普通高等教育“十二五”规划教材
高等院校电子商务系列规划教材

电子商务安全

（第二版）

曾子明　主编

Electronic Commerce

科学出版社

普通高等教育“十二五”规划教材

高等院校电子商务系列规划教材

电子商务安全

（第二版）

曾子明　主编

科学出版社

北京

内 容 简 介

本书根据电子商务专业的特点，比较系统地介绍了电子商务安全基本理论、技术、管理及电子商务安全的应用。全书共包括三个部分：第一部分主要介绍电子商务安全的基本概念和理论，包括电子商务安全的体系结构、网络安全技术、现代密码技术与应用等；第二部分主要介绍电子商务的认证技术、电子支付与安全支付协议、电子商务安全管理等内容；第三部分介绍了电子商务安全应用及案例、移动电子商务安全等内容，从安全领域的热点和前沿知识引导读者跟踪学科发展的新方向。全书强调系统性、前沿性，取材新颖、科学，内容丰富、实用，图文并茂，可读性强。

本书适合作为高等院校电子商务、信息安全、信息管理、计算机应用和金融等专业的本科生、研究生的教学用书，也可作为电子商务安全技术培训教材，还可供从事电子商务安全系统研究、设计、开发的工程技术人员和管理人员参考。

图书在版编目（CIP）数据

电子商务安全/曾子明主编. —2 版. —北京：科学出版社，2013

（普通高等教育“十二五”规划教材·高等院校电子商务系列规划教材）

ISBN 978-7-03-038402-7

Ⅰ. ①电… Ⅱ. ①曾… 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 196862 号

责任编辑：李 娜 朱大益/责任校对：柏连海

责任印制：吕春珉/封面设计：子时文化

科学出版社出版

北京东黄城根北街 16 号

邮政编码：100717

http://www.sciencep.com

新科印刷有限公司 印刷

科学出版社发行 各地新华书店经销

*

2008 年 9 月第 一 版 开本：787×1092 1/16

2013 年 8 月第 二 版 印张：14 1/2

2013 年 8 月第三次印刷 字数：325 000

定价：29.00 元

（如有印装质量问题，我社负责调换〈新科〉）

销售部电话 010-62134988 编辑部电话 010-62138978-2018（HF02）

版权所有，侵权必究

举报电话：010-64030229；010-64034315；13501151303

第二版前言

电子商务是在国际化、社会化、开放化和个性化的 Internet 环境中运作的，它的应用可能会出现各种商业信息的泄漏、客户的银行账户信息被盗、金融欺诈、无法预料的法律与公共关系及商业恢复成本，以及缺乏可信性而导致的商业丢失等各种安全与信任问题。因此，要在 Internet 这样开放的网络平台上成功地进行电子交易，必须有效解决交易网络平台的安全问题，同时提供对整个电子交易过程的保护。因此，电子商务环境下如何确保电子交易的信息安全是目前困扰和影响电子商务发展的一个重要问题，已经成为电子商务有序发展的瓶颈。

我国电子商务产业的发展，需要大批掌握电子商务安全与管理知识的人才。因此，电子商务安全已经成为计算机专业、电子商务专业、经济管理专业及其他相关专业的重要课程。同时，电子商务安全也已成为普及率较高的知识和应用技术，成为从事电子商务应用与信息系统研究、应用的专业人员所必须了解和掌握的重要知识。

