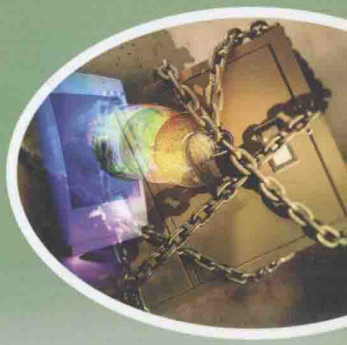
电子商务专业系列教材

DZSWZYXLJC



# 电子商务安全技术

胡伟雄　主编

华中师范大学出版社

电子商务专业系列教材

# 电子商务安全技术

主　编：胡伟雄
副主编：毛千兵　李　伟
编　者：（以姓氏笔画为序）
毛千兵　李　伟　陈艳红　姜政军
胡伟雄　郭家慧　常杰菊

华中师范大学出版社

## 内 容 摘 要

本书从系统工程的角度研究电子商务安全问题，全面介绍了电子商务安全的原理和技术，包括电子商务密码技术、电子商务安全认证技术、电子商务网络安全技术、电子商务系统安全技术等内容，并加入大量操作实践案例，从实践的角度阐述了相关技术的实施方法，最后从管理的角度介绍了与电子商务安全相关的法律法规、标准、规章制度等内容。

本书内容丰富、系统全面，同时融入作者多年从事信息网络安全工程项目和教学实践的经验，可操作性强，适合作为本科、高职高专电子商务专业的教材，也可供相关专业的研究生、从事信息安全工作的从业者参考。

**图书在版编目(CIP)数据**

电子商务安全技术/胡伟雄主编. —武汉：华中师范大学出版社，2011.6
(电子商务专业系列教材)
ISBN 978-7-5622-4691-6
Ⅰ.电… Ⅱ.胡… 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(2010)第 241521 号

书　　名：电子商务安全技术
主　　编：胡伟雄©
责任编辑：陈　鑫　杨发明　　封面设计：罗明波　　责任校对：王　炜
选题策划：华中师范大学出版社第二编辑室　电话：027－67867362
出版发行：华中师范大学出版社
地　　址：武汉市武昌珞喻路 152 号　邮编：430079
市场部电话：027－67863426　67867076　67863040　67867371　67861549
邮购部电话：027－67861321　传真：027－67863291
网址：http://www.ccnupress.com　电子信箱：hscbs@public.wh.hb.cn
印 刷 者：武汉湖印印务有限责任公司　　督　　印：章光琼
开本/规格：787 mm×960 mm　1/16　　印　　张：18　　字　　数：330 千字
版次/印次：2011 年 6 月第 1 版　　2011 年 6 月第 1 次印刷
印　　数：1-3000　　定　　价：29.80 元

# 电子商务专业系列教材编委会

# 前　言

自2001年教育部首次批准浙江大学、西安交通大学、华中师范大学等13所高校开办电子商务专业以来，电子商务专业教育发展迅猛。据2005年统计，我国开办电子商务本科专业的高校达到300多所，开办电子商务专科专业的各类高校达到800多所。这显示出电子商务专业的市场认可程度是相当高的，但同时也给电子商务专业教育的从业者们提出了更高的要求，我们必须为电子商务专业的建设不懈努力。毕竟电子商务专业是一个新专业，其人才培养方案、课程体系、教学大纲等还需要不断地修订与完善。在这个过程中，专业教材的建设是一项重要内容。

早在2001年，在华中师范大学的大力支持下，我们就开始了“电子商务专业系列教材”的建设，经过几年的努力，以华中师范大学信息管理系电子商务教研室教师为核心的教材编写团队完成了这项工作，出版了《电子商务概论》、《电子商务物流》、《网络营销》、《电子商务安全认证系统》、《网上支付与电子银行》、《电子商务政策法规导论》、《电子商务网络建设》、《电子商务数据库》、《Web站点设计与管理》、《CI与网络广告》、《电子证券与投资分析》、《电子出版与网上发行》等12本教材，受到市场的广泛欢迎与好评，其中不少教材多次重印。

