高等学校电子商务系列教材

电子商务安全与保密

祁 明 主编

高等教育出版社

高等学校电子商务系列教材

电子商务安全与保密

祁　明　主编
张　凌　宋全芳　曹妮妮　编著

高等教育出版社

内容摘要

本书较系统地介绍了电子商务安全保密的基本理论和实用技术，既简明扼要地介绍了国内外的前沿研究成果，又详细介绍了电子商务中迫切需要的安全保密知识。本书共18章，涉及的范围比较广泛，其主要内容有：电子商务安全的现状与趋势、信息加密技术、数字签名技术、身份认证与访问控制、密钥管理与数字证书、WWW安全、防火墙、计算机病毒的防治、安全协议、系统入侵检测、信息隐藏与数字水印、电子邮件安全、移动通信安全、反计算机犯罪、计算机软件保护、系统与产品评估和系统安全保护制度的建立。

本书可作为高等院校计算机、通信、经济信息管理及相关专业本科生或研究生的电子商务教材，也可供从事电子商务研究和应用开发人员学习参考。

图书在版编目(CIP)数据

电子商务安全与保密/祁明主编. —北京：高等教育出版社，2001.7
ISBN 7-04-009279-4

Ⅰ.电… Ⅱ.祁… Ⅲ.①电子商务—安全技术 ②电子商务—保密 Ⅳ.F713.36

中国版本图书馆CIP数据核字(2001)第26164号

责任编辑 董建波 **封面设计** 王凌波 **责任印制** 杨 明

电子商务安全与保密
祁 明 主编

出版发行	高等教育出版社		
社 址	北京市东城区沙滩后街55号	**邮政编码**	100009
电 话	010-64054588	**传 真**	010-64014048
网 址	http://www.hep.edu.cn http://www.hep.com.cn		
经 销	新华书店北京发行所		
印 刷	中国农业出版社印刷厂		
开 本	787×1092 1/16	**版 次**	2001年7月第1版
印 张	28.25	**印 次**	2001年7月第1次印刷
字 数	690 000	**定 价**	28.00元

本书如有缺页、倒页、脱页等质量问题，请到所购图书销售部门联系调换。

前　言

自有计算机网络以来，网络的安全就成为网络使用者不得不面对的问题。如今，随着网络应用水平的提高和电子商务的大力开展，计算机系统的安全隐患也日渐突出，由此带来的诸如高科技犯罪、机密泄露、黑客入侵、病毒侵扰等问题，其危害之严重、手段之高超，令人惊异。

据美国 FBI 的调查，美国每年因为网络安全造成的经济损失超过 170 亿美元，大约 75% 的公司财政损失是由于计算机系统的安全问题造成的，但其中只有 17% 的公司愿意报告遭受过黑客的袭击，而大部分公司由于担心负面影响而不愿声张。

中国的网络安全和电子商务安全情况并不乐观。最近，国内有关专家曾对国内多家网站的安全性做了测试，结果令人震惊——在测试的网站中有近 90% 的网站存在着不同程度的安全隐患。遭到黑客及击的网站有很多，如，新浪网、中国公众多媒体信息网、国家统计局网站等。总之，互连网与电子商务的安全问题已经引起了人们的恐慌，各国政府、IT 厂商和业界同仁在感到震惊的同时，也开始积极思考对策和提供针对不同需求的解决方案。

为了普及计算机网络和电子商务的安全保密技术，推进我国信息安全产业的发展，增进与国内外同行之间的交流，我们编著了这本教材。

本书第 1～18 章由华南理工大学祁明博士编写并担任主编，华南理工大学张凌教授和广东省保密局宋全芳研究员参与了系统安全管理和安全产品介绍等章节部分内容的编写，华南理工大学图书馆曹妮妮女士提供并翻译了许多有参考价值的外文资料，华南理工大学计算机系的研究生林卓声、许伯桐、刘迎风等人参与了本教材书稿的校对和其他文字处理工作。

在写作过程中，作者试图从理论和实践相结合的角度较系统地介绍电子商务安全保密的基本理论和实用技术。既介绍国内外的前沿研究成果，又介绍目前已经实用的具体技术；既注重介绍安全保密的基本概念和算法，又照顾到学习电子商务课程学生其来源的广泛性、知识背景的多样性和要求的多层次性。尽管作者有以上初衷，但因学术水平有限和篇幅所限，许多与电子商务有关的安全保密技术未能介绍或介绍的不够全面。另外，本书编写虽力求完美，然而谬误之处在所难免，对此，作者恳请读者的理解和批评指正。

