21世纪高职高专创新教材

电子商务系列

电子商务安全

主　编　宋林林
副主编　于海峰　于硕文　佟　昕
参　编　王　涛　刘万铭　王子轶

WUHAN UNIVERSITY PRESS
武汉大学出版社

图书在版编目(CIP)数据

电子商务安全/宋林林编著. —武汉：武汉大学出版社，2013.2
21世纪高职高专创新教材
ISBN 978-7-307-10543-0

Ⅰ. 电… Ⅱ. 宋… Ⅲ. 电子商务—安全技术—高等职业教育—教材 Ⅳ. F713.36

中国版本图书馆CIP数据核字(2013)第039158号

责任编辑：王 师

出版发行：**武汉大学出版社** (430072 武昌 珞珈山)
(电子邮件：cbs22@whu.edu.cn 网址：www.wdp.whu.edu.cn)
印刷：北京泽宇印刷有限公司
开本：787×1092 1/16 印张：16 字数：332千字
版次：2013年2月第1版 2013年3月第1次印刷
ISBN 978-7-307-10543-0/F·1757 定价：33.00元

内 容 简 介

本书是依据《国家中长期教育改革和发展规划纲要(2010—2020年)》的指导精神,并结合教育部最新颁布的教学指导要求及高职高专学校教学特点编写而成。本书注重实践能力的培养,不但要求学生掌握电子商务的安全技术,而且要求学生提升电子商务安全理念,提高电子商务安全防范的操作技能,切实提高学生专业动手实践能力和职业技术素质是本教程追求的主要目标。

全书共分9章,主要包括电子商务安全概述、网站系统的安全与防范、防火墙与VPN技术、用户终端安全设置、电子商务的数据加密技术、电子商务中的认证技术、安全电子交易协议、电子商务安全支付技术和移动电子商务安全等方面的内容。

本书可作为高职高专院校、成人高校及民办高校学生使用,亦可作为广大青年朋友学习的参考用书。

前言

本书是依据《国家中长期教育改革和发展规划纲要(2010—2020年)》的指导精神,并结合教育部最新颁布的教学指导要求及高职高专学校教学特点编写而成。

电子商务的发展给人们的工作和生活带来了新的尝试和便利,也为人们带来了无限商机。但许多商业机构对是否采用电子商务仍持观望态度,主要原因是对网上运作的安全问题存有疑虑。在竞争激烈的市场环境下,电子商务的一些信息可能属于商业机密,一旦信息失窃,企业的损失将不可估量。因此,在运用电子商务模式进行贸易的过程中,安全问题就成为电子商务最为核心的问题。

电子商务的进行都是由客户机、通信网络、服务器组成。但是由于互联网的开放性、共享性和无序性,使得电子商务面临着多种风险和威胁。电子商务安全问题一直困扰着电子商务的发展。因此电子商务专业人才应该必须具备保障电子商务安全运行的能力。

本书主要是围绕电子商务活动的安全性及其保障,针对与电子商务应用相关的基本安全问题,全面介绍电子商务安全的基本理论和关键技术,主要内容包括电子商务的安全问题、电子商务安全需求、安全体系结构、网站安全技术、防火墙技术、VPN技术、用户终端安全设置、密码学基础、公钥基础设施(PKI)、PKI的体系与功能、认证技术、数字签名、安全电子交易(SET)协议、安全套接层(SSL)协议、电子商务的主要支付机制、支付交易安全、移动电子商务安全技术等。

本书特色如下:

第一,体系完整,结构合理。既力求突出电子商务安全的技术特点,又强调

电子商务的安全本质，主线索清晰，方便教师讲解和学生学习。

第二，语言通俗易懂。概念陈述力求简洁、准确，技术介绍深入浅出，应用分析扼要、生动。

第三，案例精致，紧扣主题。本书穿插了大量局部和综合案例。案例分析主题鲜明，说明准确。

第四，注重能力的培养。通过项目任务的操作实施，注重培养学生的动手能力。

本书可作为高职高专院校、成人高校及民办高校学生使用，亦可作为广大青年朋友学习的参考用书。

本书由辽宁经济职业技术学院宋林林担任主编，于海峰、于硕文、佟昕担任副主编，王涛、刘乃铭、王子轶参加了教材的编写工作。具体分工如下：宋林林编写第1、9章，于海峰编写第4、5、7章，于硕文编写第2、3章，佟昕编写第6、8章，王涛参加了第5、6章的编写工作，刘乃铭参加了第2、9章的编写工作，王子轶参加了第3、4章的编写工作。

在编写过程中，编者借鉴和吸收了国内外专家学者的最新科研成果，同时也参阅了大量相关书籍和资料，在此谨向原作者表示深深的谢意！

由于编者水平有限，不足之处在所难免，恳请专家、同行和广大读者批评指正，以便再版时修订完善。

编　者

目录

第1章

本章索引

- 电子商务安全概念
- 电子商务安全问题
- 电子商务安全需求
- 电子商务安全体系结构

学习目标

1. 掌握电子商务安全需求分析
2. 掌握电子商务安全体系结构

引导案例

2011年蓬勃发展的电子商务成为黑客窥测的主要对象，网购、支付、配送、推广、售后等多个环节均遭到黑客有针对性的攻击。瑞星报告称：黑客和病毒攻击越来越有针对性，网购、游戏等特定人群面临较大安全风险，在可预见的时间段内，这个发展趋势仍将保持。

据瑞星公司发布《瑞星2011年度安全报告》显示，目前威胁国内互联网安全的因素主要包括3个方面：病毒和木马等恶意程序、钓鱼诈骗、黑客“拖库”攻击。黑客开始以取得的用户数据库为基础，利用“社会工程学”原理对用户进行全面的诈骗、密码猜解、身份伪造、病毒和挂马等攻击，这种新型攻击已经全面渗透到黑色产业的各个环节，显示出巨大的现实危害。

与2010年相比，由黑客“拖库”因素带来的安全问题显著上升，包括CSDN、天涯在内的一批互联网网站用户数据库被窃取，导致用户隐私大规模被泄漏，这给整个互联网带来巨大安全风险。

报告期内，瑞星公司截获病毒922万个，比去年上升22.9%，受害网民11.7亿人次。从本年度新增病毒的种类来看，木马(trojan)共有7 087 420个，占76.85%，当之无愧成为所有恶意程序中最大的类别。此外，新增的病毒中包括win32感染型病毒795 893个，占总体数量的8.63%，已经取代后门(backdoor)成为第二大类。后门和黑客程序(hack)两类的数量几乎相等，皆以4.33%的比例并列第三。病毒释放器(dropper)、蠕虫病毒(worm)和广告程序(adware)依次排列，比例分别为2.51%、2.29%和2.25%。

