普通高等教育“十一五”国家级规划教材

高等学校电子商务专业系列教材

电子商务安全与认证

胡伟雄　主编

高等教育出版社
HIGHER EDUCATION PRESS

普通高等教育“十一五”国家级规划教材

高等学校电子商务专业系列教材

电子商务安全与认证

Dianzi Shangwu Anquan yu Renzheng

胡伟雄　主编

高等教育出版社·北京
HIGHER EDUCATION PRESS　BEIJING

内容提要

本书是普通高等教育“十一五”国家级规划教材。本书从系统工程的视角来研究电子商务安全问题；以完整的框架来介绍电子商务安全的原理、技术和实施方法；从安全威胁、安全风险的层面来挖掘电子商务安全需求，选择适用的安全技术来构建电子商务安全防护体系，同时重视电子商务安全管理所起到的作用。本书全面介绍电子商务密码技术、电子商务认证技术、电子商务认证体系、电子商务安全认证系统、电子商务网络安全、系统安全技术、电子商务安全应用、电子商务安全管理等内容，并通过电子支付、PKI/CA 应用、企业网络安全防护等应用案例，帮助读者掌握基本的安全技术及其应用方法。

本书内容丰富，深入浅出，凝聚着作者十多年从事信息网络安全工程项目的经验，可操作性强，适合作为高等学校电子商务专业本科“电子商务安全与认证”课程的教材，也可供相关专业的研究生、从事信息安全工作的研究者和从业者参考。本书配套光盘中有丰富的教学资源，可以配合教材使用。

图书在版编目(CIP)数据

电子商务安全与认证/胡伟雄主编. —北京：高等教育出版社，2011.1
ISBN 978-7-04-031036-8

Ⅰ.①电… Ⅱ.①胡… 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 230834 号

策划编辑 曾飞华 **责任编辑** 康兆华 **封面设计** 杨立新 **责任绘图** 黄建英
版式设计 余 杨 **责任校对** 王效珍 **责任印制** 张福涛

出版发行 高等教育出版社
社 址 北京市西城区德外大街 4 号
邮政编码 100120

经 销 蓝色畅想图书发行有限公司
印 刷 北京市鑫霸印务有限公司

开 本 787×1092 1/16
印 张 19.5
字 数 450 000

购书热线 010-58581118
咨询电话 400-810-0598
网 址 http://www.hep.edu.cn
http://www.hep.com.cn
网上订购 http://www.landraco.com
http://www.landraco.com.cn
畅想教育 http://www.widedu.com

版 次 2011 年 1 月第 1 版
印 次 2011 年 1 月第 1 次印刷
定 价 33.00 元

物料号 31036-00

前　言

电子商务自诞生以来，安全问题就如影随形。随着通信技术的不断发展和电子商务的日益普及，在给人们的工作和生活带来便利的同时，电子商务的安全问题也日渐突出。通过电子商务交易，使得大量的经济信息在网络上传送、大量的资金在网络上划拨，这些都对电子商务安全提出了更高的要求。如何建立一个完善的、有效的电子商务安全保障体系，培养高素质的电子商务安全应用人才，提高我国公民的电子商务安全意识，已经成为政府机关、电子商务企业和教育机构义不容辞的责任和义务。

电子商务安全从整体上可以分为计算机网络安全和电子商务交易安全。计算机网络作为电子商务交易信息的传输和交换平台，其实质是保证商务信息及其传输的安全。电子商务交易安全不但包括传统商务交易中的安全问题，如欺诈、失信等，还包括在计算机网络环境下开展商务活动所涉及的管理、法律等方面的安全问题。一个完善的电子商务安全保障体系一定是综合了电子商务安全技术、安全管理和法律保障这3个基本要素而构成的。电子商务安全技术始终是三者中难度最大、关注度最高的部分。