本书是作者在华南理工大学计算机工程与科学系以及电子商务学院多年教学和研究的基础上写成的。作者在写作过程中参阅了大量的国内外资料。再此，谨向书中提到和参考文献列出的所有作者表示衷心的感谢。本书的编写和有关研究工作还分别得到了 IBM 中国有限公司大学合作部和广东省自然科学基金的资助，也得到了高等教育出版社的热情支持，在此一并表示感谢！

编者

2001 年 6 月于广州

徐如人教授，无机化学家，1991年当选为中国科学院院士。1932年2月生于浙江上虞县。1952年毕业于上海交通大学，任教于吉林大学化学系，历任教授、化学系主任、合成与催化研究所所长。长期从事无机合成化学、分子筛化学与分子工程学领域的研究与教学。现任《高等学校化学学报(中英文版)》、《无机化学学报》、《应用化学》副主编以及第三届国家自然科学基金委员会委员；《J.Materials Chem.》、《Microporous Materials》、《Catalysis Letters》、《Topics in Catalysis》、《Inorg. Chem. Commun.》与《Microporous and Mesoporous Materials》等国际性专业杂志的顾问编委。1998年当选为国际分子筛协会(IZA)执行理事

目　录

第一章　电子商务安全的现状与趋势

电子商务已成为业界的新热点，但我国现有的电子商务系统只是在一般 Web 站点的基础上增加了简单的产品目录和订购单。这种比较初级的电子商务系统因还没有与内部网连接，也就没有涉及太多的安全问题。然而，随着信息化进程的深入，它们即将被新的、真正的电子商务系统所取代：即 Web 站点与公司的后端数据库系统相连接，这样就可以向客户提供有关产品的库存、发货情况以及账款状况的实时信息。这种充分集成的 e－business 系统可以向客户提供只能通过 Web 才能得到的重要服务，同时还可以帮助商家实现业务处理的流水化。这种新的完整的电子商务系统可以将内部网与 Internet 连接，使小到本企业的商业机密、商务活动的正常运转，大至国家的政治、经济机密都将面临网上黑客与病毒袭击的严峻考验。这样，安全问题便成了电子商务系统的首要问题。

目前，Internet 上影响交易最大的阻力是交易安全，使用者担心在网络上传输的信用卡及个人资料信息被截取，或是不幸遇到“黑店”，信用卡资料被不正当运用。另一方面，特约商店也担心收到的是被盗用的信用卡号码，或是交易不认账等等，还有可能因网络不稳定或是应用软件设计不良导致被黑客侵入所引发的损失。由于在消费者，特约商店，甚至于金融单位之间，权责关系还未理清，以及每一家电子商场或商店的支付系统所使用的安全控管机制都不尽相同，都造成使用者有无所适从的感觉。以上种种，令不少有兴趣的 Internet 网上购物者因担忧而犹豫不前。因此，电子商务顺利开展的核心和关键问题是保证交易的安全性，这是网上交易的基础，也是电子商务技术的难点所在。

本章着重介绍电子商务系统安全的基本概念，安全性的基本要求，电子商务安全技术的发展状况和实际应用。

1.1　电子商务安全概述

1.1.1　电子商务安全结构与要求

1. 安全性定义

在给安全性下更详细的定义时，通常需要先定义一系列新的术语。为了理解本章所述各种安全性的含意，有必要先了解以下术语：

(1) 密码安全——通信安全的最核心部分，由技术上提供强韧的密码系统及其正确应用来实现。

(2) 计算机安全——一种确定的状态，使计算机化数据和程序文件不致被非授权人员、计算机或其程序访问、获取或修改。安全的实施可通过限制被授权人员使用计算机系统的物理范围、利用特殊(专用)软件和将安全功能构造于计算机操作规程中等方法来实现。

(3) 网络安全——包括所有保护网络的措施:物理设施的保护、软件及职员的安全,以防止非授权的访问、偶发或蓄意的常规手段的干扰或破坏。因此,有效的安全措施是技术与人事管理的一种均衡或合理配合。

(4) 信息安全——保护信息财富,使之免遭偶发的或有意的非授权泄露、修改、破坏或处理能力的丧失。

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:

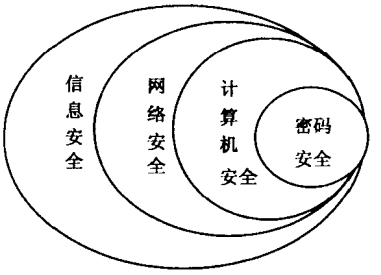

图 1.1　安全环

2. 电子商务安全的基本要求

表 1.1 列出了电子商务所需的 7 种安全性要求。其中保密性、完整性和不可否认性最为关键。

表 1.1　网络安全性要求

术语	定义
保密性	保持个人的、专用的和高度敏感数据的机密
认证性	确认通信双方的合法身份
完整性	保证所有存储和管理的信息不被篡改
可访问性	保证系统、数据和服务能由合法的人员访问
防御性	能够阻挡不希望的信息或黑客
不可否认性	防止通信或交易双方对已进行业务的否认
合法性	保证各方的业务符合可适用的法律和法规

1.1.2　电子商务安全现状

2000 年 2 月 7 日、8 日、9 日这三天,美国许多著名的网站先后遭到互联网历史上最严重的计算机黑客攻击,在美国社会引起了强烈震动。

黑客 3 天来的袭击,造成的间接和直接经济损失达 10 亿美元。2 月 7 日,除了免费电子邮件等三个站点未受影响外,雅虎的大部分网络服务陷于瘫痪。雅虎是全球第二大搜索引擎网站,每天被浏览页次达 4.65 亿次,其股市价值达 930 亿美元。8 日上午,先是当天股市的网络销售公司购买网站死机,再是网上电子拍卖网站电子港湾、网上书店及商品销售的亚马逊网站告急。电子港湾的注册用户达 1 000 万,是每月浏览达 15 亿次的网上拍卖网站,8 日下午 6 时,商品买卖一度被停止数小时。当晚,美国有线电视新闻网宣布,其网站因负荷超载,从下午 7 时至 8 时 45 分信息传送被阻断。2 月 9 日,电子商务网站再度遭殃,电子交易网站在股市开市前遭到持续 1 小时的攻击;信息技术公司的科技新闻网站 ZDNet 约有 70% 的内容被中断 2 小时,上网者无法接触到包括网站新闻和产品浏览等内容的信息。

美国联邦计算机案件处理中心主任大卫加诺说:"全美至少有数百台计算机受到袭击。所幸

的是,黑客并未进入这些网络内部,窃取业务和客户资料。如此众多的大型网站,特别是新兴的电子商务网站,在3天的短时间内连续遭到黑客攻击,这在因特网历史上还是第一次。"有关专家称,此事将进一步引起人们对网络安全和电子商务风险的关注。

近年来,网络技术和电子商务迅猛发展,人们在网络上进行从购买书、日用品到计算机、房产交易以及股票炒作、资金运作等活动剧增,网络安全问题成为人们一直关注的话题。电子安全的重要性已不言而喻。安全问题是电子商务推进中的最大路障。营造信誉良好、安全可靠的交易环境才能让众多的企业和消费者支持电子商务,否则消费者不信任网上交易,企业没有把握在网上营销,电子商务便只能是"水中花、镜中月"。尽管政府以及一些企业已意识到这一问题,但因为一直缺乏一个安全保护的完整概念,所以很多人在安全认知上仅限于对防火墙的了解,而防火墙只是安全保护的一个方面,绝不等于全部,这也正是实施了防火墙的网络仍有漏洞的原因所在。

为了对电子商务的安全问题有更感性的认识,我们可以分析一下黑客盗取信用卡的过程。黑客在互联网的新闻组上发布带有后门病毒的程序,并鼓励人们下载到自己的PC机上,一旦某台PC机下载了此程序,那么他就成为黑客可以侵略的对象。黑客可以浏览被入侵者PC机上的全部信息资源,可以实时地掌握被入侵者的桌面使用情况。如果被入侵者此时输入信用卡号,那么黑客就可以易如反掌地窃取到这一代码,这是信用卡被盗用的主要原因。即使你不曾在公共信息场所下载软件,你也很有可能成为无辜的受害者,因为黑客程序中的后门病毒具有很强的蔓延性,即一台PC机被感染后,病毒可通过此PC机上的地址簿向所有这些地址的PC机传播,然后按同样的方法再进一步把态势扩大。这些几何级的增长使病毒的蔓延速度极快,覆盖范围极广。所以,不经意间或许你的PC机就已成为黑客的盘中餐,而一个网上交易的网站一旦发生消费者信用卡泄露事件,那么将不会再有人去访问这个站点。因此,要使电子商务能健康、蓬勃地发展,就必须用全面的电子商务安全解决方案提供交易的信任保障。

