21世纪高等院校电子商务教育系列教材

电子商务安全

（第二版）

李洪心　编著

E-Commerce Security

东北财经大学出版社
Dongbei University of Finance & Economics Press

21世纪高等院校电子商务教育系列教材

电子商务安全

（第二版）

李洪心　编著

E-Commerce Security

东北财经大学出版社
Dongbei University of Finance & Economics Press

大连

图书在版编目（CIP）数据

电子商务安全／李洪心编著．—2版．—大连：东北财经大学出版社，2012.4
（21世纪高等院校电子商务教育系列教材）
ISBN 978-7-5654-0649-2

Ⅰ．电… Ⅱ．李… 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（2011）第265726号

东北财经大学出版社出版
（大连市黑石礁尖山街217号 邮政编码 116025）
教学支持：（0411）84710309
营 销 部：（0411）84710711
总 编 室：（0411）84710523
网 址：http://www.dufep.cn
读者信箱：dufep@dufe.edu.cn
大连美跃彩色印刷有限公司印刷 东北财经大学出版社发行

幅面尺寸：186mm×230mm	字数：472千字 印张：23
2012年4月第2版	2012年4月第2次印刷
责任编辑：李 彬	责任校对：刘咏宁 孙 萍
封面设计：冀贵收	版式设计：钟福建

ISBN 978-7-5654-0649-2
定价：38.00元

总序

互联网的出现为全社会提供了一种全新的商务活动方式，从而引发了对电子商务学习、实践和培训的热潮。为满足目前高等教育对电子商务教材的需求，东北财经大学出版社在2008年伊始开发了一套全新的“21世纪高等院校电子商务教育系列教材”。整套教材围绕电子商务的应用性知识分为三个模块、十三种教材：第一个模块是“原理模块”，着力覆盖电子商务的基本原理，包括《电子商务基础教程》、《电子商务与网络经济》、《电子商务系统建设与管理》、《电子商务管理》；第二个模块是“电子商务支持模块”，为学习者讲解对电子商务行为进行支持的主要体系，包括《电子商务案例》、《电子商务法》；第三个模块是“电子商务中的行为模块”，细致刻画了电子商务环境下的个体和企业的行为，包括《电子商务物流管理》、《电子商务交易的支付与结算》、《电子商务安全》、《电子商务网站建设与管理》、《客户关系管理》、《网络营销》、《电子政务》。

这套“21世纪高等院校电子商务教育系列教材”本着科学、先进、合理、可行的原则，在编写过程中努力达到如下要求：

第一，博采众长。从总体上看，由于发达国家发展市场经济的历史较长，市场经济体制也比较成熟，因而其电子商务理论及相应的学科建设确实比我国领先一步，所以学习和借鉴发达国家的电子商务理论成果十分必要。同时，我国在经历了30多年的改革开放后，企业的体制、机制改革和技术进步已取得了巨大的成绩，在电子商务实践方面也积累了不少很有特色的成功经验，值得总结提炼。在教材的编写过程中，编者们广泛参考和吸取国内外相关教材的优点，尽量做到既符合国际发展潮流，又切实反映中国电子商务实际情况。

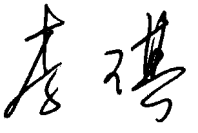
第二，努力创新。虽然我国部分高校开办电子商务专业的时间不长，但电子商务专业的建设已经从“摸着石头过河”到“如何适应市场经济中电子商

务发展的需要”发生了重要的转变。为此，电子商务专业及其教材建设在我国面临重大变革。本套教材力求在内容和形式上都有所创新：在内容方面，更新了不适应市场经济环境中当前电子商务实践及未来发展的理论和观念；在形式方面，每种教材在结构、栏目、体例及写作风格上均有所创新，且各种教材均由“主教材”和“电子课件”两者组成，大大方便了教与学。

第三，讲求实用。这主要表现在：一方面，内容上突出特色，兼顾理论系统性与实践可操作性。出于篇幅和知识点交叉的考虑，这套教材中每一种都力求围绕各自中心内容阐述，并根据实际课时量的要求在内容上取舍得当。例如，在《电子商务基础教程》中已经详细介绍过的内容，在其他教材中就尽量避免或者简略介绍。另一方面，成熟性与创新性相结合。本次编写的教材，坚持了教材内容的成熟性与创新性的统一。在阐述成熟而稳定的教材内容的同时，适当介绍新知识、新技能、新发展趋势，使教材具有适度的超前性和前瞻性。另外，本套教材的体例要求也符合教学的规律和方法。教材各章附有“学习目标”、“本章小结”、“复习思考题”、“技能实训题”等栏目，并且注重时效性，教材中的例题、案例等均取材于最新的实践成果。