本书第二版依然保留第一版的主要内容和特色，着重强调如何实现电子支付过程中的安全性。与第一版相比，第二版对部分章节内容进行了调整和优化，内容和层次安排更加严谨，读者通过学习可以对电子商务的安全体系结构在整体上有更加清晰的认识。例如，将“电子支付系统”内容合并到“电子商务交易的安全协议”中，以电子支付为安全研究的情境，重点论述电子支付过程中的安全协议设计与实现；将“公开密钥基础设施”内容合并到“电子商务的安全认证机制”中，使得电子商务安全认证这部分内容的层次更加清晰和严谨。同时，增加了电子商务安全管理内容，科学、合理地论述了安全技术和安全管理两者之间的关系，从而形成一个更为完整的安全知识体系。此外，也增加和修订了一些电子商务安全领域的新内容，如计算机木马及防治、PGP 软件、网上招投标系统安全案例、移动电子商务安全等知识。因此，本书不仅力求内容广泛新颖、取材丰富实用，同时也力求内容阐述深入浅出、结构合理清晰，增强可读性和实践性。

第二版的整体结构共分为三个部分。

第一部分包括第 1 至 3 章，介绍了电子商务安全的基本概念和理论。其中，第 1 章为概述，首先介绍电子商务面临的安全威胁、安全需求及相应的安全体系结构，并讨论电子商务安全实现的保障；第 2 章从电子商务网络安全层次介绍防火墙、虚拟专用网、网络入侵检测、计算机病毒防治及计算机木马防治技术；第 3 章从电子交易安全层面介绍数据加密技术及其应用，并以 PGP 软件为例介绍数据加密技术的实际应用。

第二部分包括第 4 至 6 章，介绍电子商务的安全认证机制、电子支付与安全支付协议、电子商务安全管理等内容。其中，第 4 章介绍电子商务的认证机制，包括数字证书、数字认证机构及公开密钥基础设施的信任模型、标准和应用等；第 5 章首先介绍了电子支付系统，并以电子支付为安全情境，重点探讨了电子支付的两种安全支付协议，即安全套接层协议和安全电子交易协议，并对这两种安全支付协议进行详细的研究和比较；

第6章介绍电子商务系统相应的安全管理方法和安全评估标准，明确电子商务安全管理的意义。

第三部分包括第7至8章，介绍电子商务安全应用、移动电子商务安全的相关内容。其中，第7章引入案例教学法，通过网上银行系统、网上证券交易系统、网上报税系统、网上招投标系统等不同的实际安全案例的讨论和分析，使读者进一步加深对电子商务安全问题的认识；第8章介绍移动电子商务安全，包括移动电子商务安全的体系结构、移动电子商务与手机病毒、移动电子商务安全协议和标准、基于无线公开密钥基础设施的安全技术实现及移动支付系统安全。这部分内容注重理论联系实际，突出电子商务安全的实际应用和研究热点。

在本书编写过程中，编者参考了众多著作，在此对相关作者表示衷心的感谢。同时，感谢我的父母和妻子，他们一直默默地为本书的编写付出了许多不为人知的努力。

限于编者的学术水平，书中疏漏之处在所难免，不足之处敬请读者批评指正。

此为试读，需要完整PDF请访问：www.ertongbook.com

第一版前言

随着 Internet 和信息技术的发展和普及，电子商务已逐步进入人们的日常生活。目前，网络银行和网络商场的出现，正悄悄地改变着人们的购物方式、消费方式和生活观念，方便了人们的日常生活，真正实现了“随时随地、足不出户”的消费方式。

虽然电子商务的观念逐渐深入人心，但电子商务是在国际化、社会化、开放化和个性化的 Internet 环境中运作的，它的应用可能会出现各种商业信息的泄漏、客户的银行账户信息被盗、金融欺诈，以及缺乏可信性而导致的商业机密丢失等各种安全与信任问题。因此，要在 Internet 这样开放的网络平台上成功地进行电子交易，必须有效解决交易网络平台的安全问题，以及提供对电子支付过程的保护。因此，电子商务环境下的安全与支付是目前困扰和影响电子商务推广的两个重要问题。