电子商务站点上的安全漏洞会造成网上交易用户的账号、交易密码泄露,恶意攻击者可以使他人资金泄露,甚至可以使用他人资金进行网上交易。中国互联网中心于2000年2月18日发布的《中国互联网络发展状况统计报告》中关于电子商务的调查表明,安全可靠性是52.26%的电子商务用户最关心的问题。安全漏洞的存在,直接影响国内电子商务站点的信誉程度。网上交易安全性若不能得到保证,就必将影响国内电子商务的顺利发展。

电子商务的安全问题是一个涉及范围极广的社会问题,希望有越来越多的企业和个人加入到关心电子商务的行列中来,一起为开创崭新商务时代出力献策!

1.1.3 网络安全十大不稳定因素

1. Cookie:这种"网络小甜饼"是一些会自动运行的小程序。网络设计师使用它们来提供方便而高效的服务。但同时通过使用这些小程序,商业公司和网络入侵者能够轻易获得他人机器上的信息。

2. Java:Java作为一种技术,到底是否成功,一直备受争议。但至少有一点是肯定的,有很多利用Java的漏洞成功入侵提供网络服务的服务器的案例。

3. CGI:很难想像没有CGI技术,网站会是什么样子。可能会很难看,可能使用会不太方便,但人们留在服务器上的隐私会得到更大的保障。

4. 电子邮件病毒:超过85%的人使用互联网是为了收发电子邮件,没有人统计其中有多少人正使用直接打开附件的邮件阅读软件。“爱虫”发作时,全世界有数不清的人惶恐地发现,自己存放在电脑上的重要文件、不重要的文件以及其他所有文件,已经被删得干干净净。

5. 认证和授权:每当有窗口弹出,问使用者是不是使用本网站的某某认证时,绝大多数人会毫不犹豫地按下“Yes”,但如果商店的售货员问:“把钱包给我,请相信我会取出合适数量的钱付款,您说好吗?”你一定会斩钉截铁地回答:“No!”这两种情况本质上没有什么不同。

6. 微软:微软的软件产品越做越大,发现漏洞之后用来堵住漏洞的补丁也越做越大,但是又有多少普通用户真正会去下载它们?

7. 比尔盖茨:很多技术高手就是因为看不惯他,专门写病毒让微软程序出问题,攻击使用微软技术的站点。但盖茨没有受到太大影响,遭罪的是普通人。

8. 自由软件:有了自由软件,才有互联网今天的繁荣。自由软件要求所有结果必须公开,据说让全世界的程序员一起来查找漏洞,效率会很高。这要求网络管理员有足够的责任心和技术能力根据最新的修补方法消除漏洞。不幸的是,跟薪水和股权相比,责任心和技术能力显得没有那么重要。

9. ICP:人们提供私人信息,ICP让其注册,并提供免费服务,获得巨大的注意力,以及注意力带来的风险投资。这是标准的注意力经济模式。但并没有太多人去留意有很多经济状况不太好的ICP把用户的信息卖掉,换钱去了。

10. 网络管理员:管理员可以得到人们的个人资料、看他们的信、知道他们的信用卡号码,如果做些手脚的话,还能通过网络控制他们的机器。人们只能期望这些人技术高超、道德高尚。

早些时候,电子商务网站eBay、Amazon.com和Buy.com、门户网站Yahoo!、新闻网站CNN.com等著名站点均遭到黑客攻击。联邦调查局也成为了一个类似攻击的目标,该局的网站在2000年2月18日被关闭了3个多小时,当时黑客向该网站发送了大量虚假信号使其被堵塞。

研究和教育机构SANS(系统管理、连网及安全学会)目前公布,Internet存在十大安全威胁。威胁名单包括那些最经常地被用来入侵计算机网络的软件弱点。SANS学会公布这一名单旨在帮助系统管理员识别那些应当被立即清除的弱点,以挫败黑客的攻击行动。

列于名单榜首的是一些针对目录服务——明确地说就是伯克利Internet名称域(BIND)的攻击活动。这个学会说,在那些使用最广泛的域名服务工具中,BIND可以让人们通过名称找到系统的位置,而不必知道具体的IP地址。

