可下载教学资料

http://www.tup.tsinghua.edu.cn

高等学校教材

信息管理与信息系统

电子商务安全技术

张爱菊 主编

熊平 朱平 陆安生 等 编著

清华大学出版社

高等学校教材

信息管理与信息系统

电子商务安全技术

张爱菊 主编

熊平 朱平 陆安生 等 编著

清华大学出版社

北京

内容简介

本书内容分为8章。第1章介绍电子商务安全的基本概念、电子商务安全系统的体系结构及相关技术；第2章介绍信息加密技术与应用；第3章介绍计算机网络安全技术，包括防火墙、虚拟专用网、病毒知识等；第4章介绍公钥基础设施；第5章介绍电子支付技术；第6章介绍安全套接层协议，包括认证算法、实现和协议分析等；第7章介绍电子商务安全的SET安全电子交易协议；第8章介绍其他电子商务安全技术，包括无线电子商务安全技术、信息隐藏、数字水印和数字版权。

本书可作为电子商务、信息管理、计算机、国际贸易类专业本科生和研究生的教材，也可以作为相关领域高级管理人员的培训教材或参考用书。

图书在版编目(CIP)数据

电子商务安全技术/张爱菊主编. —北京：清华大学出版社，2006.12
(高等学校教材·信息管理与信息系统)
ISBN 7-302-13610-6

Ⅰ.电… Ⅱ.张… Ⅲ.电子商务—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091683号

责任编辑：丁　岭　张为民
责任校对：李建庄
责任印制：杜　波
出版发行：清华大学出版社　　**地　　址**：北京清华大学学研大厦
http://www.tup.com.cn　　**邮　　编**：100084
c-service@tup.tsinghua.edu.cn
社 总 机：010-62770175　**邮购热线**：010-62786544
投稿咨询：010-62772015　**客户服务**：010-62776969
印 装 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**：15.25　**字　数**：376千字
版　　次：2006年12月第1版　　**印　　次**：2006年12月第1次印刷
印　　数：1～3000
定　　价：24.00元

本书如存在文字不清、漏印、缺页、倒页、脱页等印装质量问题，请与清华大学出版社出版部联系调换。联系电话：(010)62770177转3103　　产品编号：022124-02

读者意见反馈

亲爱的读者：

感谢您一直以来对清华版计算机教材的支持和爱护。为了今后为您提供更优秀的教材，请您抽出宝贵的时间来填写下面的意见反馈表，以便我们更好地对本教材做进一步改进。同时如果您在使用本教材的过程中遇到了什么问题，或者有什么好的建议，也请您来信告诉我们。

地址：北京市海淀区双清路学研大厦 A 座 602 室　计算机与信息分社营销室　收

邮编：100084　　电子信箱：jsjjc@tup. tsinghua. edu. cn

电话：010-62770175-4608/4409　　邮购电话：010-62786544

教材名称：电子商务安全技术

ISBN：7-302-13610-6/TP・8220

个人资料

姓名：_____　年龄：_____所在院校/专业：_____

文化程度：_____　通信地址：_____

联系电话：_____　电子信箱：_____

您使用本书是作为：□指定教材 □选用教材 □辅导教材 □自学教材

您对本书封面设计的满意度：

□很满意 □满意 □一般 □不满意　改进建议_____

您对本书印刷质量的满意度：

□很满意 □满意 □一般 □不满意　改进建议_____

您对本书的总体满意度：

从语言质量角度看　□很满意 □满意 □一般 □不满意

从科技含量角度看　□很满意 □满意 □一般 □不满意

本书最令您满意的是：

□指导明确 □内容充实 □讲解详尽 □实例丰富

您认为本书在哪些地方应进行修改？(可附页)

_____

_____

您希望本书在哪些方面进行改进？(可附页)

_____

_____

电子教案支持

敬爱的教师：

为了配合本课程的教学需要，本教材配有配套的电子教案（素材），有需求的教师可以与我们联系，我们将向使用本教材进行教学的教师免费赠送电子教案（素材），希望有助于教学活动的开展。相关信息请拨打电话 010-62776969 或发送电子邮件至 jsjjc@tup. tsinghua. edu. cn 咨询，也可以到清华大学出版社主页(http://www. tup. com. cn 或 http://www. tup. tsinghua. edu. cn)上查询。