本书较为深入和完整地阐述了电子商务安全与支付的基本理论和相关技术。全书的整体结构共分为三个部分。

第一部分包括第一至四章，介绍了电子商务安全与支付的基本概念和理论。其中，第一章为概述，主要介绍电子商务的安全威胁、安全技术、安全体系结构等；第二章从网络安全层次介绍防火墙、虚拟专用网、网络入侵检测和计算机病毒防治技术；第三章从电子交易安全层次介绍数据加密技术及其应用；第四章主要介绍了电子支付和网上银行系统。

第二部分包括第五至八章，介绍电子商务的认证技术、公开密钥基础设施、电子商务交易的安全协议等内容。其中，第五章介绍电子商务的认证机制，包括数字证书和认证机构两大内容，并重点对国内认证中心的发展进行实例介绍；第六章对公开密钥基础设施进行介绍，包括公开密钥基础设施的互操作信任模型、认证管理协议、不可否认机制、体系的发展等内容；第七章对安全电子交易协议和安全套接层协议这两种安全支付协议进行详细的研究和比较；第八章引入案例教学法，通过网上银行系统、网上证券交易系统、网上报税系统这三个实际安全案例的讨论和分析，使读者进一步加深对电子商务安全问题的认识。

第三部分即第九章，介绍了移动电子商务安全和移动支付，包括移动商务安全的基本内容、移动商务安全相关技术，以及移动支付及其安全解决方案。本章从电子商务安全领域的热点和前沿知识出发，引导读者跟踪学科发展的新方向。

本书具有以下两个特点：

1）实用性强。本书以技术为主线，突出实际应用，既传授基础理论知识又引导应用技能的提高，通过精品教材提高学生的相应素质。体现素质教育的思想，这是作者在编写教材的过程中特别注重的地方。

2）层次结构清晰。本书层次结构分为三个部分，第一部分为基础部分，涉及电子商务安全和支付基础理论知识；第二部分为核心部分，包括电子商务安全认证机制、公开密钥基础设施、电子商务的安全协议、电子商务安全案例及分析；第三部分则从安全

领域研究的新动态介绍移动商务和移动支付安全。读者可以根据自身情况，选读其中的章节内容。全书层次分明，可读性强，适应不同层次读者的需要。

本书在编写过程中参考了众多著作，在此对这些著作的作者表示衷心的感谢。同时，武汉大学电子商务系系主任张李义教授和全体同事对本书编写给予了许多有益的建议和指导，在此深表谢意！

由于编者水平有限，且电子商务安全理论与技术处在快速发展之中，本书的不足之处在所难免，真诚希望广大读者批评指正，以便再版时修订。

目　录

第 1 章　电子商务安全概述

电子商务作为一种全新的贸易活动，为政府的管理、企业的经营和人们的工作、生活提供了简单、快捷的服务和低廉的交易成本。但是，电子商务给我们的生活带来方便的同时，也带来了不少安全隐患，特别是在线交易和支付过程中的安全风险。因此，可以认为：影响电子商务广泛应用的一个首要问题就是安全问题。

1.1　电子商务基础

1.1.1　电子商务的定义和特征

1. 电子商务的定义

电子商务源于英文 electronic commerce（或 electronic business，EB），简写为 EC。顾名思义，电子商务的内容包含两个方面，一是电子方式，二是商贸活动。通俗地说，电子商务就是在计算机网络（主要指 Internet）的平台上，按照一定标准开展的商务活动。

电子商务的定义有多种，各国政府、学者和企业界人士根据自己所处的地位和对电子商务的参与程度，给出了不同的表述方法。

1）世界贸易组织（World Trade Organization，WTO）在其《电子商务》专题报告中，对电子商务的定义是：电子商务是通过电信网络进行的生产、营销、销售和流通活动，它不仅指基于因特网（Internet）上的交易活动，而且指所有利用电子信息技术（information technology，IT）来解决问题、降低成本、增加价值和创造商业和贸易机会的商业活动，包括通过网络实现从原材料查询、采购、产品展示、订购到出品、储运、电子支付等一系列的贸易活动。