排名第二的是公用网关接口(CGI)程序,即一项确定在网页上运行外部程序规则的标准。许多Web服务器带有一些缺省安装的CGI程序,使它们很容易遭到黑客的攻击。

名列第三的是针对网络系统上的共享文件的入侵行动。众所周知,黑客们一直利用一项叫做“远程过程调用(RPC)”的功能,此项功能可以让一台计算上的程序与另一台计算机上的程序“交谈”。

这份报告也提到了文件共享程序、通用电子邮件程序和用户ID或口令访问中的Internet安全缺陷。该报告说,一些管理员要么忘记了一个默认口令,要么没有时间修改安装在系统上的默认口令。大多数“Demo”或“Guest”口令广为人知,使得这一弱点可能成为黑客攻击一个计算机系统的最容易的方法。

SANS学会的研究主任Alan Paller说,这份十大安全威胁名单是全国各地的代表一致得

出的结果，这些代表包括联邦调查局、国家安全局、设在大学的技术研究部门和 CERT 协调中心。

1.1.4 触发电子商务安全问题的原因

日益严重的网络信息安全问题，不仅使上网企业、机构及用户蒙受了巨大经济损失，而且使国家的安全与主权面临严重威胁。要避免网络信息安全问题，首先必须搞清楚触发这一问题的原因。归纳起来，主要有以下几个方面。

(1) 黑客的攻击。由于缺乏针对网络犯罪卓有成效的反击和跟踪手段，因此黑客的攻击不仅"杀伤力"强，而且隐蔽性好。目前，世界上有 20 多万个黑客网站，其攻击方法达几千种之多。

(2) 管理的欠缺。网站或系统的严格管理是企业、机构及用户免受攻击的重要措施。事实上，很多企业、机构及用户的网站或系统都疏于这方面的管理。据 IT 界企业团体 ITAA 的调查显示，美国 90% 的 IT 企业对黑客攻击准备不足。目前，美国 75%～85% 的网站都抵挡不住黑客的攻击，约有 75% 的企业网上信息失窃，其中 25% 的企业损失在 25 万美元以上。

(3) 网络的缺陷。因特网的共享性和开放性使网上信息安全存在先天不足，因为因特网最初的设计考虑是该网不会因局部故障而影响信息的传输，但它仅是信息高速公路的雏形，在安全可靠、服务质量、带宽和方便性等方面存在着不适应性。

(4) 软件的漏洞或"后门"。1999 年底保加利亚软件测试专家发现微软网络浏览器 IE 存在安全漏洞，它可以使不怀好意的网站管理人员入侵访问者的计算机文件，随后微软公司承认这一事实。

(5) 人为的触发。基于信息战和对他国监控的考虑，个别国家或组织有意识触发网络信息安全问题。

1.1.5 安全问题制约电子商务的发展

网络这个给人们带来种种实惠的事物，怎么这么脆弱？其实，有矛才有盾，所谓"魔高一尺，道高一丈"。在已具备一定技术条件的情况下，就应该联合起来建立中国网络防御长城。

2000 年 5 月 4 日，菲律宾一名电脑高手制造出一种称为"爱虫"的电脑病毒，短短四五天内侵袭了全世界 100 多万台计算机，造成数十亿美元的损失。"CIH"、"梅利莎"、"爱虫"等电脑病毒不断兴风作浪，一次又一次敲响了信息安全的警钟。

一台计算机、一条电话线、一个 Modem 就能发动全球信息战。随着新经济时代的来临，网络中无所不包的信息资源，方便的查询和通信方式使网络用户呈几何级数增长，新的挑战——电子攻击也随之而生。

据美国联邦调查局的调查，美国每年因为网络安全造成的经济损失超过 170 亿美元。2001 年 2 月，黑客大肆攻击雅虎、EBAY 等著名商业网站及其他各类站点，造成了直接经济损失 12 亿美元，并引起股市动荡。早在 1997 年，美国就出现了两次大的互联网络瘫痪事件，使人们感受到信息战争的巨大威胁。著名的美国联机公司因人为操作的技术上失误，使其 600 万用户陷入瘫痪 10 小时。

863 安全责任专家、上海格尔软件公司总经理吴田平博士说，从军事意义上看，信息是最精确的制导武器。它可以直接瞄准军事系统的首脑机关。除了特殊用途，军用装备采用很多民用