本书全面涵盖电子商务安全保障体系中的3个基本要素。第1章从整体上介绍电子商务安全保障体系的相关概念、知识体系和本书的主要内容，是全书的导读部分。第2~8章主要介绍电子商务安全技术。第9章介绍电子商务安全管理和电子商务法律法规保障体系。在电子商务安全技术部分，又可以分为电子商务安全基础、电子商务安全认证体系、电子商务安全技术和电子商务安全应用等组成部分。第2章“电子商务密码技术”是实现电子商务安全保障的基础；第3章“电子商务认证技术”、第4章“电子商务认证体系”、第5章“电子商务安全认证系统”一起构成了一个电子商务安全认证体系。第3章“电子商务认证技术”是电子商务安全认证的基础，第4章“电子商务认证体系”是电子商务认证体系的组织框架和实施标准，第5章“电子商务安全认证系统”是电子商务认证体系的具体应用。电子商务认证体系可以解决交易双方的身份、所交换的商业信息、电子合同的签署等电子商务交易构件的真实性、完整性、机密性问题，在电子商务安全防护技术中具有独特的地位和作用，所以本书特别把电子商务认证体系从电子商务安全技术中脱离出来详加介绍。第6章“电子商务网络安全”、第7章“系统安全技术”构成电子商务安全技术模块。第8章“电子商务安全应用”注重理论联系实际，以系统工程的思想给出若干电子商务安全防护与应用案例。这些章节一起构成了一个较为完整的电子商务安全保障体系与知识体系。

本书作者多年来始终坚持教学、科研与电子商务安全实践相结合。首先，本书主编多年来一直讲授华中师范大学电子商务专业的“电子商务安全与认证”课程，对该课程的内容十分熟悉，并能掌握学生在学习过程中需要消化的重点和难点。其次，作者一直从事“电子商务安全与认证”方面的研究，并取得一定的研究成果。最后，作者多年来一直从事信息系统安全工程方面的工作，为多家企事业单位进行过信息安全、网络安全、电子商务安全与认证等方面的工程咨询与安全防护体系建设工作，能够将理论与实际相结合，并时刻关注着“电子商务安全与认证”在社

会中的实际应用与发展趋势。《电子商务安全与认证》是作者从事大量的理论研究与实践活动的结晶，本书具有以下特点。

（1）内容丰富，深入浅出

本书内容涵盖教育部高等学校电子商务专业教学指导委员会最新出版的《普通高等学校电子商务本科专业知识体系》中所涉及的电子商务安全技术、电子商务安全管理以及与电子商务安全相关的电子商务法律的所有知识点，全面介绍电子商务安全的原理、技术和实施方法。在编写过程中，力求做到行文准确、简明。

（2）以理论为基础，紧密结合实际

本书在介绍电子商务安全基本理论的同时，注重与实际应用相结合，帮助读者掌握基本的电子商务安全技术及其应用方法。

（3）以系统工程的观点进行电子商务安全防护

作者从电子商务安全技术、安全管理和法律保障这3个电子商务安全基本要素出发，以系统工程的观点来组织电子商务安全防护体系。

（4）适用范围广

本书凝聚着作者十多年从事信息网络安全工程项目的经验，可操作性强，既适合作为高等学校电子商务专业本科“电子商务安全与认证”课程的教材，也可供相关专业的研究生、从事信息安全工作的研究者和从业者参考。同时，本书配套光盘中提供了丰富的教学资源，为读者提供了更多的知识和相关信息。

本书在编写过程中参照了国内外专家和同行的大量文献资料和研究成果，在此谨致诚挚的感谢！各章后面均列出了主要的参考文献，如有疏漏，谨向相关资料的作者致歉。

在本书的写作过程中，华中师范大学信息管理系副主任、博士生导师王伟军教授在百忙中审阅了全书，并提出了许多中肯的建议；武汉大学信息管理学院博士生导师、中国科学评价研究中心主任、中国科教评价网首席专家、华中师范大学特聘教授、博士生导师邱均平教授，华中师范大学信息管理系主任、博士生导师王学东教授，以及华中师范大学信息管理系全体同事都给出了许多宝贵的建议和无私的帮助，在此对他们致以深深的谢意。

本书的编写分工是：胡伟雄编写第1、2章，毛千兵、胡伟雄编写第3章，陈艳红、胡伟雄编写第4、5章，陈艳红、肖毅编写第6章，常杰菊、肖毅编写第7章，常杰菊、李伟编写第8、9章；姜正军、郭家慧参与了全书的校订工作；全书由胡伟雄负责审定编写大纲和统稿。