出版说明

改革开放以来，特别是党的十五大以来，我国教育事业取得了举世瞩目的辉煌成就，高等教育实现了历史性的跨越，已由精英教育阶段进入国际公认的大众化教育阶段。在质量不断提高的基础上，高等教育规模取得如此快速的发展，创造了世界教育发展史上的奇迹。当前，教育工作既面临着千载难逢的良好机遇，同时也面临着前所未有的严峻挑战。社会不断增长的高等教育需求同教育供给特别是优质教育供给不足的矛盾，是现阶段教育发展面临的基本矛盾。

教育部一直十分重视高等教育质量工作。2001 年 8 月，教育部下发了《关于加强高等学校本科教学工作，提高教学质量的若干意见》，提出了十二条加强本科教学工作提高教学质量的措施和意见。2003 年 6 月和 2004 年 2 月，教育部分别下发了《关于启动高等学校教学质量与教学改革工程精品课程建设工作的通知》和《教育部实施精品课程建设提高高校教学质量和人才培养质量》文件，指出“高等学校教学质量和教学改革工程”是教育部正在制定的《2003—2007 年教育振兴行动计划》的重要组成部分，精品课程建设是“质量工程”的重要内容之一。教育部计划用五年时间（2003—2007 年）建设 1500 门国家级精品课程，利用现代化的教育信息技术手段将精品课程的相关内容上网并免费开放，以实现优质教学资源共享，提高高等学校教学质量和人才培养质量。

为了深入贯彻落实教育部《关于加强高等学校本科教学工作，提高教学质量的若干意见》精神，紧密配合教育部已经启动的“高等学校教学质量与教学改革工程精品课程建设工作”，在有关专家、教授的倡议和有关部门的大力支持下，我们组织并成立了“清华大学出版社教材编审委员会”（以下简称“编委会”），旨在配合教育部制定精品课程教材的出版规划，讨论并实施精品课程教材的编写与出版工作。“编委会”成员皆来自全国各类高等学校教学与科研第一线的骨干教师，其中许多教师为各校相关院、系主管教学的院长或系主任。

按照教育部的要求，“编委会”一致认为，精品课程的建设工作从开始就要坚持高标准、严要求，处于一个比较高的起点上；精品课程教材应该能够反映各高校教学改革与课程建设的需要，要有特色风格、有创新性（新体系、新内容、新手段、新思路，教材的内容体系有较高的科学创新、技术创新和理念创新的含量）、先进性（对原有的学科体系有实质性的改革和发展，顺应并符合新世纪教学发展的规律，代表并引领课程发展的趋势和方向）、示范性（教材所体现的课程体系具有较广泛的辐射性和示范性）和一定的前瞻

性。教材由个人申报或各校推荐(通过所在高校的“编委会”成员推荐),经“编委会”认真评审,最后由清华大学出版社审定出版。

目前,针对计算机类和电子信息类相关专业成立了两个“编委会”,即“清华大学出版社计算机教材编审委员会”和“清华大学出版社电子信息教材编审委员会”。首批推出的特色精品教材包括:

(1) 高等学校教材·计算机应用——高等学校各类专业,特别是非计算机专业的计算机应用类教材。

(2) 高等学校教材·计算机科学与技术——高等学校计算机相关专业的教材。

(3) 高等学校教材·电子信息——高等学校电子信息相关专业的教材。

(4) 高等学校教材·软件工程——高等学校软件工程相关专业的教材。

(5) 高等学校教材·信息管理与信息系统。

(6) 高等学校教材·财经管理与计算机应用。

清华大学出版社经过20多年的努力,在教材尤其是计算机和电子信息类专业教材出版方面树立了权威品牌,为我国的高等教育事业做出了重要贡献。清华版教材形成了技术准确、内容严谨的独特风格,这种风格将延续并反映在特色精品教材的建设中。