报告期内，瑞星还截获挂马网站3 471 148个，比去年同期下降了89.74%(2010年为3 382万个)。从数据上来看，单个挂马网站的侵害人数保持平稳，这说明黑客并未放弃网站挂马的攻击方式。

报告数据显示，单个受害用户的受损金额与往年相比有很大增长，这是因为2011年出现了多种诈骗方式：黑客通过MSN和QQ进行“老同学，帮我买几张充值卡”诈骗，利用团购进行“假iPhone诈骗”，利用搜索引擎广告来出售假冒伪劣商品等多种新型钓鱼诈骗方式，使得网民一旦中招，就会损失数千、甚至上万的金钱。

随着Internet的发展，电子商务已经逐渐成为人们进行商务活动的新模式，越来越多的人通过Internet进行商务活动。电子商务的发展给人们的工作和生活带来了新的尝试和便利，前景十分诱人，也为人们带来了无限商机。但许多商业机构对是否采用电子商务仍持观望态度，主要原因是对网上运作的安全问题存有疑虑。在竞争激烈的市场环境下，电子商务的一些信息可能属于商业机密。一旦信息失窃，企业的损失将不可估量。因此，在运用电子商务模式进行贸易的过程中，安全问题就成为电子商务最核心的问题，也是电子商务得以顺

利推行的保障。它包括有效保障通信网络、信息系统的安全，确保信息的真实性、保密性、完整性、不可否认性和不可更改性等。

1.1　电子商务安全概念

电子商务作为一种全新的商务模式，它有很大的发展前途。同时，这种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。如何建立一个安全、便捷的电子商务应用环境，对信息提供足够的保护，是商家和用户都十分关注的话题。

电子商务安全就是保护在电子商务系统里的企业或个人资产不受未经授权的访问、使用、篡改或破坏。电子商务安全覆盖整个电子商务链的各个环节：由客户端→通信传输→服务器端、甚至相关企业的后台信息系统等。电子商务安全问题已成为电子商务的关键和核心。

商务交易安全紧紧围绕传统商务在互联网上应用时产生的各种安全问题，在计算机网络安全的基础上，保障电子交易和电子支付等电子商务的顺利进行，即实现电子商务的保密性、完整性、可鉴别性、不可伪造性和不可抵赖性等。

计算机网络安全与商务交易安全实际上是密不可分的，两者相辅相成，缺一不可。没有计算机网络安全作为基础，商务交易安全就犹如空中楼阁，无从谈起；没有商务交易安全保障，即使计算机网络再安全，仍然无法达到电子商务所特有的安全要求。

电子商务安全以网络安全为基础，但是，电子商务安全与网络安全又是有区别的。首先，网络不可能绝对安全，在这种情况下，还需要运行安全的电子商务；其次，即使网络绝对安全，也不能保障电子商务的安全。电子商务安全除了基础要求之外，还有特殊要求。

从安全等级来说，从下至上有计算机密码安全、局域网安全、互联网安全和信息安全之分，而电子商务安全属于信息安全的范畴，涉及信息的机密性、完整性、认证性等方面。电子商务安全又有它自身的特殊性，即以电子交易安全和电子支付安全为核心，有更复杂的机密性概念和更严格的身份认证功能，对不可拒绝性有新的要求，需要有法律依据性和货币直接流通性特点，还需要网络设有的其他服务（如数字时间戳服务）等。

电子商务安全具有如下四大特性。

1. 电子商务安全是一个系统概念

电子商务安全问题不仅仅是个技术性的问题，更重要的是管理问题，而且它还与社会道德、行业管理以及人们的行为模式等紧密地联系在一起。

2. 电子商务安全是相对的

就像房子的窗户上只有一块玻璃一样，一般说来是安全的，但是如果用石头去砸，那就不安全了。但我们不会因为石头能砸碎玻璃而去怀疑玻璃的安全性，因为大家都有一个普遍的认识，那就是玻璃是不能砸的，有了玻璃就可以保证房子的安全。同样，不能追求一个永远也攻不破的安全系统，安全与管理始终是联系在一起的。也就是说，安全是相对的，而

不是绝对的，要想网站永远不受攻击，不出安全问题是不可能的。

3. 电子商务安全是有代价的

无论是现在国外的 B2B 还是 B2C，都要考虑到安全的代价和成本问题。如果只注重速度，就必定要以牺牲安全作为代价；如果要考虑安全，速度就得慢一点。当然这与电子商务的具体应用有关，如果不直接牵涉到支付等敏感问题，对安全的要求就可以低一些；如果牵涉到支付问题，对安全的要求就要高一些，所以安全是有成本和代价的。作为一个经营者，应该综合考虑这些因素；作为安全技术的提供者，在研发技术时也要考虑到这些因素。

4. 电子商务安全是发展的、动态的

今天安全，但明天不一定安全，因为网络的攻防是此消彼长、道高一尺魔高一丈的事情。尤其是安全技术，它的敏感性、竞争性以及对抗性很强，需要不断地检查、评估和调整相应的安全策略。没有一劳永逸的安全，也没有一蹴而就的安全。

1.2 电子商务安全问题

自电子商务产生之后，安全事故经常出现。例如：从 2000 年 2 月 7 日至 2 月 9 日，短短三天的时间内，美国几大主要网上站点均遭受不明黑客攻击，其中包括著名的电子商务网站电子港湾(eBay)和亚马逊(Amazon)。在黑客开始所谓“拒绝服务(Denial of Service，DoS)”式的攻击后，亚马逊(Amazon)站点容纳顾客的能力急剧下降。数分钟后访客数量只有平时同一时段访客数量的 1.5%，大约一小时后亚马逊网站才恢复正常。据统计，三天来黑客袭击各大网站所造成的直接或间接经济损失高达数十亿美元。

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 Internet 交通均发生了大面积堵塞，估计至少有 22 000 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 13 000 台自动取款机瘫痪，大量银行客户无法使用取款机取款。

电子商务的安全威胁，需要从客户机到电子商务服务器的整个过程以及电子商务交易过程中的安全性。在考察“电子商务链”上每个逻辑链条时，必须包括客户机、在通信信道上传输的消息、万维网(WWW)和电子商务服务器(包括服务器端所有的硬件)等。