教材建设是一个永不停息的过程，随着电子商务的发展和对电子商务研究的深入，教材的内容也需要不断吸收新的研究成果，以反映学科发展的内容，适应市场的需求。于是我们又开始了“电子商务专业系列教材”的修订与增补这项浩繁的工作。我们认为，电子商务专业是在网络经济时代到来后适应商务运作的变化而产生的以商务的电子化为主体，融入经济学、管理学、计算机科学、信息科学等知识而形成的一个综合性的专业，它是打破学科界限、按照市场人才需求而形成的职业性专业。在专业知识上，电子商务职业要求从业者具有多学科知识，而这些知识的体系化表现为以多学科知识为基础和在某一知识模块中多学科知识的融合。基于这种思想，本次电子商务专业系列教材的修订与增补，按照知识基础与知识模块设计了五大系列，即电子商务理论与基础（包括《电子商务概论》、《电子商务政策法规》、《国际电子商务》、《管理学》、《电子商务专业英语》），电子商务流程（包括《电子商务物流管理》、《网上支付与金融服务》、《网络营销》），电子商务技术（包括《电子商务网络建设》、《电子商务数据库应用技术》、《电子商务网站设计与管理》），电子商务集成与应用（包括《电子商务系统分析与

设计》、《电子商务安全技术》、《电子商务案例分析》、《电子商务项目管理》、《客户关系管理》)和实验(包括《电子商务实验》)共17本教材。

该系列教材的编写立足于“新”,即反映电子商务的新理论、新知识、新技术;规范于“质”,即反映电子商务活动的信息流、物流和资金流的运作机理;重在于“用”,即强调电子商务的操作技能与应用。

该系列教材适合于各类学校的电子商务专业的教学之用,也可供电子商务从业人员参考。

编委会

2011年4月

# 目 录

# 第1章 电子商务安全技术概论

因特网所固有的各种安全问题一直是人们担忧的焦点，网络黑客所使用的技术手段越来越高明，网络安全事件也越来越多，给网络用户造成了极大的损失。

在因特网上开展电子商务的一个首要问题是解决商务过程各环节的安全性和可靠性。任何电子商务系统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，才能真正开展和普及电子商务。

电子商务安全保障体系包括技术保障、管理保障和法律保障，它们都有各自不同的侧重点，但一起构成一个完整的电子商务保障体系。其中，电子商务安全技术尤其重要，它是电子商务安全的物质基础。

本章首先探讨与电子商务安全有关的概念和术语的定义；然后讨论电子商务安全的主要安全风险，讨论电子商务安全服务，安全机制及其它们的相互关系，最后探讨了电子商务安全体系。

## 1.1 安全性概念

在ISO安全框架文件中，“安全”被解释为“一种使资产和资源遭受攻击的可能性减少到最小的方法”。可见，安全是相对的，并没有绝对安全的网络实体。

在定义相关的安全性概念时，通常使用不同的安全属性来对某个安全概念进行不同侧面的描述。这些经常用来定义具体安全概念的安全属性有机密性、完整性、真实性(可鉴别性)、可用性、不可否认性等。

机密性指存储的信息不被非法窃取或传输的信息不被非法截取；完整性是指信息在存储或传输时不被非授权的修改、破坏，信息能保持一致性；真实性是指商务活动中每个交易方身份的真实合法性；可控性确保系统、数据和服务只能由合法的人员进行合法的访问；不可否认性用来防范交易方在事后对所认可的交易行为的抵赖；可用性是指系统工作正常，能够及时和有效地为合法用户提供服务，它是系统有效性、可靠性和安全性的综合体现。

电子商务建立在因特网之上，电子商务安全基础是因特网安全，它与密码安全、计算机安全、网络安全、信息安全等是密不可分的。因此，为了理解本书所述的各种安全概念的含意，有必要先讨论密码安全、计算机安全、网络安全、信息安全的概念。

### 1.1.1 密码安全

通信安全是对从一个系统传送到另一个系统的信息进行的安全保护。密码安全是通信安全的最核心部分，通过在技术上提供强力的密码系统及其正确的应用来实现通信安全。

信息安全问题是国家信息化建设的关键问题，对信息安全问题的重视和解决程度，将直接制约信息化进程和发展。信息安全所要求的信息机密性、真实性、完整性和可用性，可以通过数据加密、完整性检验、身份认证和访问控制等技术来解决，而这些技术的核心是密码技术。

密码具有特殊性，密码安全关系到国家的安全和利益。密码同时又是一种技术手段，要为保护国家利益和市场经济领域中的各种商业活动服务。我国对密码采取既大力发展又严格管理的基本政策，实行“统一领导、集中管理、定点研制、专控经营、满足使用”的发展和管理方针。全国用于金融商业的密码由国家密码管理委员会统一领导，由国家密码管理委员会办公室具体管理。研究、生产和经销密码须经国家密码主管部门批准。未经批准，任何单位和部门不得研制、生产和经销密码。需要使用密码技术手段保护信息安全的单位和部门，必须按照国家密码管理规定，使用国家密码管理委员会指定研制、生产的密码，不得使用自行研究的密码，也不得使用从国外引进的密码。