第四，注重质量。本套教材由众多国内电子商务领域的专家、学者领衔编撰。他们多年从事该领域的教学与研究，具有丰富的教学及教材编写经验。他们中的大多数曾在欧美高校进修学习、合作研究或访问交流，因而对各学科的最新进展比较熟悉。他们长期关注中外企业电子商务实践，善于总结提炼。此外，各门课程教材的基本体系、结构和内容都经过各教材领衔作者的集体讨论，互提意见和建议，集思广益，严把质量关。

尽管编者们已经付出了最大努力，使现在所奉献给读者的这套教材体现了上述特点，但作为创新的初步尝试，难免会存在不足乃至缺陷。因此，这套教材的推出应该是任重而道远。我们希望能够尽快得到来自各方面尤其是读者方面的反馈意见，以为我们在不久的将来再版修订提供有益的参考。我们也希望并有信心通过不断修订，使教材紧随时代步伐，及时反映学科的最新进展，为培养未来的电子商务专业人才做出持续的贡献。



于西安交通大学

第二版前言

本书修订的背景是：

第一，电子商务平稳发展。

CNNIC《第28次中国互联网络发展状况统计报告》显示，截至2011年6月，中国网民规模达到4.85亿人，互联网普及率攀升至36.2%，在经历了2009—2010年快速增长之后，商务类应用迎来了相对平缓的发展期。目前，大部分商务类应用依然处在上行通道，如网络购物用户规模达到1.73亿，使用率提升至35.6%，半年用户增长了7.6%；团购应用发展势头迅猛，使用率从4.1%提升到8.7%，增幅达到125%。中国网上支付用户数从2010年底的1.37亿增至2011年中的1.53亿，用户增长11.7%。网上银行的用户使用率也小幅上升。电子商务市场的发展势头说明网民对网络安全的信心有所增强。

第二，网络安全诚信问题严峻。

随着互联网的发展，尤其是商务类应用的快速发展，许多不法分子纷纷将牟利黑手伸向互联网，导致近年来网络安全威胁和诚信危机事件频发。虽然近年来政府不断加大对网络安全问题的集中治理力度，网络安全诚信问题有了明显的改善，但形势依旧严峻，问题仍不容忽视。

CNNIC《第28次中国互联网络发展状况统计报告》显示，2011年上半年，遇到过病毒或木马攻击的网民达到2.17亿人，比例为44.7%；有过账号或密码被盗经历的网民达到1.21亿人，占24.9%，较2010年增加3.1个百分点；有8%的网民在网上遇到过消费欺诈，该群体网民规模达到3 880万人。

第三，互联网络安全问题突出。

由于目前流行的各种热门网站、客户端软件和浏览器，都存在着众多漏洞和安全薄弱点，使得用户遭到攻击的渠道暴增；而且，随着黑客病毒产业链臻于完善，支撑互联网发展的多种商业模式都遭到了盗号木马、木马点击器的侵

袭，使得用户对于网络购物、网络支付、网游产业的安全信心遭到打击。长此以往，必将影响整个互联网的健康发展。

当前网络安全形势严峻的原因主要有以下几个：一是由于近年来中国互联网持续快速发展，我国网民数量、宽带用户数量、.cn 域名数量都已经跃居全球第一位，而我国网络安全基础设施建设、民众的网络安全意识培养还跟不上互联网发展的步伐，庞大的用户群、信息系统群加之粗放式网络安全管理埋下了安全隐患；二是随着技术的不断提高，攻击工具日益专业化、易用化，攻击方法也越来越复杂、隐蔽，防护难度加大；三是互联网业务与现实社会中诸如货币、交易、讯息交互等活动不断融合，为网络世界的虚拟要素附加了实际价值，越来越多的承载这类业务的信息系统成为黑客攻击的目标。

传统的安全模式亟待变革，否则无论是安全厂商还是互联网用户，都将被淹没在病毒与黑客攻击的海洋中，互联网的各项基础应用和发展也将极大受损。互联网安全专家表示，互联网安全诚信问题受到来自科技、社会、法制等多方面因素制约，因此需要政府相关管理部门、互联网相关企业和全体网民共同行动起来，从完善域名安全保障机制、加强企业网络安全防护体系、提升网民辨别网络安全诚信能力等各环节出发，才能真正建立起各类综合防范机制，实现安全可信的互联网环境。