1.2.1 客户机安全问题

在实时的、动态的、可交互的 WWW 内容出现前，网页是静态的。静态页面是用 WWW 标准页面描述语言 HTML 编制的，其作用只是显示内容并提供到其他页面的链接。为增加页面的生动性以及客户机与服务器之间的交互能力，同时也为了分担服务器端的负载，动态网页技术得以广泛应用，相应地安全状态也就发生了变化。此外，一些其他的相关技术也成为威胁客户机安全的不确定性因素，如被恶意利用也会招致不良后果。

1. 动态内容

动态内容是指在页面上嵌入一段对用户透明的程序，它可产生一些动态的效果，例如显

示动态图像、下载和播放音乐或实现基于 WWW 的电子表格程序、客户机中的表单数据提交等交互操作。动态内容扩展了 HTML 的功能，使页面更为生动活泼，同时，动态内容还将原来要在服务器上完成的某些辅助性处理任务转给在多数情况下处于闲置状态的客户机来完成，均衡了服务器的负载。

动态内容有多种形式，最著名的动态内容形式包括 JavaScript 和 VBScript、JavaApplet 和 ActiveX 控件等。这些程序经常被企图破坏客户机的人伪装成无害的内容，一旦触发运行，就会对客户机带来安全威胁。这种隐藏在程序或页面里而掩盖其真实目的的程序被统称为特洛伊木马。它可窃听计算机上的保密信息，并将这些信息传给它的远程 WWW 服务器，从而构成保密性侵害。而且，特洛伊木马还可改变或删除客户机上的信息，构成完整性和不可拒绝性侵害。

2. 相关技术或机制

能够威胁到客户机安全的因素，除了动态内容，还包括其他一些相关技术或机制。这些技术或机制和动态内容相呼应，使得其对客户机的安全威胁势态扩大，或者后果更加严重。

(1)cookie

cookie 的存在也使得客户机更加容易泄露用户的秘密。通过 WWW 页面潜入的恶意代码可使通常存放在 cookie 里的信用卡号、用户名和口令等敏感信息暴露。cookie 的设计目的是解决需要记忆关于顾客订单信息或用户名与口令等问题。因为互联网是无状态的，它不能记忆从一个页面到另一个页面间的响应。但这也给有些恶意的动态内容提供了可乘之机。

(2)邮件通讯簿

使用客户端邮件收发软件的用户通常在电子邮件通讯簿上存放联系人的信息，一些计算机病毒可以成功地检测到这些内容，并把病毒发给这些联系人。

(3)信息隐蔽

一般情况下，计算机文件中都有冗余的或能为其他信息所替代的无关信息。后者一般驻留在背景中，使人无法看到。信息隐蔽是指隐藏在另一段信息中的信息，它提供将加密的文件隐藏在另一个文件中的保护方式，粗心的观察者看不到其中含有的重要信息。

1.2.2　通信信道的安全问题

互联网是将客户机和电子商务服务器连接起来的电子通道。安全威胁的第二个环节就是将客户机连到服务器上的传输信道，即互联网。虽然互联网起源于军事网络，但美国国防部高级研究项目中心建造网络的主要目的不是为了安全传输，而是为防止一个或多个通信线路被切断即提供冗余传输。互联网发展到今天，其不安全状态与最初相比并没有多大改观。在互联网上传输的信息，从起始节点经由若干中间节点到目标节点之间的路径是随机选择的。在同一起始节点和目标节点之间发送信息时，每次所用的路径也都是不同的，所以根本无法控制信息的传输路径，也不知道信息包曾到过哪里，因而无法保证信息传输时所通

过的每台计算机都是安全的和无恶意的。如果信息包在传递途中被任意一个中间节点窃取、篡改甚至删除，那么客户所遭受的损失将是无法弥补的。

1. 搭线窃听

开展电子商务的一个很大的安全威胁就是敏感信息或个人真实信息被窃。在互联网上，有种叫做“嗅探器”的特殊软件能够记录下通过某个网关或路由器的信息。它类似于在电话线上搭线并录下一段对话。嗅探器可以截获并阅读电子邮件信息，也可记录敏感信息或个人真实信息，或者用来攻击相邻的网络，并且能够做到不留痕迹。

2. IP 欺骗

所谓 IP 欺骗，就是伪装成合法主机的 IP 地址与目标主机建立连接关系。通过这种欺骗方法可以把某个服务器的访问者引到一个虚假网站，或者假冒合法用户主机名进入目标服务器。

当用户主机与目标服务器之间建立了 TCP 连接后，通过双方信息包的不断交互取得用户主机或服务器的信息。入侵者猜测出信息包的序列号，就能够向用户主机或服务器发出伪造的、看上去是来自合法主机的数据包，构成对完整性的威胁。

此外，用户主机与服务器之间建立网络连接时经常需要某种形式的认证，发生在应用层上的认证是不透明的，如进行 FTP 或 Telnet 连接时需要用户输入密码和账号。IP 地址欺骗可以针对非应用层的、通常是自发的、无需用户参与的认证，从而达到非法入侵的目的。

3. IP 源端路由选择

IP 数据包在互联网上传输达到最终目的主机之前通常要经过许多路由器。路由器动态决定了 IP 数据包的传输路线。允许源端路由选择就是允许 IP 数据包向经过的路由器声明达到目标主机所希望经过的路由。

入侵者利用 IP 数据包源端路由选择避开那些包含过滤路由器、防火墙以及其他安全检查机制的路由，就可以访问在正常情况下所不能访问的主机。另外，如果目标主机的访问控制机制是认证源主机的 IP 地址，入侵者使用 IP 源端路由选择就可以有效地通过目标主机的认证。

4. 目标扫描

入侵者在确定扫描目标系统后，利用一些扫描程序和安全分析工具，如 ISS 扫描器、SATAN 等，寻求该系统的安全漏洞或弱点，并试图找到安全性最弱的主机作为入侵的对象。如果目标主机的管理员系统配置不当，或者未能及时发现并更新针对产品或系统安全漏洞的补丁程序，就极易被攻破薄弱主机，继而造成对与本机建立了访问链接和信任关系的其他网络计算机被攻破的连锁反应，最终威胁到整个系统。