2）经济合作与发展组织（Organisation for Economic Co-operation and Development，OECD）对电子商务的定义是：电子商务是发生在开放网络上的包含企业之间（business to business）、企业与消费者之间（business to customer）的商业交易。

3）国际标准化组织（International Organization for Standardization，ISO）及国际电工委员会（International Electrical Commission，IEC）关于 EB 谅解备忘录对 EB 的定义是：电子商务（EB）是企业之间、企业与消费者之间信息内容与需求交换的一种通用术语。

4）美国政府在《全球电子商务纲要》中指出：电子商务是通过 Internet 进行的各项商务活动，包括广告、交易、支付、服务等活动，全球电子商务将会涉及世界各国。

5）加拿大电子商务协会给出电子商务更为严格的定义：电子商务是通过数字通信进行商品和服务买卖及资金转账，它还包括公司间和公司内利用电子邮件、电子数据交换（electronic data exchange，EDI）、文件传输、传真、电视会议、远程计算机联网所能实现的全部功能（如市场营销、金融结算、销售、商务谈判）。

此为试读，需要完整PDF请访问：www.ertongbook.com

6）IBM 公司给出的电子商务定义是：电子商务是在计算机网络环境下的商业化应用，不仅仅是硬件和软件的结合，而是在因特网（Internet）、企业内部网（Intranet）、企业外部网（Extranet）下进行的业务活动，其定义公式可以表示为：电子商务＝IT＋Web＋Business。

7）美国通用电气（General Electric，GE）公司对电子商务的定义是：电子商务是通过电子方式进行商业交易，分为企业与企业之间的电子商务、企业与消费者之间的电子商务。企业与企业间的电子商务以 EDI 为核心技术，以增值网（value added netword，VAN）和因特网（Internet）为主要手段，实现企业间业务流程的电子化，配合企业内部的电子化生产管理系统，提高企业从生产、库存到流通（包括物质和资金）各个环节的效率。企业与消费者之间的电子商务以 Internet 为主要服务提供手段，实现公众消费及相关付款方式的电子化。

综上所述，电子商务的定义可以从“广义”和“狭义”两个角度加以理解。广义的电子商务定义为：电子工具在商务活动中的应用。这些电子工具无论是初级的还是高级的，均涵盖其中，如电话、电报、Internet 等；商务活动是从泛商品的需求活动到泛商品的合理、合法的供给，除去典型的生产过程后的所有活动。其中的泛商品指实物与非实物、商品与商品化的生产要素等。狭义的电子商务定义为：在技术、经济高度发达的现代社会里，由掌握现代信息技术与商务理论及实务活动规则的人，系统化地运用网络手段和使用各类电子工具，高效率、低成本、安全、方便地从事以泛商品交换为中心的各种经济事务活动。一般认为，狭义电子商务是指基于互联网环境下的商品交易及以商品交易相关的商务活动；广义电子商务是指一切利用电子手段进行的商业活动，如电话购物、电视购物、POS（point of sale，销售终端）联机销售等。

2. 电子商务的特征

电子商务作为一种新型的应用，它的特征包括普遍性、方便性、整体性、安全性和协调性。

1）普遍性：电子商务作为一种新型的交易方式，将生产企业、流通企业、消费者和政府带入了一个网络经济、数字化生存的新天地。

2）方便性：在电子商务环境中，人们不再受到地域的限制，客户能通过非常便捷的方式完成过去较为繁杂的商务活动，如通过网络银行能够全天候地存取资金账户、查询资金进出等，同时可以使得企业对客户的服务质量大大提高。

3）整体性：电子商务能够规范事务处理的工作流程，将人工操作和电子信息处理集成为一个不可分割的整体，这样不仅能提高人力和物力的利用率，也可以提高系统运行的严密性。

4）安全性：在电子商务中，安全性是一个至关重要的问题，也是制约电子商务能否持续发展的重要因素。它要求系统能够提供一整套相关的安全解决方案，如加密机制、数字签名机制、存取控制、防火墙、安全管理等，既包括安全技术，也包括安全管理和相应的法律规范，这与传统的商务活动有着很大的不同。

