活中的交易活动。

例如，一个简单的电子商务系统大致需要商品展示模块、订购模块（购物车模块）、支付模块、客户信息管理模块、用户注册和登录模块，以及后台的商品管理、订单处理、物流管理等模块。其中，除了商品展示模块外，其他功能模块都直接与安全密切相关。可以说，一个完善的电子商务系统有 80%以上的功能模块设计和硬件设备部署都要在整体安全策略的指导下考虑安全问题。

为了说明安全对于电子商务系统的重要性，下面来分析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 3 层，如图 1.1 所示。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，各层的功能如下。

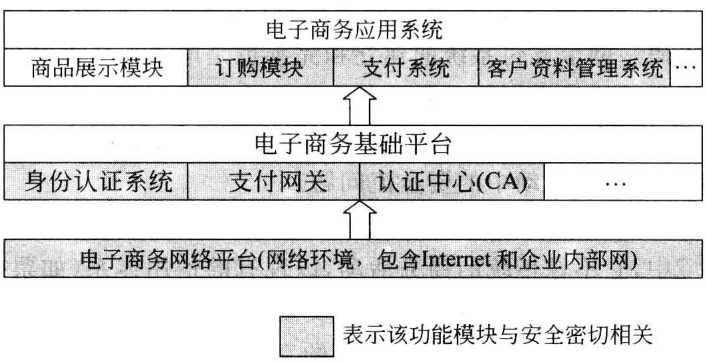


图 1.1 电子商务系统的组成

(1) 电子商务网络平台（网络环境），是指支撑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参与各方接入的手段，其结构一般包括软件和硬件两方面。网络环境是开展电子商务的基础，信息的传送、网上资金账户的认证、资金的划转等，都需要安全的网络环境。

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

利用网络互联设备将内部网与 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，是指为各种电子商务应用系统提供服务的基础设施。包括认证机构(Certificate Authority，CA)、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。

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，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 3000 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是技术问题，还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。

(3) 支付系统。如果仅仅利用网络发布或获取商务信息，在进行商品交易时还得借助于传统的银行业务，即支付手段不能在网上进行时，无疑会使交易的支付成为电子商务进一步发展的障碍。网上支付系统的建立和完善也是电子商务系统的重要目标之一。虽然网上银行与支付系统的发展不是目前各个商业企业所能解决的事情，但随着电子商务的进一步发展和金融环境的逐渐优化与完善，企业在时机成熟时，和网上银行建立合作关系，可以解决电子商务活动中的资金流问题。

(4) 安全认证系统。安全认证系统是电子商务成功实施的重要保障。电子商务建立在虚拟的网络环境中，它不像传统的商务活动，以现有的信用体系(如票据、现金、企业实力、担保等)为依托。因此，如何确保电子商务交易过程中的商业信用、如何确信交易双方的身份、如何保证网上账户和数据传送来源的真实性，都是安全认证系统需要完成的工作。

(5) 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(Customer Relationship Management，CRM)、企业资源计划(Enterprise Resource Planning，ERP)等)。

试读结束，需要全本PDF请购买 www.ertongbook.com