清华大学出版社教材编审委员会

E-mail: dingl@tup.tsinghua.edu.cn

前言

随着电子商务如火如荼的发展，这种全新的商务模式对管理水平、信息传递技术都提出了更高的要求，作为保障电子商务活动正常进行的核心内容——电子商务安全技术，受到了人们的密切关注。目前，很多国家都开展了电子商务安全技术研究，针对不同的电子商务活动，建立了许多电子商务安全系统。电子商务安全技术涉及面广，包括密码技术、网络安全技术、公钥基础设施和各种应用技术等。

有关电子商务安全技术的书很多，其中不乏精品教材。然而，笔者在实际的教学过程中感到这些书籍中适合文科类的不多见：有的侧重于注重技术，深奥难懂，系统性不够；有的过于强调系统性，强调概念，忽视具体的内容，书读到最后，学生往往感觉仍不能将学到的理论运用于具体的实践。“电子商务安全技术”这门课程属于电子商务专业的核心基础课，涉及的技术非常广泛，但在有限的时间里不可能对所有的技术都作清晰的介绍，只能有所取舍，对一些基础的、核心的、前沿的技术作重点阐述，其他技术只能作简单介绍。本书在内容编排上，力求贴近实际专业和对象，在阐述各种电子商务安全技术时，多精选实例来讲解，理论联系实践，由浅入深，循序渐进，以求得实效；在章节安排上，按照电子商务安全系统的功能结构和逻辑层次来逐步推进，先讲解电子商务安全的基础结构再讲综合应用，先讲基本技术再讲核心技术，使读者对电子商务安全技术的掌握更加得心应手。

本书内容分为8章。第1章主要对电子商务安全的基本概念、电子商务安全系统的体系结构及相关技术进行介绍；第2章主要对信息加密技术与应用进行介绍，由浅入深介绍了各种加密技术；第3章对计算机网络安全技术进行详细介绍，包括防火墙、虚拟专用网、病毒知识等；第4章对公钥基础设施进行介绍；第5章对电子支付技术进行介绍，主要介绍了电子支付和网上银行系统；第6章介绍安全套接层协议，包括认证算法、实现和协议分析等；第7章介绍了电子商务安全的另一个协议——SET安全电子交易协议；第8章介绍其他电子商务安全技术，这是对前面章节的补充，包括无线电子商务安全技术、信息隐藏、数字水印和数字版权。

纵观本书的章节安排，可以看出，本书编写的特色在于：

(1) 由浅入深，循序渐进。将复杂的电子商务安全技术，如加密技术、公钥基础设施、各种协议等，按逻辑思维来进行编写，有利于读者对知识的融会贯通。

(2) 理论和实践相结合。每个章节主要通过实例来阐述复杂理论，将枯燥的理论

融于具体的实例当中，使理论教学丰富起来，有利于读者对电子商务安全技术的实践与掌握。

（3）博采众长，独树一帜。结合加密技术、计算机网络知识和无线局域网技术等，从电子商务安全的角度来阐释安全，这些特点令人耳目一新。

（4）有主有次。在章节内容的安排上，强调技术的实用性和先进性，围绕电子商务活动，重点介绍电子商务安全的基本技术及其实现方法，以适当篇幅介绍前沿技术，对一些用得少或较深奥的安全理论只作原理性介绍。

本书可作为电子商务、信息管理、计算机、国际贸易类专业本科生和研究生的教材，也可以作为相关领域高级管理人员的培训教材或参考用书。

本书由中南财经政法大学信息学院计算机系的张爱菊担任主编，中南财经政法大学信息学院计算机系的熊平和朱平，以及武汉工业学院计算机系的陆安生等参与编写，武汉大学的李少雄给予本书许多参考性的意见，并提供了大量文献资料。编写人员及具体分工如下：张爱菊编写第1、2、4和8章，朱平编写第3章，熊平编写第6、7章，陆安生编写第5章。在此要感谢刘腾红、朱少林和肖慎勇三位老师，他们对本书的编写提出了许多宝贵的意见，特别是朱少林老师对书的整个编写过程进行了指导。