5）协调性：商务活动本身是一种协调过程，它需要客户与公司内部、生产商、批发商、零售商间的协调。在电子商务环境下，更需要银行、金融机构、配送中心、网络通信部门等多个部门间的通力协作。电子商务的全过程往往是一气呵成的。

1.1.2　电子商务的交易模式

电子商务交易是指在网络平台上直接进行的在线交易（trade online），利用数字化技术将企业与企业、企业与消费者或消费者之间有机连接起来，实现从浏览、洽谈、签约、付款到交货等全部或部分业务的自动化处理。目前，按照电子商务中参与交易的对象，可以把电子商务的交易模式分为以下几种类型。

1）企业对企业（business to business）模式，简写为 B2B 模式，指企业与企业之间通过网络进行产品或服务的经营活动。例如，企业通过 Internet 与供应商联系订货、接收发票和付款。企业之间也可以通过网络来实现协同作用、资源管理及信息共享，以推动分销商、经销商和中心企业之间供应链的重组，提高业务的有效性并降低成本。基于该模式的电子商务活动，从未来的发展来看，仍将是电子商务的主流。

2）企业对消费者（business to customer）模式，简写为 B2C 模式，是企业通过 Internet 为消费者提供产品或服务的经营活动。随着网上商店的出现，产生了这种电子商务模式。这种模式既包括网上购物，也包括针对个人的网上银行等服务型的业务。例如，在 Internet 上已出现许多大型的网络商店，向消费者直接提供从图书、服装、食品到计算机、汽车等众多商品和服务。网上交易通常只涉及信用卡或其他电子货币。这种模式直接针对消费者，开创了一个崭新的庞大市场，其发展势头被普遍看好。

3）消费者对消费者（customer to customer）模式，简写为 C2C 模式，指网络服务提供商利用计算机和网络技术，提供有偿或无偿使用的电子商务平台和交易程序，允许交易双方（主要为个人用户）在其平台上独立开展以竞价、议价为主的在线交易模式。C2C 模式能够体现 Internet 的优势，在不同地域、不同时间，数量巨大的买方和同等数量的卖方通过一个平台找到合适的对象进行交易。同传统的市场相比，它不受时间和空间的限制，交易方式灵活，因而节约了大量的交易成本。

4）政府对企业（government to business）模式，简写为 G2B 模式，指政府组织与企业间的各项电子商务活动。例如，政府将采购的细节在 Internet 上公布，通过网上竞价方式进行招标，企业也要通过电子商务的方式进行投标。政府在推动电子商务发展方面起到了重要的作用，企业可以通过 Internet 办理缴税和投标等各项业务。

1.1.3　电子商务的交易流程

商务交易流程对于电子商务系统是十分重要的，它是指具体从事一个商贸交易过程中的实际操作步骤和处理流程。商品流通过程是以物流（商品的实物流动）为物质基础，信息流（商品相关信息的流动）贯穿始终，引导资金流（货币流动）正向流动的动态过程。电子商务的交易流程基于传统商务流程，但与传统商务流程有所不同。它是建立在 Internet 基础上，涉及商家、消费者、银行或金融机构、企业、政府机构、认证机构等多个方面。由于参与电子商务中的各方在物理上是互不了解的，因此整个过程并不是物理世界交易流程的完全照搬。

一般来说，电子商务的交易流程大致可以分为以下三个环节。

（1）交易前的准备

这一环节主要是指买卖双方和参与交易各方在签约前的准备活动。买方根据自己的需求，随时上网查询自己所需要的商品信息和商家，通过市场查询，确定自己的购货计

划（包括确定购买商品的种类、数量、规格、价格、购物地点和交易方式等）。卖方则利用 Internet 和各种贸易网络发布商品广告，积极上网推出自己商品的信息资源，寻找贸易伙伴和交易机会，扩大贸易范围和商品所占市场份额。在电子商务系统中，贸易信息的交流是通过买卖双方的网址和主页来完成的，这种信息的沟通方式，无论从效率还是从实践上，都是传统交易方式无法比拟的。