由于作者水平有限，书中难免存在疏漏之处，恳请广大读者批评指正，所有评价和建议请发往 wilson@ mail. ccnu. edu. cn。

胡伟雄

2010年7月于武昌桂子山

目　录

第1章　电子商务安全导论

内容提要

在因特网上开展电子商务的首要问题是解决商务过程中各个环节的安全性和可靠性。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。如何保障电子商务活动的安全，是电子商务的核心研究领域之一。

本章介绍电子商务活动所面临的安全问题，概述电子商务的安全需求，讨论电子商务安全的概念，总结电子商务活动所面临的主要安全威胁，给出电子商务安全服务和主要的安全机制，并进一步探讨电子商务安全体系。

学习目标

1. 了解电子商务活动所面临的安全问题
2. 理解电子商务的安全需求
3. 了解电子商务安全的概念
4. 理解电子商务活动所面临的主要安全威胁
5. 掌握电子商务安全服务和主要的安全机制
6. 了解电子商务安全体系及其主要内容

1.1　电子商务面临的安全问题

由于电子商务的经济、便捷、不受时空限制等特性，相对于传统的商务模式来说，电子商务具有更大的发展优势。然而，中国互联网络信息中心（CNNIC）于2010年1月发布的《第25次中国互联网络发展状况统计报告》表明，截至2009年12月31日，我国网民规模达到3.84亿人，普及率达到28.9%。其中，商务交易类应用的用户规模增长最快，平均年增幅达到68%。但是，按参与人数占网民总人数的比例来计算，网络购物、旅行预订、网上支付、网上银行和网络炒股分别只占28.1%、7.9%、24.5%、24.5%和14.8%，还是处于比较低的水平。目前大多数网民（约占网民总人数的75%）对电子商务还是持观望或不信任的态度。对于那些参与电子商务交易的网民来说，也多是集中在服饰、化妆品、书籍等低价值的交易领域中。我国电子商务发展的广度和深度均尚未达到其应有的水平，其中一个主要的原因是大部分网民对电子商务应用都没有充分的信任。电子商务的安全性、可靠性已经成为制约电子商务应用扩展的一个瓶颈。因此，只有采取

更加有力的措施来解决电子商务活动中存在的安全问题，提供一个可信的交易环境，才能促进电子商务的普及和发展。

电子商务为人们带来了巨大的发展机遇，也存在着各种各样的安全问题。电子商务安全从整体上可以分为计算机网络安全和商务交易安全这两个方面。网络作为电子商务交易活动中的信息的传输和交换平台，其实质是保证商务信息传输的安全性。商务交易安全既包括传统商务交易中的安全问题，如欺诈、失信等，也包括在网络环境下开展商务活动所产生的商务安全问题。所以，电子商务活动所面临的安全问题或者说电子商务的安全风险，可以从交易信息传输过程中存在的安全问题、交易实体的信用安全问题和管理安全问题等方面来进行讨论。

1.1.1 信息传输过程中存在的安全问题

信息传输过程中存在的安全问题是指在进行网上交易时，因为信息被窃取、篡改、丢失或伪造，从而导致网上交易存在风险。

1. 客户面临的安全问题

客户面临的安全问题包括客户的个人信息被窃取、篡改、丢失或伪造的可能性。客户的个人信息包括账号、密码、信用卡信息、客户计算机系统及数据等。信息被盗取的途径主要有以下4种：利用欺骗性网站盗取，从销售商或网络服务提供商处盗取，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

欺骗性网站的类型主要有两种，一种是由黑客设立的假冒网站，另一种是黑客利用现有网站程序中存在的漏洞欺骗客户。假冒网站是由黑客在因特网上建立的、假冒合法的销售站点的网站。当客户购物时，一旦输入信用卡号等敏感信息，就会被黑客窃取。黑客利用已有网站程序中存在的漏洞来欺骗客户，这种情况一般难以发现。黑客利用一些网站程序中存在的漏洞来监控、记录客户的账号、密码等信息，或者利用网络浏览器的漏洞来窥探访问者的硬盘，还有可能利用木马程序来查看客户的硬盘并盗窃用户计算机中的文件。