1.2.3 服务器的安全问题

客户机、互联网和服务器的电子商务链上第三个环节是服务器。企业借助各种服务器软件设置自己的 WWW 服务器、FTP 服务器、E-mail 服务器等。对企图破坏或非法获取信息的人来说，服务器有很多弱点可被利用。攻击的入口有 WWW 服务器及其软件、数据库

和数据库服务器以及通用网关接口 CGI(Common Gateway Interface)程序或其他工具程序。

1. WWW 服务器

WWW 服务器软件是用来响应 HTTP 请求并传送 HTML 格式的页面的,其主要设计目标是支持 WWW 服务和方便使用。通常该类软件比较复杂,包含错误代码的概率也较高,因此含有许多已知的和未知的安全漏洞。这些漏洞经常被攻击者利用,加之系统管理员的一些不当管理行为,极易造成系统的瘫痪或信息的泄露等严重后果。

2. 数据库服务器

电子商务系统用数据库存储用户数据,并可从 WWW 服务器所连的数据库中检索产品信息。数据库除存储产品信息外,还可能保存有价值的信息或隐私信息,如果这些信息被更改或泄露将会给公司带来无法弥补的损失。

现在多数大型数据库都使用基于用户名和口令的权限安全措施,一旦用户获准访问数据库,就可查看数据库中相关内容。而有些数据库没有以安全方式存储用户名与口令,或没有对数据库进行安全保护,仅仅依赖 WWW 服务器的安全措施。如果有人得到用户的认证信息,他就能伪装成合法的数据库用户来下载保密的信息。

此外,隐藏在数据库系统里的恶意程序可将数据权限降级,把敏感信息发到未保护的区域。这样,所有用户都可访问这些信息,其中当然包括那些潜在的侵入者。

3. CGI

通用网关接口 CGI 可实现从 WWW 服务器到另一个程序(如数据库程序)的信息传输。CGI 和接收它所传输数据的程序为网页提供了动态内容。同 WWW 服务器一样,CGI 脚本是能以高权限运行的程序,并且运行起来不受 Java 运行程序安全的限制,如果滥用就会带来安全威胁。因此,恶意的 CGI 程序能自由访问系统资源,使系统失效、调用删除文件的系统程序或查看顾客的保密信息。

4. ASP

活动服务器页面 ASP(Active Server Pages)是微软公司推出的工具软件,可以在服务器端运行脚本语言 VBScript 和 JavaScript 编写的程序。ASP 简单实用、灵活而强大,可实现与客户端交互信息和数据库访问等操作。但 ASP 也存在安全漏洞,通过 ASP 可以入侵 WWW 服务器,窃取服务器上的文件,捕获 Web 数据库等系统的用户口令,删除服务器上的文件,直到造成系统损坏。

5. 邮件炸弹

邮件炸弹是将大量的消息发给同一个电子邮件地址,目标电子邮件地址收到的大量邮件超出了所允许的邮件区域限制,导致邮件系统堵塞或失效。邮件炸弹通常会导致邮件服务器拒绝服务。

6. 溢出攻击

通过客户机传输给 WWW 服务器或直接驻留在服务器上的 Java 或 C++程序需要经

常使用缓存。缓存中存放了从文件或数据库中读取的数据，是数据进出的临时存放区域。但是向缓存发送数据的程序如果出错，就会导致数据或指令替代了内存指定区域外的内容，即缓存溢出。缓存溢出的后果就是，程序运行遇到意外然后死机，从而破坏服务器的“不可拒绝性”。互联网蠕虫病毒就是这样的程序，它引起的溢出会消耗掉所有系统资源，直到主机停止运行。

另一种溢出攻击就是将指令写在关键的内存位置上，使侵入的程序在完成了覆盖缓存内容后进入系统保留区。保留区内存储着关键性信息，如 CPU 寄存器的内容和控制权移交前程序的计算状态。当控制权返还给原程序时，保留区的内容就会重新载入 CPU 寄存器，将控制权交给程序的下一条指令。但在攻击发生时，控制权将返还给攻击程序。而不是让出控制权的原程序。WWW 服务器通过载入记录攻击程序地址的内部寄存器来恢复运行。恢复运行的攻击程序将会获得很高的超级用户权限，这就使每个程序都可能被侵入的程序泄密或破坏。

7. 口令破译

用户所选的口令不当或者攻击者使用一些工具软件，也会构成安全威胁。有的用户所选的口令非常简单或者规律性很强，极易被猜出；再者是有人通过使用字典攻击程序，按电子字典里的每个单词来验证口令，那些较短并缺少变化的口令就能被攻破。另外，攻击者使用网络监听工具软件也可以监视网络上传输的数据包，从而使口令等关键信息被截获。用户口令的泄露往往会使非法者以合法的身份进入服务器敏感区域，并且可能长时间不会被发现。

1.2.4 交易实施的安全问题

目前电子商务发展面临的主要问题之一是如何保障电子商务交易实施中的安全性。交易安全是网上贸易的基础和保障，同时也是电子商务技术的难点，围绕电子商务安全的相关技术已经成为目前电子商务研究的重点之一。

交易实施安全是电子商务系统所特有的安全要求。在交易过程中，消费者和商家面临的安全威胁通常有如下几种。

①虚假订单。假冒者以客户名义订购商品，而要求客户付款或返还商品。

②收不到商品。买家付款后，却收不到商品。

③得不到货款。商家发货后，得不到付款。

④否认交易。交易双方之一方在交易后，否认交易曾经发生，或否认曾授权进行此交易的事实。

1.3 电子商务安全需求

由于互联网本身的开放性及目前网络技术发展的局限性，网上交易面临着种种安全性威胁。交易安全问题可归结为如下几个核心问题：机密性、完整性、匿名性、防抵赖性、有效性和可靠性。

1.机密性

电子商务是建立在开放的网络环境上的，维护商业机密是电子商务系统的最根本的安全需求。电子商务系统应对传输信息进行加密处理，以防止交易过程中信息被非法截获或读取，从而导致泄密。

传统的交易中，一般是通过面对面的信息交换，或者通过邮寄或可靠的通信渠道发送商业报文，达到商业保密的目的。而电子商务是建立在一个开放的网络环境上，当交易双方通过互联网交换信息时，其他人就有可能知道他们的通信内容。同样，存储在网络上的文件信息如果不加密的话，也有可能被黑客窃取。因此，电子商务的另一个重要的安全需求就是信息的保密性。也就意味着，一定要对重要信息进行加密，即使中间被人截获或窃取了数据，也无法识别信息的真实内容，这样就可以确保商业机密信息不致被泄露。