（2）交易协商和签订合同

这一环节主要指买卖双方对所有交易细节进行协商，并将双方协商的结果以文件的形式确定下来，即以书面文件形式和电子文件形式签订贸易合同。电子商务的特点是可以签订电子商务贸易合同，交易双方可以利用现代电子通信设备和通信方法，经过认真谈判和磋商后，将双方在交易中的权利和所承担的义务，以及对所购买商品的种类、数量、价格、交货地点、交货期、交货方式和运输方式、违约和索赔等合同条款，全部以电子交易合同作出全面详细的规定。合同双方可以利用 EDI 进行签约。也可以通过数字签名等方式进行签约。

（3）结算付款和索赔

买卖双方“签订”电子合同后，交易涉及的有关各方（如中介方、银行或金融机构、信用卡公司等）将参与到交易过程中。买卖双方要利用与电子商务有关的各方进行各种电子票据和电子单证的交换，直到办理完可以将所购商品从卖方按合同规定开始向买方发货的一切手续为止。其间最重要的是电子支付环节。

传统的以现金和支票为基础的付款方式在网络环境下有了很大的改变。改变的结果是，原来的支票支付方式被电子支票方式所取代；原来的现金支付方式被信用卡和电子现金所取代。电子商务中的电子支付系统能够完成资金的支付、清算，出具相应的交易单据，以及发货、到货管理等，直到买方收到自己所购的商品。这类系统由于涉及银行、运输等部门，因此运行机制的复杂程度和系统开发的难度会大大增加。另外，索赔过程是在买卖双方交易过程中出现违约时，需要进行违约处理的工作，由受损方向违约方索赔。

由此可见，该环节是整个电子商务交易流程最重要也是实现难度最大的一个环节，电子支付的完善是电子商务真正实现的基础，目前只有少数发达国家建立了较为完善的电子支付体系。

1.2　电子商务面临的安全威胁

1.2.1　电子商务中安全威胁的类型

1. 电子商务交易过程中的安全威胁

目前，电子商务发展面临的主要问题之一是如何保障电子交易过程中的安全性。交易的安全是网上贸易的基础和保障，也是电子商务技术的难点。围绕电子商务安全的防护技术已经成为目前电子商务研究的重点之一。在电子交易过程中，消费者和商家面临的安全威胁通常有以下几个方面，如图 1-1 所示。

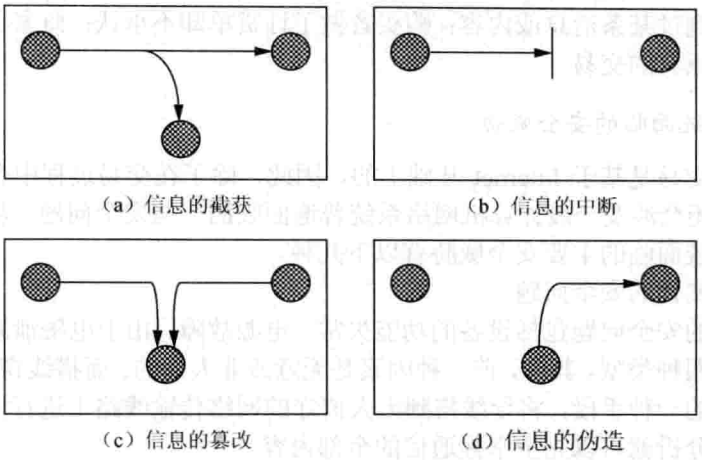

图 1-1　电子交易过程中安全威胁的类型

（1）信息的截获

在电子商务中，信息流和资金流以数据的形式在 Internet 中传输。在传输过程中，如果没有采用加密措施或加密强度不够，攻击者可能通过 Internet 在电磁波范围内安装截获装置或在数据报通过的网关和路由器上截获数据，获取传输的机密信息，或通过对信息流量、通信频率和长度等参数的分析，推测出有用的信息，如消费者的银行账号、密码，以及企业的商业机密等。