（2）从销售商或网络服务提供商处盗取

客户在进行电子商务活动时要向销售商或网络服务提供商提供大量的隐私信息（如信用卡的卡号等）。如果黑客入侵了销售商或网络服务提供商的服务器，客户的私有信息就有可能被盗取。

（3）从客户计算机上的 Cookies 文件中盗取

当客户第一次访问某个网站时，主机会分配给用户一个独立的标识码，并创建一个 Cookies 文件，将客户的账号、密码存放在里面，并将该文件保存在客户计算机的硬盘上。当客户计算机被非法访问或入侵时，Cookies 文件的被盗将会导致客户信息的泄露。

（4）直接骗取

直接骗取是指黑客假扮系统管理员等特殊身份，通过电子邮件或电话与客户取得联系，谎称网络现在有故障，要求客户提供密码。

2. 商家面临的安全问题

在电子商务活动中，商家面临的安全问题主要有假客户、拒绝服务和数据安全问题。

（1）假客户

假客户是指假扮合法客户来订购产品或服务的那些客户。例如,用伪造信用卡来骗取免费服务和免费产品;或者提交订单,客户拒不执行订单;或者在收到货物后,客户却拒绝付款。

(2) 拒绝服务

拒绝服务是指商家的计算机和网络资源被黑客攻击和消耗殆尽,从而导致无法提供正常的销售服务。

(3) 数据安全问题

数据安全问题包括数据被窃取、篡改、丢失和伪造。其中,数据被窃取是商家面临的一种常见的安全问题。黑客可以随时、随地作案,而且很难被追踪到。被窃取的数据则包括商家的商业机密信息、客户的个人信息等。

1.1.2 交易实体的信用安全问题

交易实体的信用安全问题主要来自以下 3 个方面。

1. 来自买方的信用安全问题

对于个人消费者来说,在进行网络支付时,有可能恶意透支信用卡,或者使用伪造的信用卡来骗取商品和服务;对于集团消费者来说,有可能拖延货款。以上风险都必须由卖方来承担。

2. 来自卖方的信用安全问题

卖方不能按质、按量、按时提供消费者所购买的货物,或者不能完全履行与集团消费者签订的合同,造成买方的货款存在风险。

3. 抵赖行为

买卖双方中的一方或双方对某项交易的全部或部分内容事后抵赖,拒不执行交易中的约定,带来一定的信用风险。

1.1.3 管理安全问题

所谓"三分技术、七分管理",这句话真实地说明了管理在电子商务活动中的重要性。在电子商务的各个环节中,都必须制定严格的管理制度和规范,并在实施过程中严格执行这些管理制度和规范,才能保证交易的安全、可靠,保护各参与方的利益。网上交易的管理安全问题是指由于交易流程管理、人员管理、网络系统管理等方面尚不完善所带来的安全风险。

1. 交易流程管理安全问题

在 C2C(Customer to Customer,客户对客户)交易过程中,交易平台(网络商城)不仅要监督买方按时付款,同时还要监督卖方按时提供符合买方要求的货物。在这些具体的环节上,都存在着大量的管理问题。如果管理不善,势必造成较大的交易风险。

2. 人员管理安全问题

人员管理是电子商务管理安全中最为薄弱的环节。近年来,我国一些单位中出现了内部计算机犯罪,其主要原因是部分工作人员的职业道德修养不高,所在单位的安全教育和管理松懈。一些单位还存在向竞争对手派出商业间谍或者收买竞争对手的内部管理人员的不良行为,以此窃取对方的账号、密码、机密文件等信息。

3. 网络系统管理安全问题

人们必须重视对电子商务赖以存在的网络系统的安全进行管理。如果没有按照相关的安全

管理要求对网络和信息系统进行严格的安全管理,将导致许多安全问题。目前,还有许多企业没有专门的安全管理人员、没有全面的安全管理制度、没有明确的安全技术操作规范、没有定期的安全检查与测试制度、没有实时的安全监控系统等。这一系列安全管理工作的缺失,将会带来很大的管理安全问题。