2.完整性

电子商务系统应防止对交易信息的篡改，防止数据传输过程中交易信息的丢失和重复，并保证信息传递次序的统一。

当网络面临主动攻击时，攻击者通过篡改或部分删除交易过程中发送的信息，破坏信息的完整性，使交易的双方蒙受损失。例如，A给B发了如下一份报文："请给C汇一百元。"报文在传输过程中遭到D的篡改，D将报文改为："请给D汇一百元。"这样，最终B收到的报文为："请给D汇一百元。"B按照报文给D汇了一百元，显然这不是A的本意。从这个例子可以看到，保证信息的完整性也是电子商务活动中一个重要的安全需求。这就要求交易双方能够验证收到的信息是否完整，即信息是否被篡改或部分删除等。

3.匿名性

电子商务系统应确保交易的匿名性，防止交易过程被跟踪，保证交易过程中不把用户的个人信息泄露给未知的或不可信的个体，确保合法用户的隐私不被侵犯。

4.防抵赖性

电子商务系统应有效防止商业欺诈行为的发生，保证商业信用和行为的不可否认性，保证交易各方对已做交易无法抵赖。

传统交易中，交易双方通过在交易合同、契约或贸易单据等书面文件上的手写签名或印章，确定合同、契约、单据的可靠性并预防抵赖行为的发生，也就是常说的"白纸黑字"。但在无纸化的电子交易中，不可能再通过传统的手写签名和印章来预防抵赖行为的发生。因此，保证交易过程中的不可否认性也是电子商务活动中的一个重要的安全需求。这意味着，电子交易通信过程的各个环节都必须是不可否认的，即交易一旦达成，发送方不能否认发送的信息，接收方不能篡改所收到的信息。

5.有效性

电子商务系统应有效防止系统延迟或拒绝服务情况的发生。要对网络故障、硬件故障、操作错误、应用程序错误、系统软件错误及计算机病毒所产生的潜在威胁加以控制和预防，保证交易数据在确定的时刻、确定的地点是有效的。

6. 可靠性

电子商务系统应该提供通信双方进行身份认证的机制，确保交易双方身份信息的可靠和合法，应该实现系统对用户身份的有效确认和对私有密钥与口令的有效保护，对非法攻击能够进行有效防范，防止假冒身份在网上交易、诈骗。

在传统的交易中，交易双方往往是面对面进行交易活动的，这样很容易确认对方的身份，即使互不熟悉，还可以通过对方的签名、印章、证书等一系列有形的身份凭证来鉴别对方的身份，还可以通过声音信号来识别对方身份。然而，网上交易的双方可能素昧平生、相隔万里，所以电子商务首要的安全需求应是保证身份的可认证性。也就是说，在双方进行交易前，首先要确认对方的身份，要求交易双方的身份不能被第三者假冒或伪装。

1.4 电子商务安全体系结构

电子商务的安全体系结构是保证电子商务中数据安全的一个完整的逻辑结构，同时它也为交易过程的安全提供了基本保障。电子商务安全体系结构如图 1-1 所示。

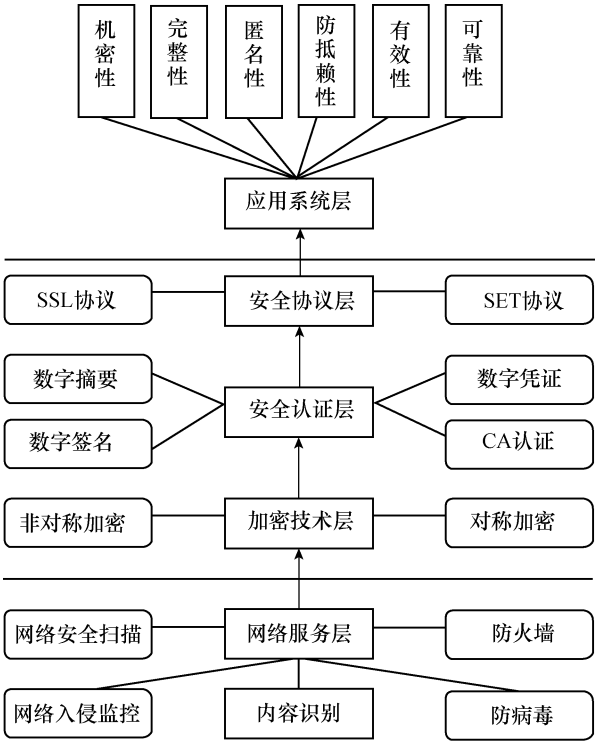

图 1-1 电子商务安全体系结构

电子商务安全体系结构由网络服务层、加密技术层、安全认证层、安全协议层、电子商务应用系统层 5 个层次组成。从图 1-1 中可以看出，下层是上层的基础，为上层提供了技术支

持，上层是下层的扩展与递进。各层之间相互依赖、相互关联，构成统一整体。电子商务安全问题可归结为网络安全和商务交易安全这两个方面。网络服务层提供网络安全，加密技术层、安全认证层、安全协议层、应用系统层提供商务交易安全。

计算机网络安全和商务交易安全是密不可分的，两者相辅相成、缺一不可。没有计算机网络安全作为基础，商务交易安全无从谈起；没有商务交易安全，即使计算机网络本身再怎么安全，也无法满足电子商务所特有的安全要求，电子商务安全也无法实现。

1.4.1　网络安全

电子商务系统是通过网络实现的，需要利用互联网的基础设施和标准，因此构成电子商务安全系统结构的底层是网络服务层。网络服务层是各种电子商务应用系统的基础，提供信息传输功能、用户接入方式和安全通信服务，并保证网络运行安全。网络服务层是电子商务应用系统的网络服务平台。

网络服务层也提供计算机网络安全。计算机网络安全主要包括：计算机网络的物理安全、计算机网络系统安全和数据库安全等。网络安全主要是针对计算机网络本身可能存在的安全问题，实施网络安全方案。计算机网络安全采用的主要安全技术有防火墙技术、加密技术、漏洞扫描技术、入侵检测技术、反病毒技术和安全审计技术等，用以保证计算机网络自身的安全。