（2）信息的中断

这是针对可用性信息进行的攻击。在中断过程中，信息资源变得易损失或不可用。网络故障、操作错误、应用程序错误及计算机病毒等恶意攻击都能导致电子交易不能正常进行。

（3）信息的篡改

当攻击者熟悉了网络信息格式后，通过各种技术和手段对网络传输的信息进行中途修改并发往目的地，从而破坏信息的完整性。例如，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；删除某个消息或消息的某些部分；在消息中插入一些信息，让接收方不懂或接收错误的信息等。

（4）信息的伪造

当攻击者掌握了网络信息数据规律或解密了商务信息以后，可以伪装成合法用户或发送伪造的信息来欺骗其他用户，主要有以下两种方式。

一种是伪造电子邮件。例如，虚开网站和电子商店，给用户发电子邮件，收订货单；伪造大量用户，发电子邮件，穷尽商家服务器的资源，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等。

另外一种是假冒他人身份。例如，伪装成他人身份，进行非授权信息资源的访问或者骗取对方的信任；冒充网络控制程序，套取和修改使用权限、保密字、密钥等信息；接管合法用户，欺骗系统，占用合法用户的资源。

（5）交易抵赖

交易抵赖包括多个方面，如发送方事后否认曾经发送过某条消息或内容；接收方事

后否认曾经收到过某条消息或内容；购买者做了订货单却不承认；商家卖出的商品因价格差而不承认原有的交易。

2. 网络系统面临的安全威胁

由于电子交易是基于 Internet 基础上的，因此，除了在交易过程中会面临上述一些安全威胁外，还会涉及一般计算机网络系统普遍面临的一些安全问题。从网络安全角度考察，网络系统面临的主要安全威胁有以下几种。

（1）物理实体的安全问题

物理实体的安全问题包括设备的功能失常、电源故障、由于电磁泄漏引起的信息失密和搭线窃听四种类型。其中，前三种因素是无意或非人为的。而搭线窃听则是人为的，是非法者常用的一种手段，将导线搭到无人值守的网络传输线路上进行监听，通过解调和正确的协议分析就可以完全掌握通信的全部内容。

（2）自然灾害的威胁

计算机网络设备大多是一种易碎品，不能受重压或强烈的震动，更不能受强力冲击。所以，各种自然灾害、风暴、泥石流、建筑物破坏、火灾、水灾、空气污染等对计算机网络系统都构成了极大的威胁。

（3）黑客的恶意攻击

所谓黑客，现在一般泛指计算机信息系统的非法入侵者。黑客的攻击手段和方法多种多样，一般可以分为以下两种：一种是主动攻击，它以各种方式有选择地破坏信息的有效性和完整性；另一种是被动攻击，它是在不影响网络正常工作的情况下，进行截获、窃取、破译以获得重要机密信息。

（4）软件的漏洞和“后门”

在计算机网络安全领域，软件的漏洞是指软件系统上的缺陷，这种缺陷导致非法用户未经授权而获得访问系统的权限或提高其访问权限。随着计算机系统越来越复杂，开发一个大型的电子商务应用软件时，要想进行全面彻底的测试已经变得越来越不可能了。一个实际的电子商务系统，总会留下某些缺陷和漏洞。而“后门”是软件设计者为了进行非授权访问而在程序中故意设置的万能访问口令，这些口令无论是被攻破，还是只掌握在设计者手中，都对使用者的系统安全构成严重的威胁。