因此，加强电子商务系统的安全教育刻不容缓，我们于 2008 年出版的《电子商务安全》也有必要根据新形势重新进行修订。

本次修订的内容有：

第一，对各章相关的过时数据和内容进行了更新。

第二，删除了“4.4.3 数字证书”、“15.1.1 容错技术的种类”、“图 4—13 安全交易过程”和“4.1.3 SHA-1 算法”。

第三，修改了“8.4 电子支付安全的法律政策保障”，这是由于《非金融机构支付服务管理办法》已于 2010 年 6 月正式颁布。

第四，“11.5.4 CNCERT/CC2003 年应急处理案例”由“11.5.4 CNCERT 2008 年上半年应急处理案例”代替。

本书的修订由李洪心教授策划与设计，盖印修改了第 12 章、第 13 章，姜明修改了第 14 章，李洪心修改了其余各章并汇总统稿。在修订本书过程中，作者查阅和借鉴了一些相关网站上的内容，作者衷心感谢所有为本书写作提供了丰富参考内容的学者们，感谢东北财经大学的研究生王婷婷、张晓娜、李婷、李燕、梁锋、李冬杰、王玉刚、初阳、李巍、才雨和郑艺，他们在本书资料的收集整理和 PPT 课件的制作方面做了大量的工作。书中的不当之处，也恳请专家与读者指正。

作　者

2012 年 3 月

第一版前言

互联网络的普及促进了电子商务的快速发展，但人们在享受电子商务带来的便利和高效的同时，也面临着电子商务安全的严峻考验。计算机系统安全、网络与信息系统安全、交易和支付系统安全逐渐成为广大电子商务用户特别关注的问题，同时政府、国防、公安、金融机构、各大企业和电子商务运营商也急需了解电子商务的安全隐患、熟悉安全防范措施，以及出现了安全问题能及时处理的专业人员。

面对着电子商务的飞速发展以及电子商务教育体系的不断完善，2008 年年初，教育部高等学校电子商务专业教学指导委员会发布了高等学校普通本科电子商务专业教育知识体系。这套知识体系的提出为高等学校电子商务专业教学计划，特别是核心课程体系的设计给出了设计原则。

为解决电子商务发展中出现的安全问题和满足电子商务专业本科教学的需要，规范电子商务领域的安全教育，加快信息系统和网络安全人才的培养，我们参考教育部高等学校电子商务专业教学指导委员会制定的电子商务专业知识体系框架，编写了《电子商务安全》。本教材在内容安排上既考虑到不同学科背景电子商务专业本科生的课程教学，又充分考虑了电子商务专业教育知识体系中核心知识单元和可选知识单元中的关键知识点。全书覆盖了电子商务相关的技术知识领域中电子商务安全技术知识模块的全部内容，并且注重了知识的系统性和覆盖面的广泛性。

本书共 16 章，分四大部分：第一部分是理论基础，从第 1 章到第 3 章，介绍计算机系统和信息系统安全问题的基本理论和电子商务安全的概念，包括电子商务安全概述、系统安全的可靠性和加密与识别技术；第二部分是电子商务安全的核心技术，从第 4 章到第 9 章，介绍数字签名技术、公钥基础设施 PKI、电子商务的认证技术、电子商务安全技术协议、电子支付安全、电子商

务中的身份认证和访问控制；第三部分是电子商务系统安全环境，从第 10 章到第 13 章，包括防火墙与虚拟专用网、拒绝服务攻击及应急处理、计算机病毒和系统入侵及检测；第四部分从第 14 章到第 16 章，介绍电子商务发展过程中遇到的新问题以及应对措施，包括移动商务安全、电子商务系统的容错性分析和电子商务系统审核与取证。为了方便不同知识背景电子商务专业的教师和学生使用本书，作者在某些章节中用星号 * 注明了有一定难度和开放性的选学内容。另外本书在基于角色的访问控制 RBAC 的应用和电子商务的容错性系统研究方面给出了对电子商务研究和应用的最新成果，供感兴趣的电子商务专业本科高年级学生和研究生进一步研究参考。

本书的框架由李洪心教授设计，并负责统纂、修改和定稿，盖印编写了第 12 章、第 13 章，姜明编写了第 14 章，李洪心编写了其余各章并汇总统稿。在撰写本书过程中，作者查阅和借鉴了大量已发表的论文和书籍，还有一些相关网站上的内容，均在最后的主要参考文献中统一列出。作者衷心感谢所有为本书写作提供了丰富参考内容的学者们，感谢东北财经大学电子商务学院的研究生张晓娜、李婷、李燕、梁锋、李冬杰、王玉刚、初阳、李巍、才雨和郑艺，他们在本书资料的收集整理和 PPT 课件的制作方面做了大量的工作，感谢东北财经大学出版社编辑在本书写作和出版过程中给予的帮助和指导。

本书可作为高等学校电子商务专业的专业课程教材，也可以作为相关专业的本科生了解电子商务安全问题的入门教材或自学教材。本书所涉及的领域发展快、内容新，文稿虽经多次修改，仍难免有问题或疏漏。不当之处，恳请专家和读者指正，以利于今后的提高和完善。