1. 防火墙技术

防火墙是一种常用的网络安全装置，安放在内部网络与外部网络的连接处。它既可以防止外部人员对内部网络的恶意攻击，又可以防止内部人员非法访问外部网络。但是，由于内部人员访问内部网络时不需要经过防火墙，因此它防止不了内部人员的攻击。有多种实现防火墙的技术，如包过滤、代理服务器、双穴主机和屏蔽子网网关等。其中实现起来比较简单的是包过滤，它是一个检查通过它的数据包的路由器，限定外部用户的数据包。其原理是监视并过滤网络上流入流出的 IP 包，拒绝发送可疑的包。包过滤是运用一定的规则把一些经过它的 IP 包过滤掉的方法来实现的。通常，可以根据 IP 中的以下字段来进行过滤操作：源 IP 地址、目的 IP 地址、TCP/UDP 源端口或 TCP/LTDP 目的端口号等。

2. 加密技术

数据加密技术可以用来保护网络系统中包括用户数据在内的所有数据流。只有接收信息的用户或网络设备才能够解密所加密的数据，从而在不对网络环境作特殊要求的前提下从根本上保证网络信息的机密性、完整性和可用性。

3. 漏洞扫描技术

漏洞扫描是自动检测远端或本地主机安全漏洞的技术。它通过执行一些脚本文件对系统进行攻击并记录它的反应，从而发现其中的漏洞。

漏洞是硬件、软件或策略上的缺陷，这些缺陷使得攻击者能够在未授权的情况下访问甚至控制系统。漏洞的危害可以简单地用木桶原理加以说明：一个木桶能盛多少水，不在于组成它的最长的那根木料，而取决于木桶上最短的那一根。同样对于一个系统来说，它的安全

性不在于它是否采用了最新的加密算法或最先进的设备，而是由系统本身最薄弱之处，即漏洞所决定的。只要这个漏洞被发现，系统就有可能成为网络攻击的牺牲品。

早期的扫描程序是专门为 UNIX 系统编写的。随着越来越多的操作系统开始支持 TCP/IP，每一种平台上都出现了扫描工具(Scanner)，例如基于 Windows 平台的扫描常用技术包括 Ping 扫射、端口扫描、操作系统识别和穿透防火墙的扫描等。

4. 入侵检测技术

入侵检测技术通过获取网络上的所有报文，并对报文进行分析处理，报告异常和重要的数据模式和行为模式，使网络安全管理员清楚地了解网络上发生的事件，以便能够采取行动阻止可能发生的破坏。

入侵检测可被定义为对计算机和网络资源的恶意使用行为进行识别和响应的处理过程。它不仅检测来自外部的入侵行为，同时也检测内部用户的未授权活动，还能发现合法用户滥用特权，提供追究入侵者法律责任的有效证据。该技术通过分析入侵过程的特征、条件、排列以及事件间的关系，具体描述入侵行为的迹象。这些迹象不仅对分析已经发生的入侵行为有帮助，而且对将来可能发生的入侵也有警戒作用。

5. 反病毒技术

计算机病毒数据将导致计算机系统瘫痪，程序和数据遭受严重破坏，使网络的效率和作用大大降低，许多功能无法使用或不敢使用。反病毒技术大体分为病毒检测、病毒清除、病毒免疫和病毒预防等。

对计算机病毒应以预防为主，研制出高品质预防技术，才是上策。良好的管理和安全措施，可以大大减少病毒攻击的危险，并有效地防御大多数病毒。

6. 安全审计技术

安全审计是一个安全的网络必须支持的功能特性，审计是记录用户使用计算机网络系统进行所有活动的过程，它是提高安全性的重要工具。它不仅能够识别是谁访问了系统，还能指出系统正被怎样地使用。

在确定是否发生网络攻击这一点上，审计信息对于确定问题和攻击源十分重要。同时，系统事件的记录能够更迅速、更系统地识别问题，并且它是下一阶段事故处理的重要依据，为网络犯罪行为及泄密行为提供取证基础。另外，通过对安全事件的不断收集与积累并且加以分析，有选择性地对其中的某些站点或用户进行审计跟踪，以便对已经发生或可能产生的破坏性行为提供有力的证据。

具体而言，网络的审计系统应该由 3 个层次组成，具体如下。

①网络层的安全审计：主要利用防火墙的审计功能、网络监控与入侵检测系统来实现。

②系统的安全审计：主要利用各种操作系统和应用软件系统的审计功能实现，包括用户访问时间、操作记录、系统运行信息、资源占用等。

③对信息内容的安全审计，属高层审计。

各层次的安全审计措施是网络安全系统的重要组成部分，而对审计数据的维护是其重

要内容之一。

1.4.2　交易安全

交易安全是针对传统商务在互联网上运用时产生的各种安全问题而设计的一套安全技术。目的是在计算机网络安全的基础上确保电子商务过程的顺利进行，即实现电子商务的机密性、完整性、可靠性、匿名性、有效性和防抵赖性等。

加密技术层、安全认证层和交易协议层一起构成电子商务交易安全。交易协议层是加密技术层和安全认证层的安全控制技术的综合运用与完善。

1. 加密技术层

加密技术是电子商务最基本的安全措施。在目前技术条件下，加密技术通常分为对称加密和非对称加密两类。

(1)对称密钥加密

对称加密采用相同的加密算法，并只交换共享的专用密钥(加密和解密都使用相同的密钥)。如果进行通信的交易各方能够确保专用密钥在密钥交换阶段不发生泄露，可以通过对称加密方法对信息进行加密，并随加密信息发送报文摘要，以保证保密性和完整性。在对称密钥加密中，密钥安全交换是关系到对称加密有效性的重要环节。目前常用的对称加密算法有 DES、AES 和 3DES 等。

(2)非对称密钥加密

不同于对称加密，非对称加密的密钥被分解为公开密钥和私有密钥。公开密钥和私有密钥构成一个密钥对，密钥对生成后，公开密钥以非保密方式对外公开，私有密钥则保存在密钥发布者手里。任何得到公开密钥的用户都可以使用该密钥加密信息发送给该公开密钥的发布者，而发布者得到加密信息后，使用与公开密钥相对应的私有密钥进行解密。目前常用的非对称加密算法有 RSA 和 ECC 等。

在对称和非对称两类加密方法中，对称加密的特点是加密速度快(通常比非对称加密快 10 倍以上)、效率高，被广泛应用于大信息量的加密。但该方法的致命缺点是密钥的传输与交换面临着安全威胁，密钥易被截获。而且，若和大量用户通信，难以安全管理大量的密钥，因此大范围应用存在一定问题。而非对称密钥则相反，它能很好地解决对称加密中由于密钥数量过多导致管理难及费用高等问题，无须担心传输中的私有密钥的泄露，保密性能优于对称加密技术。但由于非对称加密算法复杂，加密速度难以达到理想状态。因此，目前电子商务实际运用中常常是两者结合使用。