本书在编写过程中，参考了部分图书资料和大量的网站资料，最后均以参考文献的形式列出。由于水平有限，对相关技术的把握不当之处，敬请读者不吝赐教。

编者

2006年11月

目 录

第1章

电子商务安全概论

随着信息技术日新月异的发展，基于 Internet 网络技术的电子商务已逐渐成为人们进行商务活动的新模式。电子商务就是利用电子数据交换(EDI)、电子邮件(E-mail)、电子资金转账(EFT)及 Internet 等技术在个人、企业和国家之间进行无纸化的业务信息的交换。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。电子商务被认为是通过信息技术(IT)将企业、用户、供应商及其他商贸活动涉及的职能机构结合起来的应用，是完成信息流、物流和资金流转移的一种行之有效的方法。电子商务作为一种新的流通方式，具有贸易效率高、交易成本低、加速商务发展的特点，在商务活动中正发挥着越来越重要的作用。

根据中国互联网络信息中心 2006 年 7 月发布的《中国互联网络发展状况统计报告》，我国网民总人数为 1.23 亿，其中使用在线音乐收听及下载(在线广播)、在线影视收看及下载(在线电视)、文件上传下载(不包含音乐、影视下载)，以及网上购物等网络服务的比例分别占到 38.3%、37.1%、33.8%和 24.5%。2004 年，中国电子商务的增长率为 73.7%，营业额达到 4800 亿人民币，约为全球电子商务营业额的 2%。网上支付市场在最近几年属于快速发展阶段，2005 年网上支付金额全年超过 60 亿，而网上支付用户占使用互联网用户数的比例从 2004 年前的 17%增长到 26%。网上支付平台市场在 2001 年是 1.6 亿元，2004 年则迅速增长为 23 亿元，预测 2007 年中国第三方网上支付平台市场规模将达 215 亿元左右。

2004 年，全球电子商务的增长率为 25.3%，整体营业额为 27 748 亿美元，通过电子商务实现的交易占全球贸易的 15%～20%。另外，专家预计美国的网上零售额将从 2005 年的 1720 亿美元增加到 2010 年的 3290 亿美元，保持平均每年 14%的稳定增长率，电子商务交易将占据美国零售总额的 13%。在所有的网上销售领域中，在线旅游继续成为最大的网上零售行业，将从 2005 年的 630 亿美元增加到 2010 年的 1190 亿美元。通用商品(包括汽车、食品饮料和旅游在内的所有零售目录商品)的网上销售也将在 2005 年首次超过 1000 亿美元。

随着电子商务如火如荼的发展，这种全新的商务模式对管理水平、信息传递技术都提出了更高的要求，其中安全体系的构建又显得尤为重要。本节将对电子商务的安全问题作一个基本的概述，并将主要从技术上对电子商务安全进行介绍。

1.1 电子商务安全问题

资源共享、快速、便捷是电子商务迅速发展的原因，而这种开放性使电子商务在安全方面先天不足。目前，电子商务安全问题变得越来越突出，已经成为制约电子商务快速发展的

障碍。如何保障电子商务活动的安全，一直是电子商务研究的核心问题。基于 Internet 技术的电子商务安全，很大程度上依赖于网络的安全性，然而，网络安全事故总是时有发生。

2001 年，计算机病毒在我国感染情况严重，特别是“红色代码”二型、“尼姆达”(Nimda)等恶性病毒在我国大面积传播，造成一些政府机构、教育科研单位等行业的网络通信阻塞，甚至出现服务器瘫痪。2002 年，以电子邮件、特洛伊木马、文件共享等为传播途径的混合性病毒肆虐，影响最大的“求职信”病毒持续六个月高居感染率第一。再如，从 2003 年 1 月 25 日中午开始，一种蠕虫病毒在 Internet 上快速蔓延。美国一家网络监测公司报告说，北美、欧洲和亚洲的因特网交通均发生了大面积堵塞，估计至少有 2.2 万个网络服务器遭到了病毒攻击，其中受影响最严重的地区是欧洲北部、美国东部和亚洲的一些地区。美国美洲银行称 1.3 万台自动取款机瘫痪，大量银行客户无法使用取款机取款。在亚洲地区，韩国受害最重。1 月 25 日下午 2 点左右，韩国 Internet 用户发现网络连接困难，负责 Internet 服务的韩国电信公司部分域名服务器受到大量数据连续攻击，服务器几乎陷于瘫痪。韩国通过 Internet 提供的服务项目如各种票务预订、网上购物、电子邮件、网络电话等都受到了极大损失，遍布韩国的网吧经营也遭到打击。在事故发生后韩国情报通信部立即宣布进入紧急工作状态，韩国电信公司也组织专家组成对策小组恢复系统。2003 年 8 月 11 日，一种名为“冲击波”(WORMMSBLAST. A)的新型蠕虫病毒在国内互联网和部分专用信息网络上传播。全国有上万台电脑遭感染。其变种病毒 WORM-MSBLAST. D 在全球感染了数百家企业。