李洪心
于东北财经大学电子商务学院
2008 年 8 月

目录

第1章

电子商务安全概述

学习目标

1. 了解电子商务的安全需求
2. 熟悉电子商务安全管理内容
3. 了解电子商务安全体系结构
4. 了解电子商务安全威胁表现形式

1.1 电子商务安全的基本概念

1.1.1 电子商务面临的安全问题

随着互联网技术的发展和应用的普及，电子商务已经逐渐成为人们进行商务活动的常用模式。越来越多的人通过互联网进行商务活动。电子商务的发展前景十分诱人，而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，对交易信息提供足够的保护，已经成为商家和用户都十分关心的问题。

1）由互联网的特点带来的安全隐患

互联网具有四个特点：国际化、社会化、开放化和个人化。这些特点决定了互联网络应用面临的风险。

（1）国际化：互联网络的触角伸向全球各地，网络的攻击不仅仅来自本地网络的用户，它还可以来自互联网上的任何一台机器。

（2）社会化：全球信息化飞速发展，信息化系统已经成为各个国家的关键基础设施，诸如电信、电子商务、金融网络等。社会对计算机网络的依赖日益增强。

（3）开放化：网络的技术和资源是开放的，任何个人、团体都可能获得。开放性和资源共享是网络安全隐患的根源。

（4）个人化：随着网络应用的深入，个人的生活和工作越来越离不开网络，人们可以自由地访问网络，自由地使用和发布各种类型的信息，那么来自网络的安全威胁毫无疑问地会给网络上的个人用户带来损失。

2）人为与不可抗拒因素带来的损失

（1）1995 年，来自俄罗斯的黑客 Vladimir Levin 在互联网上上演了一场“偷天换日”。他是历史上第一个通过入侵银行电脑系统来获利的黑客。他侵入美国花旗银行并盗走 1 000万美元。之后，他把账户里的钱转移至美国、芬兰、荷兰、德国、爱尔兰等地。同年他在英国被国际刑警逮捕。

（2）2006 年 12 月，大规模爆发的“熊猫烧香”病毒，造成的危害十分严重：据统计，中国有上百万台电脑遭受感染，数以千计的企业受到侵害。

（3）2006 年 12 月 26 日晚至 27 日凌晨，中国台湾南部海域发生强烈地震，使附近国家和地区的国际长途、国际互联网网站受到严重影响，其中包括 8 条光缆。经过夜以继日地抢修，3 个月后才恢复到震前水平。

（4）2008 年 1 月 30 日，一艘停泊在埃及亚历山大港外的船只，在恶劣海象中试图下锚以稳住正在漂流的船身，却不慎割断地中海海底的两条电缆线，造成中东、印度与南亚

地区的国际电话和网络通信受阻。

3）电子商务面临的安全威胁

电子商务在给企业带来新的商机、给用户带来方便的同时，由于互联网本身的开放性，计算机技术、网络技术以及其他高科技技术的发展，使得通过网络的犯罪和不道德行为比传统方式更加隐蔽和难以控制，网上交易也面临着种种危险。人们从面对面的交易和作业变成网上相互不见面的操作，没有国界、时间限制，可以利用互联网的资源和工具进行访问、攻击甚至破坏。概括起来，电子商务面临的安全威胁主要有以下几个方面：

（1）在网络的传输过程中信息被截获。攻击者可能通过互联网、公共电话网、搭线或在电磁波辐射范围内安装截收装置等方式，截获传输的机密信息，或者通过对信息流量和流向、通信频度和长度等参数的分析，推断出有用信息并截获，如消费者的银行账号、密码等。

（2）传输的文件可能被篡改。攻击者可能从以下三个方面破坏信息的完整性：

①篡改。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等。

②删除。删除某个消息或消息的某些部分。

③插入。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。

（3）伪造电子邮件。

①虚开网站和商店。给用户发电子邮件，收订货单。

②伪造大量用户。发电子邮件，穷尽商家资源，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。

③伪装用户。发大量的电子邮件，窃取商家的商品信息和用户信用等信息。

（4）假冒他人身份。

①冒充他人身份。如冒充领导发布命令、调阅密件。

②冒充他人消费，栽赃。

③冒充主机欺骗合法主机及合法用户。

④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。

⑤接管合法用户，欺骗系统，占用合法用户的资源。

（5）不承认或抵赖已经做过的交易。

①发信者事后否认曾经发送过某条消息或内容。

②收信者事后否认曾经收到过某条消息或内容。

③购买者确认了订货单而过后不承认。

④商家卖出的商品因价格差而不承认原有的交易。

1.1.2 电子商务安全的内涵

1）电子商务安全的意义

（1）保证数据传输的安全。电子商务系统既不是单纯的商务系统，也不是简单的计