2. 安全认证层

仅有加密技术层提供的加密技术不足以保证电子商务中的交易安全，身份认证技术是保证电子商务安全的又一重要技术手段。认证的实现包括数字签名技术和数字证书技术等。

(1)报文摘要

通过使用单向哈希函数将需要加密的明文“摘要”成一个固定长度(如 128 bit)的密文。

不同的明文加密成不同的密文，对明文的微小改动都会造成报文摘要的完全不同；相同的明文其报文摘要必然相同。因此，利用报文摘要就可以验证通过网络传输收到的明文是否是初始的、未被篡改过的，从而保证数据的完整性。

(2)数字签名

数字签名是非对称加密技术的一种特定应用。其主要方式为：报文发送方从报文文本中生成一个报文摘要，并用自己的私有密钥对这个报文摘要进行加密，形成发送方的数字签名；然后，这个数字签名将作为报文的附件和报文一起发送给报文的接收方；报文接收方首先从接收到的原始报文中计算出报文摘要，接着再用发送方的公开密钥来对报文附加的数字签名进行解密得到报文摘要。如果这两个报文摘要相同，那么接收方就能确认该数字签名是发送方的。利用数字签名技术，接收者可以确定发送者的身份是否真实，同时发送者不能否认发送的消息，接收者也不能篡改接收的消息。

(3)数字证书

数字证书用电子手段来标识一个用户的身份。数字证书的内部格式是由 ITU－T X.509国际标准所规定的，包含证书拥有者的姓名、证书拥有者的公共密钥、公共密钥的有效期、颁发数字证书的单位、数字证书的序列号。数字证书的使用涉及数字认证中心。

目前，数字证书有个人证书、企业证书和软件证书，其中前两类较为常用。个人证书仅仅为某单个用户提供凭证，用以帮助其个人在网上进行安全交易操作。企业证书通常为网上的某个 Web 服务器提供凭证，拥有 Web 服务器的企业就可以用具有凭证的互联网站点(Web Site)来进行安全电子交易。

(4)认证中心

在电子商务系统中数字证书的发放需要有一个具有权威性和公正性的第三方认证机构来承担。认证中心(CA)正是这样的一个受信任的第三方。CA 为用户签发数字证书，提供身份认证服务，是整个系统的安全核心。

在非对称密钥认证系统中，用户的公钥和私钥通常是分开的，而 CA 只知道用户的公钥，这样就避免了可信第三方被攻击而导致整个系统陷入瘫痪的严重问题。此外，在认证系统中，CA 只负责审核用户的真实身份并对此提供证明，而不介入具体的认证过程，从而缓解了可信第三方的系统瓶颈问题。而且 CA 只需管理每个用户的一个公开密钥，大大降低了密钥管理的复杂性。这些优点使得非对称密钥认证系统适用于用户众多的大规模网络系统。

3.交易协议层

除加密技术层和安全认证层提到的各种安全控制技术之外，电子商务的运行需要一套完整的安全交易协议。目前，比较成熟的协议有 SSL 和 SET 等协议。

(1)安全套接层 SSL 协议

安全套接层(Secure Sockets Layer，SSL)协议是网景(Netscape)公司于 1996 年推出的安全协议。它位于运输层和应用层之间，由 SSL 记录协议(SSL Record Protocol)、SSL 握

手协议(SSL Handshake Protocol)、修改加密约定协议(Change Cipher Spec Protocol)和报警协议(Alter Protocol)组成。

在互联网中由于TCP/IP本身非常简单,没有加密、身份认证等安全特性,从而对通过互联网进行的商务活动带来了很大的安全隐患,因此要向上层应用提供安全通信的机制就必须在TCP之上建立一个安全通信层次。在此方面,网景公司开发了可以在互联网客户与服务之间数据传送进行加密和鉴别的SSL协议。

SSL握手协议被用来在客户与服务器传输应用层数据之前建立安全机制。当客户与服务器第一次通信时,双方通过握手协议在版本号、密钥交换算法、数据加密算法和哈希算法上达成一致,然后互相验证对方身份,最后使用协商好的密钥交换算法产生一个只有双方知道的秘密信息,客户和服务器各自根据此秘密信息产生数据加密算法和哈希算法参数。

SSL记录协议根据SSL握手协议协商的参数,对应用层送来的数据进行压缩、加密,计算报文验证码(Message Authentication Code,MAC),然后经网络传输层发送给对方。修改加密约定协议由单个报文组成。该报文由值为1的单个字节组成,由客户机或服务器发出,用以通知接收方接下来的记录将受到刚达成的密码参数和密钥的保护。报警协议用来在客户和服务器之间传递SSL出错信息。

(2)安全电子交易SET协议

安全电子交易协议(Secure Electronic Transaction,SET)是由VISA和Master Card两大信用卡组织制订的标准。SET用于划分与界定电子商务活动中消费者、网上商家、银行、信用卡组织之间的权利义务关系,给定交易信息传送流程标准。SET主要由3个文件组成,分别是SET业务描述、SET程序员指南和SET协议描述。SET协议保证了电子商务系统的保密性、完整性、不可否认性和身份的合法性。

案例:百度被劫持事件

1.案例背景

目前,百度是全球最大的中文搜索引擎,2000年1月创立于北京中关村。百度的使命是让人们最便捷地获取信息,找到所求。百度的核心价值观是“简单可依赖”。

在面对用户的搜索产品不断丰富的同时,服务于生机勃勃的企业的搜索推广应运而生。多年来,通过搜索推广,极大地促进了中国数十万中小企业的生存与发展。搜索推广,以及基于搜索推广的百度推广也得到迅速发展。以全球以及中国500强为主的大型企业,在百度搜索平台上开展以搜索推广为基础的品牌推广,为企业的品牌、产品推广创造了不同凡响的收益。同时,百度近年来响应网民的诉求,进入C2C电子商务领域,为网民提供更多更好的一站式服务。

为推动中国数百万中小网站的发展,百度借助超大流量的平台优势,联合所有优质的各类网站,建立了世界上最大的网络联盟,使各类企业的搜索推广、品牌营销的价值、覆盖面均大面积提升。与此同时,各网站也在联盟大家庭的互助下,获得最大的生存与发展机会。