### 1.1.2 计算机安全

计算机安全，又称计算机系统安全。目前，对它的定义并不统一，常见的定义是：计算机安全是指计算机系统的硬件、软件和数据受到保护，不因偶然的和恶意的原因而遭到破坏、更改和显露，系统连续正常运行。

“计算机安全”一词的含义首先是信息的机密性，其次是信息的完整性，另一个与计算机安全紧密相关的概念是可用性。计算机安全包括物理安全和逻辑安全。物理安全指系统设备及相关设施受到物理保护，免于破坏、丢失等。逻辑安全包括信息完整性、机密性和可用性。

### 1.1.3 网络安全

网络安全，又称为计算机网络安全，是指保证在任何两个实体之间的信息交换和通信的安全可靠，满足计算机网络对信息的可用性、完整性、真实性、机密性和占有性的要求。

占有性是指存储信息的主机、磁盘等信息载体不被盗用，对信息占用权的保护。保护信息占有性的方法有使用版权、专利权、商业秘密，提供物理和逻辑的

存取限制方法；维护和检查有关盗窃文件的审计记录、使用标签等。

网络安全的研究内容从广义上说，包括物理安全、通信安全、计算机安全、管理安全、人事安全、媒体安全和辐射安全。从系统外来看，研究内容还包括管理和法律两个方面，它们的综合构成了一个合理的研究结构和层次。

物理安全包括门锁、门卫以及其他物理访问控制设施；敏感设备的防篡改能力，如红外线报警装置等不能被侵入者随意停用；环境控制包括温度、湿度、防尘等内容。

人事安全包括员工的素质，敏感岗位的身份识别；雇员筛选过程；安全培训和安全意识；安全监察等内容。

管理安全包括控制软件从外部进入，安全泄露事件调查，审计跟踪和责任控制检查的操作程序等。

媒体安全指存储的信息保护；控制敏感信息的记录、再生和销毁过程；确保废弃的纸张或含有敏感信息的磁性介质得到安全的销毁；对媒体进行扫描，以便发现病毒。

辐射安全是指控制射频(RF)及其他电磁(EM)辐射所造成的信息泄露的防护。

### 1.1.4 信息安全

信息安全是指信息系统的系统资源与信息资源不受自然和人为有害因素的威胁和危害，防止窃取、篡改和非法操作；在信息的采集、存储、处理、转播和运用过程中，信息的机密性、完整性、可用性等都能得到良好保护的一种状态。

信息安全涉及信息存储安全(存储保密)、信息传输安全(传输保密)和对网络传输信息内容的审计三方面。信息传输安全是指在网络上传递的信息没有被故意的或偶然的非法授权泄露、更改、破坏或是使信息被非法系统识别、控制，网络信息的机密性、完整性、可用性、可控性得到良好保护的状态。为保障信息传输安全，可以采用数据传输加密技术、数据完整性鉴别技术；为保证信息存储安全，必须保障数据库安全和终端安全；信息内容审计，则是实时对进出内部网络的信息进行内容审计，以防止或追查可能的泄密行为。

网络信息安全的传统提法一般是指信息的机密性、完整性和可靠性。可靠性是指信息的可信度，包括信息的完整性、准确性和发送人的身份证实等方面，可靠性也是信息安全性的基本要素。

以上几类安全性之间的关系，可用如图 1-1 所示的安全环表示。

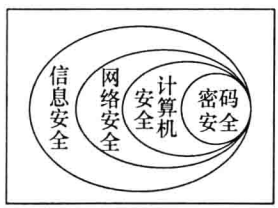



图 1-1 安全环

### 1.1.5 电子商务安全

电子商务安全是指通过制定安全策略，并在安全策略的指导下构建一个完整的综合保障体系，来规避信息传输风险、信用风险、管理风险和法律风险，以保证网上交易的顺利进行，满足开展电子商务所需的机密性、完整性、真实性、可控性、可用性、不可否认性等安全性需求。