此外,还存在着法律安全保障的问题,许多电子商务活动的交易方法、手段都需要获得法律的支持和认可,如数字签名活动。由于我国在电子商务立法方面有些滞后,因此电子商务交易尚存法律方面的安全问题。

1.2 电子商务的安全需求

电子商务安全是一项复杂的系统工程,若要全面地总结电子商务的安全需求,将是一个十分困难的问题。针对前文所讨论的电子商务的安全问题,可以归纳出机密性、完整性、真实性、可控性、不可否认性、可用性等基本的安全属性作为电子商务的基本安全需求。

1. 机密性

机密性是指所存储的信息不被非法窃取或所传输的信息不被非法截取。

在电子商务活动中,交易各方通过网络传送商业信息。在被交换的信息中,不乏企业的商业机密信息、个人的敏感信息等,这样就必须提供一种保护机制来确保这些信息不被泄露。同时,开展电子商务活动的各方都必须把自己的计算机或网络接入开放式网络中,如何保护内部网络中所存储的信息的安全性,防止未经授权者的非法访问或信息泄露,也是一个很重要的问题。所有这些安全问题构成了电子商务活动的机密性需求。

2. 完整性

完整性是指信息在被存储或传输时不会被非授权地修改、破坏,信息能够保持一致性。

电子商务交易数据往往表示一些重要的商业信息,比如货物的品名、数量、价格、出厂日期等,它们是用户的商业需求的真实体现。重要商业数据的丢失、重复、篡改甚至次序上的颠倒,都将导致商业行为不正常,严重时将导致交易各方之间发生商业纠纷。保持相关数据的完整性是电子商务活动得以正常开展的基础,是电子商务活动中的又一个基本的安全需求。

3. 真实性

真实性是指电子商务活动中的每个交易方的身份的确凿合法性。

在传统商务活动中,由于是当面交易,有些问题可以立即验证并完成交易。即使不能当场完成交易,由于已经真实地掌握了对方的身份,可以凭借对方以往的交易信用状况来决定是否完成交易。即使对方失信,也能够很方便地找到对方进行索赔。计算机网络则是一个虚拟的世界,要在这个比现实世界更加难以捉摸的虚拟环境中产生对别人的信任,并与之开展商务活动,是一个十分难以做出决策的问题。对方是谁?他所声称的身份是否合法?有没有假冒他人身份?发货后,我方会不会收不到货款?客户支付后,能否收到货物?所收到的货物是否有质量保证?这一切事项都离不开信任。可见,解决上述问题的一个重要的因素是对方身份的真实性。只有甄别了对方的真实身份,才能决定是否信任对方,才能在对方失信时追究其法律责任。所以,在计算机网络环境中的身份真实性的保证,是顺利开展电子商务活动的前提。

4. 可控性

可控性是指确保电子商务系统、数据和服务只能由合法的人员进行合法的访问。

企业掌握各种信息资源，例如系统、数据、服务等，合理地利用和共享资源是使企业效用最大化的一个重要方面。在开展电子商务活动时，许多信息资源都被载入网络中，由各方共享使用。如何保证企业对计算机网络中的自有资源的控制和占有，保证其合理、合法地被使用，是电子商务活动的又一个基本的安全需求。可控性要求对哪个实体能够访问哪些资源以及如何使用这些资源进行控制，保证信息资源不被未经授权地访问以及非法地使用。

5. 不可否认性

不可否认性是指防范交易方在事后对所认可的交易行为作抵赖。

交易方在商业环境中出现了对自己已经认可的交易协定不利的情况时，拒不执行交易协定的抵赖行为，将给电子商务的顺利实施造成巨大的破坏。虽然，用户的抵赖是一种主观上的故意行为，很难用技术和管理的手段杜绝其发生，但不可否认性作为电子商务的一个重要的安全需求，还是很有必要通过技术、管理和法律等手段综合加以实现的，以保证良好的电子商务交易环境的持续性。