从以上分析可以得出，软件的漏洞和“后门”虽然都会对系统的安全造成威胁，但它们存在着明显的区别：漏洞是不可避免的，而“后门”是完全可以避免的；漏洞是难以预知的，而“后门”是人为故意设置的。

（5）网络协议的安全漏洞

众所周知，电子商务系统是基于 Internet 平台上的信息系统，通过 Internet 基础设施向电子商务应用提供各种网络服务。而网络服务是通过各种协议来实现的。目前，Internet 采用的是 TCP/IP（transmission control protocol/Internet protocol，传输控制协议/因特网互联协议）协议簇，如 TCP、FTP（file transfer protocol，文件传输协议）和 HTTP（hypertext transfer protocol，超文本传输协议）等，在安全方面都存在着一定的缺陷。当今许多黑客攻击就是利用了这些协议的安全漏洞才得逞的。事实上，网络协议的安全漏洞是当前 Internet 面临的一个重要安全问题。

（6）计算机病毒的攻击

由于 Internet 的开放性，计算机病毒在网络上的传播比以前快了许多，而且 Internet

的发展和普及又促进了病毒制造者之间的交流，使新病毒及其变种层出不穷，杀伤力也大有提高，这些都给个人和企业带来了许多不便和经济损失。

1.2.2　电子商务消费者面临的安全威胁

在电子商务活动中，消费者面临的威胁有以下几种。

1）虚假订单。一个假冒者可能会以客户的名字来订购商品，而且有可能收到商品，而此时客户却被要求付款或返还商品。

2）付款后不能收到商品。在客户付款后，销售商中的内部人员不将订单和款项转发给执行部门，因而使客户不能收到商品。

3）机密性丧失。客户有可能将秘密的个人数据或自己的身份数据［如 PIN（personal identification number，个人识别码）、口令等］发送给冒充销售商的机构，这些信息也可能会在传递过程中被窃听。

4）拒绝服务。攻击者可能向销售商的服务器发送大量的虚假订单来挤占其资源，从而使合法用户不能得到正常的服务。

5）电子货币丢失。可能是由物理破坏或者被偷窃导致，这通常会给用户带来不可挽回的损失。

1.2.3　电子商务商家面临的安全威胁

除普通的安全威胁外，电子商务服务器通常还面临如下一些特殊的安全威胁。

1）系统中心安全性被破坏。入侵者假冒成合法用户来改变用户数据（如商家送达地址）、解除用户订单或生成虚拟订单等。

2）竞争者威胁。恶意竞争者以他人的名义来订购商品，从而了解有关商品的递送状况和货物的库存情况。

3）商业机密安全。客户资料被竞争者获悉。

4）假冒威胁。不诚实的人建立与销售者服务器名字相同的另一个 Web 服务器来假冒销售者；虚拟订单；获取他人的机密数据。例如，某人想要了解另一人在销售商处的信誉时，他以另一人的名字向销售商订购昂贵的商品，然后观察销售商的行动。假如销售商认可该订单，则说明被观察者的信誉度高；否则，则说明被观察者的信誉度不高。

5）信用威胁。买方提交订单后却不付款。

1.3　电子商务系统的安全体系结构

电子商务的一个重要技术特征是利用信息技术来传输和处理商业信息。既然电子商务系统是建立在计算机系统之上的商务系统，我们从逻辑上可以将整个体系结构分为底层的物理网络安全和上层的电子交易安全这两个方面。网络服务层提供物理网络的安全保障；而加密技术层、安全认证层、交易协议层和电子商务应用系统层提供电子交易安全保障。计算机网络安全包括计算机网络设备安全、计算机网络系统安全、数据库安全等，其特征是针对计算机网络本身可能存在的安全问题，实施网络安全增强方案，以保证计算机网络自身的安全性为目标。电子交易安全则紧紧围绕传统商务在互联网上应用

此为试读，需要完整PDF请访问：www.ertongbook.com