密码安全、计算机安全、网络安全和信息安全是电子商务安全的基础。它们所采用的安全技术都是电子商务安全技术的一个重要组成部分。

电子商务安全与网络安全、信息安全等一样，包括相互关联的两个方面：一是面向技术的安全系统方法的研究与应用，二是社会人文环境的建设，包括管理、法律法规以及信息道德、伦理等网络文化的构建。本书主要从技术层面讨论电子商务的安全需求、安全服务和安全机制，并结合电子商务自身的属性，探讨电子商务安全技术的原理和应用。

## 1.2 电子商务的安全风险与安全威胁

安全威胁是指某个人、物、事件或概念对某一资源的机密性、完整性、可用性、可控性所造成的危险。威胁的具体实现就是网络攻击。

安全威胁是由于系统存在的脆弱性而导致的。脆弱性是指在防护措施中和在缺少防护措施时系统所具有的弱点。

系统存在许多的弱点，这些不同的弱点被攻击时造成的损失是不同的。常用风险来衡量脆弱性所导致的安全威胁的大小。风险是关于某个已知的、可能引发某种成功攻击的脆弱性的代价的测度。当某个脆弱的资源的价值较高，以及成功攻击的概率较高时，风险也就高；与之相反，当某个脆弱的资源的价值较低，成功攻击的概率较低时，风险也就低。

防范安全威胁的一个基本方法是采取有效的安全防护措施。防护措施是指保护资源免受威胁的一些物理的控制、机制、策略和过程。不同防护措施的功能不同，成本也有很大差异。风险分析能够提供定量的方法来确定防护措施的支出是否应予保证。

### 1.2.1 电子商务的安全风险

电子商务既带来了巨大的机遇，也存在着各种风险。电子商务的安全风险，主要包括信息传输风险、信用风险和管理风险。

**1. 信息传输风险**

信息传输风险是指进行网上交易时，因传输的信息失真或者信息被非法窃取、篡改和丢失，而导致网上交易的不必要损失。

(1)客户面临的风险

客户面临的风险是指客户一方的私有信息被盗用或破坏的可能性。私有信息包括：客户的账号及密码、信用卡信息、客户计算机系统及数据等。被盗取的途径主要有以下四种：利用欺骗性网站盗取；从销售商或网络服务提供商(ISP)那里盗取；从客户计算机上的 Cookies 文件中盗取；直接骗取。

①利用欺骗性网站盗取：欺骗性网站主要有两种，一种是黑客设立的假冒网站，另一种是黑客利用现有网站程序的漏洞欺骗客户。假冒网站是黑客在 Internet 上设立的，假冒某个合法的销售站点的网站。客户在访问或购物时，会被要求提供信用卡号及其他的信息，黑客在骗取了大量的客户信息后，便撤销网站。而黑客利用已有网站程序中的漏洞来欺骗客户，这种情况更不容易被发现。黑客利用一些现有网站程序中的漏洞来监控，记录用户的账号、密码等信息，或利用网络浏览器的漏洞窥探访问者的硬盘，或者由一个临时性的假冒网站产生一个 Bug 程序，利用这个程序可以查看用户的硬盘并盗窃客户计算机上的文件。

②从销售商或网络服务提供商(ISP)那里盗取：在电子商务中，客户在进行商务活动时要提供给销售商和 ISP 大量的隐私信息(如信用卡号等)。如果黑客入侵了销售商或 ISP 的服务器，客户的私有信息就可能被盗取。

③从客户计算机上的 Cookies 文件中盗取：当客户第一次访问一个网站时，主机会分配给用户一个独立的标识码，并创建一个 Cookies 文件，将用户的账号、密码存放在里面，并将该文件存在用户的计算机的硬盘上。当用户的计算机被非法访问或侵入时，Cookies 文件的被盗导致用户信息的泄露。

④直接骗取：直接骗取是指黑客假扮系统管理员等，通过 E-mail 或电话与客户联系，谎称网络有故障，要求得到客户的密码。

(2)销售商面临的风险

在电子商务中，销售商面临的风险主要有三方面，即虚假客户、服务拒绝和数据被窃取。

①虚假客户：虚假客户是指一些人假扮客户来订购产品或服务。例如，用假信用卡来骗取免费服务和免费产品，或者要求送货而没有人来支付。

②服务拒绝：服务拒绝是指销售商的计算机和网络资源被黑客攻击和封锁，从而导致无法提供正常的销售服务。

③数据被窃取：数据被窃取是销售商们面临的一种很常见的风险。黑客可以随时、随地作案，而且很难被追踪到。