6. 可用性

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。可用性是电子商务系统的有效性、可靠性和安全性的综合体现。

1.3 电子商务安全的概念

在国际标准化组织的安全框架文件中，“安全”被解释为“一种使资产和资源遭受攻击的可能性降至最低的方法”。可见，安全是相对的，并没有绝对意义上的安全。

电子商务建立在因特网之上，电子商务安全的基础是因特网安全，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。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。

1. 密码安全

密码安全是通信系统安全的核心部分，通过在技术上提供功能强大的密码系统及其正确的应用来实现。

密码具有特殊性，密码安全关系到国家的安全和利益。与此同时，密码又是一种技术手段，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。我国采取既大力发展又严格治理的密码管理政策，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。我国用于金融行业的密码由国家密码管理委员会统一领导，国家密码管理委员会办公室负责具体管理。研究、生产和经销密码须经国家密码主管部门批准。未经批准的任何单位和部门不得研究、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方面的有关规定，使用国家密码管理委员会指定研究、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。

2. 计算机安全

常见的关于计算机安全的定义是：计算机系统的硬件、软件和数据受到保护，不会因为偶然

或恶意的原因而遭到破坏、更改和泄露，系统连续、正常运行。

计算机安全包括物理安全和逻辑安全。物理安全是指系统设备及相关设施受到物理上的保护，免于遭受破坏、丢失等。逻辑安全则包括信息的完整性、机密性和可用性。

3. 网络安全

网络安全是指保证在任何实体之间的信息交流以及通信的安全、可靠，满足计算机网络对信息的可用性、完整性、真实性、机密性和占有性等安全性方面的需求。

从广义上说，网络安全的内容包括物理安全、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，下面将抽取主要内容进行介绍。从系统外部来看，需要研究的内容还包括管理和法律这两个方面，它们的综合体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的安全；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、湿度恒定及防尘等内容。

管理安全包括控制软件从系统外部进入系统内部，安全泄露事件的调查，审计跟踪和责任控制检查，等等。

人事安全包括员工的素质提升，敏感岗位的身份识别，雇员的严格筛选，安全培训和安全意识创建，安全监察，等等。

媒体安全包括被存储的信息的保护，控制敏感信息的记录、再生和销毁的过程，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计算机病毒，等等。

辐射安全是指防止射频(Radio Frequency，RF)及其他电磁辐射所造成的信息泄露。

4. 信息安全

信息安全是指信息系统中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、传播和运用的过程中，信息的机密性、完整性、可用性和共享性等都能得到良好保护的一种状态。

5. 电子商务安全

电子商务安全尚无统一的定义，本书采用下述定义：

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电子商务活动中的信息传输风险、信用风险、管理风险和法律风险，以保证网络交易的顺利进行，满足开展电子商务活动所需的机密性、真实性、完整性、可控性、可用性、不可否认性和合法性等安全性需求。这里的“合法性”是指保证交易各方的业务符合适用的法律和法规。

安全策略是进行系统安全防护的指导思想，是系统内所有安全活动都必须遵守的规则集，它由系统中的安全权力机构建立，并由安全控制机构来描述和实施。

1.4 电子商务安全威胁

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。安全威胁的具体体现就是网络攻击。

安全威胁是由系统中固有的脆弱性而导致的。脆弱性是指在执行防护措施或在缺少防护措施时系统所具有的弱点。

系统存在许多弱点，这些不同的弱点在引发攻击时所造成的损失是不同的。人们常用风险

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且发生成功攻击的概率较高时，风险也就较高；与之相反，当某个脆弱的资源的价值较低且发生成功攻击的概率较低时，风险也就较低。

防范安全威胁的一个基本方法是采取安全防护措施。安全防护措施是指保护资源免受威胁的一些物理上的控制、机制、策略和过程。不同的防护措施的功能有所不同，成本也有很大的差异。风险分析能够提供定量的方法来确定防护措施的执行是否应予以保证。