2005 年，“MSN 性感鸡”、“狙击波”、“手机病毒”、“以名人和新闻为载体的病毒”等病毒一波又一波，给网络安全带来了严重的考验。其中，以商业为目的，以欺骗用户为手段的间谍软件，如网络钓鱼软件、鱼叉网络钓鱼软件成为网络安全最严重的威胁。据《金山 2005 年安全报告》显示，干扰人们日常工作、数据安全和个人隐私的各类间谍软件的危害已经超越传统病毒，成为互联网安全最大的威胁，感染率由 2004 年的 30%激增到 2005 年的 90%。2005 年，黑客模仿中国工商银行、中国银行等金融机构设计了类似的网页，用来盗取用户账号和密码信息，并从中获取利益。这一现象在 2005 年以平均每个月 73%的数字增长，使很多用户对网络交易的信心大减。

2005 年，美国超过 300 万的信用卡用户资料外泄，导致用户财产损失严重。美国 FBI 在其 2005 年计算机犯罪调查报告中指出，在对 2000 多家公司进行了调查后发现，这些公司中有 87%承认曾经遭受过某种类型的攻击。其中，攻击次数最多的为病毒、间谍软件和端口扫描，分别占 83.7%、79.5%和 32.9%。这些攻击的共同点是使用病毒或者间谍软件渗透进企业网络，更先进的攻击包括破坏数据和端口控制，这些攻击给许多企业带来了严重的损失。

除了网络安全问题外，在电子商务的实施过程中，还涉及安全技术、人员和设备管理、法律法规等安全问题。大量的事实表明，安全是制约电子商务发展的关键问题，安全得不到保障，即使使用 Internet 再方便，电子商务也无法得到广大用户的认可。

1.2　电子商务安全要素及相应的安全措施

1.2.1　电子商务安全要素

电子商务安全要素涉及面广，在使用电子商务的过程中主要的安全要素有以下几点。

1. 真实性

真实性是指网上交易双方身份信息和交易信息要真实有效。双方交换信息之前通过数字签名、身份认证以及数字证书来辨别参与者身份的真伪，防止伪装攻击。交易时，对提供的交易信息也要保证其真实性，防止欺骗交易行为。

2. 保密性

电子商务作为贸易的一种手段，其信息直接代表着个人、企业或国家商业信息，有些可能已经是商业机密。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。电子商务建立在开放的网络环境之上，并且功能越是强大的电子商务系统，其开放性越大，在这样的开放环境下，如何维护商业机密是电子商务全面推广应用的重要保障。信息的保密性要求信息在传输过程或存储中不被他人窃取。

3. 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完整性和统一性的问题。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。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。完整性包括信息传输和存储两个方面。在存储时，要防止非法篡改和破坏网站上的信息。在传输过程中，接收端收到的信息与发送的信息完全一样，说明在传输过程中信息没有遭到破坏。

4. 不可否认性

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、单据等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模式下，通过手写签名和印章进行贸易方的鉴别已是不可能的。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，这种标志信息用来保证信息的发送方不能否认已发送的信息，接收方不能否认已收到的信息，身份的不可否认性常采用数字签名来实现。

5. 可靠性

可靠性是指防止计算机失效、程序错误、传输错误、自然灾害等引起的计算机信息失效或失误。保证存储在介质上的信息的正确性。