2005年8月5日，百度在美国纳斯达克上市（股票代码：BIDU），其上市当日，即成为该年度全球资本市场上最为耀眼的新星，通过数年来的市场表现，其优异的业绩与值得依赖的回报，使之成为中国企业价值的代表，傲然屹立于全球资本市场。2011年3月24日百度市值收盘报460.72亿美元，超过腾讯（00700.HK）23日收盘时约445亿美元。五年来，中国互联网企业市值第一的头衔首次易主。

2.案例简介

2010年1月12日上午6点左右起，全球最大中文搜索引擎百度突然出现大规模无法访问，主要表现为跳转到雅虎出错页面，显示伊朗网军图片，出现“天外符号”等，范围涉及四川、福建、江苏、吉林、浙江、北京、广东等国内绝大部分省市。

这次百度大面积故障长达5个小时，也是百度2006年9月来最大最严重的断网事故，在国内外互联网界造成了重大影响，百度蒙受的经济损失超过700万元。更为重要的是，百度安全性的脆弱表现对其品牌的负面影响很大。

据中国电子商务研究中心跟踪分析，其大致攻击过程解剖如下。

①2010年1月12日上午约6点起，百度域名DNS服务器被劫持更换，同时主域名已经被解析到一个荷兰的IP。

②域名被更换后，访问百度时页面自动跳转到租用的雅虎服务器的空间；该IP的网站实际使用英文Yahoo下的租用空间，因此访问百度旗下网站时，会出现英文Yahoo的出错信息页面。

③由于页面请求数量过于庞大导致雅虎服务器瘫痪或者流量超限，服务器瘫痪。

④服务器瘫痪后，访问百度的网民页面自动跳转到雅虎的提示页面。

⑤在超限之前，部分网页显示伊朗网军的黑客页面，攻击者在百度首页自称是“Iranian Cyber Army”的组织承认篡改了百度主页，并留下阿拉伯文字。

⑥2010年1月12日上午，国内大部分城市用户和海外用户只能通过未被劫持的备用域名http://www.baidu.com.cn访问。

⑦2010年1月12日上午近10点，百度相关人士出面表示，故障“还在查，目前原因不知”，此前均表示不知情或拒接电话。

⑧2010年1月12日上午约11点起，部分地区陆续恢复正常访问。

⑨下午起，百度正在陆续恢复域名解析，出现了各地逐渐恢复访问的情况。

⑩根据解析速度，如不出意外，全世界将在48小时内全部恢复访问。

3.案例分析

（1）对百度自身影响分析

“全球最大中文搜索网站”技术形象有损，该事件或将引发进一步的攻击。百度作为中国代表性的互联网企业，却遭受多次被黑事件，且这次故障恢复时间长达5小时，折射出百度对安全技术投入和应急准备明显不足。

而包括国外网络军队在内的各种黑客看到百度是如此的脆弱，可能会发起对国内网络

更大规模的攻击，百度搜索引擎的行业地位进一步显现。

(2)对其他搜索引擎影响分析

百度无法访问后，谷歌、爱问、有道、搜搜、中国雅虎等其他搜索引擎访问量都出现激增情况，而且“百度”成为谷歌今日上升最快关键词。“此消彼长”，这也从另一面说明搜索市场整体竞争激烈。

另据权威“搜索榜”(top.toocle.com)数据监测显示，2010年1月11日各主流搜索引擎份额分别为，百度占55.65%，谷歌占17.93%，搜狗、搜搜、微软Bing和有道分别占7.72%、7.61%、7%和4.08%。对此，我们预计1月12日“搜索榜”份额甚至排名将出现重大变化，谷歌等其他搜索引擎的访问量与份额比例有望明显上升。

(3)对门户网站影响分析

调查显示：目前搜索引擎给门户网站带来的流量占到20%左右，部分甚至占到40%，而其中百度带来的流量要占70%，Google大于20%。

百度无法访问后，四大门户、各大行业网站等均遭受不同程度的损失，流量受到一定影响，由于百度访问障碍时间较长，从第二天的Alexa排名来看，国内门户网站将普遍略有所下降。

在此次百度被黑事件里，四大门户中流量较大的腾讯、新浪受到影响较少，预计流量将下降大约在5%左右，而搜狐和网易受到的影响可能会稍大些，预计流量将会下降10%左右。

(4)中小网站影响分析

中小网站由于搜索引擎依赖度较高，遭受的直接影响最大，如音乐类搜索方面，主要集中于百度(百度MP3)、搜狗、中搜等多家综合搜索引擎带来的下载量，而百度就占到80%左右。此外，这次百度被黑事件将明显对数百万中小网站造成心理上的负面影响。

(5)对网民影响分析

百度等知名互联网企业遭受域名劫持，使得普通用户上网安全更难保障，黑客极容易将木马等恶意程序植入。但同时，该事件对网民上网安全意识与防范意识起到了警示作用。

(6)对客户影响分析

百度尽管用“凤巢”替代竞价排名，但其商业模式还是点击产生付费，在这次长达5小时的被黑事件中，将会对数十万的百度企业客户造成心理上的负面影响，若在线模式被黑客入侵，将会遭受惨重的损失，甚至在被黑客连续的攻击下无法持续经营，破产关门。

(7)对互联网业界影响分析

①DNS根服务器设置：因为DNS服务是互联网的基础服务，不是个人或者小公司负责的业务，所以DNS被劫持再次说明国内的基础服务安全防范意识不高。除了日常做好服务器基础安全漏洞的跟进和修复外，更需提高互联网安全意识。

②网络安全警钟：从现象上看，这次百度被黑baidu.com这个域名在根域解析上被黑客控制(这个域名是美国管理的)，不只是国内的互联网厂商需要增强防范意识，而是整个国际

互联网社会同样面临着网络安全威胁。

③域名争论：百度域名遭篡改本质原因在于域名注册商系统存在漏洞，域名注册商是美国的 REGISTER.COM。律师于国富认为，百度应该起诉位于美国的国际域名管理机构。此前，另一家互联网巨头 QQ 已经将域名从国外转移到国内。这次被攻击事故发生后，百度方面是否会立即采取转移行动也成了业界关注的焦点。

本章习题

(1)简述电子商务的安全特性。
(2)简述客户机的安全问题。
(3)简述通信信道的安全问题。
(4)简述服务器的安全问题。
(5)简述电子商务的安全需求。
(6)简述电子商务的安全体系结构。
(7)简述网络安全技术。