1.4.1 安全威胁的分类

可以采用不同的分类方法对安全威胁进行划分。

1. 按安全威胁的来源分类

按安全威胁的来源分类，可以将安全威胁分为内部威胁和外部威胁。

① 内部威胁是指系统的合法用户以非授权的方式访问系统。大多数已知的计算机犯罪都和系统内部攻击有着密切的关系，它们会导致系统安全遭受严重的损害。

② 外部威胁是指外部用户对系统所造成的危险。外部威胁的实施又称远程攻击。远程攻击可以采用的办法有搭线（主动的或被动的）、辐射截取、冒充成系统的授权用户、旁路等。

2. 按安全威胁的动机分类

按安全威胁的动机分类，可以将安全威胁分为偶发性威胁与故意性威胁。

① 偶发性威胁是指那些不带预谋的威胁，包括自然灾害、系统故障、操作失误和软件出错等。

② 故意性威胁是指针对计算机系统的有意图、有目的的威胁，包括使用简单的监视工具随意进行检测，或者使用特别的系统知识进行精心的攻击。如果某种故意性威胁被实现，就可以认为它是一种“攻击”或“入侵”。

3. 按安全威胁所造成的结果分类

按安全威胁所造成的结果分类，可以将安全威胁分为被动威胁和主动威胁。

① 被动威胁是指对信息的非授权泄露但是并未篡改任何信息，并且系统的操作与状态也都不被改变，例如搭线窃听。

② 主动威胁是指对系统的状态进行故意的、非授权的改变，包括对系统中的信息、状态或操作的篡改，例如非授权的用户改动路由选择表、篡改消息、重发消息、插入伪消息、冒充授权实体以及拒绝服务等。

4. 从通信模型的角度分类

从通信模型的角度分类，可以将安全威胁分为中断、窃听、篡改和伪造。

① 中断威胁是指使运行中的信息系统被毁坏或不能使用，即破坏其可用性。例如，硬盘等硬件设备的毁坏、通信线路的切断、文件管理系统的瘫痪等均属于中断威胁，如图 1-1 所示。

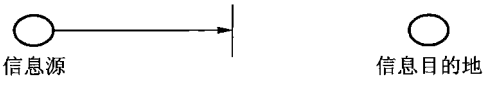

图 1-1 中断威胁

② 窃听威胁是指非授权方接入系统进行窃听，破坏系统的机密性。这种类型的威胁包括搭线窃听、文件或程序的不正当复制、射频截获等，如图 1-2 所示。

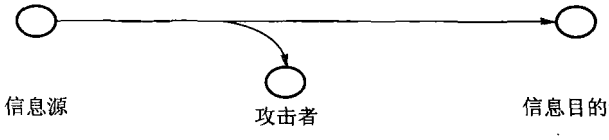

图 1-2 窃听威胁

③ 篡改威胁是指非授权方不仅介入系统而且篡改系统信息，破坏系统的完整性。例如，改变数据文件的内容、改变程序使之不能正确执行、修改信息等，如图 1-3 所示。

图 1-3 篡改威胁

④ 伪造威胁是指非授权方将伪造的信息插入系统中，破坏系统的真实性。例如，在计算机网络中插入虚假信息或者在文件中追加记录等，如图 1-4 所示。

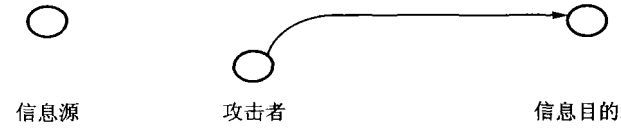

图 1-4 伪造威胁

1.4.2 常见的电子商务安全威胁

电子商务所面临的威胁有以下几种。

1. 假冒身份

这是电子商务活动中常见的一种破坏方式。网络黑客伪装成合法的用户进行未经授权的访问，或者做出有害于合法用户的行为，或者特权较少的用户为了得到额外的特权进行身份冒充，以期达到欺骗系统、占有合法用户的资源的目的。

2. 篡改数据

篡改数据包括对本地存储的订单、合同等电子单据的内容进行篡改，或者对接收端所存储的电子单据的内容进行篡改，或者对其他数据进行篡改。

3. 窃取信息

这是指未经授权地窃取他人的报文内容以获取商业秘密。