普通高等教育“十一五”国家级规划教材

高等学校计算机科学与技术教材

- 原理与技术的完美结合
- 教学与科研的最新成果
- 语言精炼，实例丰富
- 可操作性强，实用性突出

电子商务安全

□ 祝凌曦 主编
□ 刘 军 主审

清华大学出版社 ● 北京交通大学出版社

普通高等教育“十一五”国家级规划教材
高等学校计算机科学与技术教材

电子商务安全

祝凌曦　主编
刘　军　主审

清华大学出版社
北京交通大学出版社
·北京·

内 容 简 介

电子商务系统是一个涉及多方面的复杂的大系统，本书主要从技术的角度出发，讲述在电子商务系统中涉及电子商务交易部分的安全理论、方法和技术。

本书主要内容包括电子商务安全的现状、电子商务安全的体系结构、密码学基础、公钥基础设施 PKI、PKI 的体系与功能、认证机构 CA、数字签名、安全电子交易协议 SET、安全套接层协议 SSL、电子商务的主要支付机制、支付交易安全及电子商务的应用安全等。

本书具有较高的系统性、前沿性，内容丰富实用，讲解深入浅出，图文并茂，具有很好的可读性。

本书适合作为高等学校电子商务、信息管理、信息安全、网络安全及计算机技术等专业的教材，特别适合同时开设电子商务安全和计算机安全保密课程的教学使用，在编排上保证了两门课程的内容不会有重叠。同时，本书可以作为电子商务安全技术培训的教材，也适合从事电子商务系统分析与设计研究和开发的相关的工程技术人员作为参考书使用。

图书在版编目(CIP)数据

电子商务安全/祝凌曦主编. —北京：清华大学出版社；北京交通大学出版社，2006.11
（高等学校计算机科学与技术教材）
ISBN 7－81082－740－5

Ⅰ. 电… Ⅱ. 祝… 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（2006）第 040484 号

责任编辑：谭文芳　　特邀编辑：宋林静
出版发行：清 华 大 学 出 版 社　　邮编：100084　　电话：010－62776969
　　北京交通大学出版社　　邮编：100044　　电话：010－51686414
印 刷 者：北京东光印刷厂
经　　销：全国新华书店
开　　本：185×260　　印张：19.5　　字数：496 千字
版　　次：2006 年 11 月第 1 版　　2006 年 11 月第 1 次印刷
书　　号：ISBN 7－81082－740－5/F·158
印　　数：1～5000 册　　定价：28.00 元

序

近些年来，伴随着电子商务在我国的不断深入，电子商务人才的培养问题日益突出。2000年全国相关高校成立了电子商务高校协作组，2006年教育部成立了电子商务专业教学指导委员会，以加强这一新兴本科专业的建设。教材建设是本科专业建设中的重要内容，2006年教育部电子商务专业指导委员会亦将电子商务安全等课程作为该专业核心课程。

伴随电子商务的兴起，电子商务安全一直成为这一领域的热门方向。传统的交易依赖直接谋面的买卖双方独立判断对方的合法身份以建立信任关系。网络交易却因为买卖活动的时空分离而带来从网络数据到交易互信等一系列涉及交易安全的问题。因此，电子商务安全涉及面很广，不仅涉及交易安全，还涉及网络安全、信息安全等。在教学过程中这些内容却涉及若干课程，究竟如何安排是一个值得研讨的问题。由于知识的差异，因此电子商务安全方面教材的教学内容在安排上就有很大的不同。

祝凌曦同志从2003年起一直作为电子商务本科专业的一线教师，承担本科教学工作，对课程及教学过程有较深入的体会。本次出版的教材是在全国高校电子商务协作组拟定大纲的指导下，在三届本科生教学讲义的基础上编辑出版的，对本科教学很有针对性。这本教材从内容组织上将网络安全、计算机安全与电子商务安全进行了梳理，着重介绍有关交易过程安全涉及的内容，因而与其他前驱和后续课程的分工更加合理，在教学计划的安排上较合适。

希望这本教材的出版对电子商务专业的建设做出一定的贡献。

刘　军

2006.10.18

前　言

近年来，随着数字化、网络化技术的不断发展，社会信息化的程度越来越高，人类社会信息化的程度也越来越大。随着互联网在中国的日益普及，网络已经深入到人们生活的方方面面。现在，人们在网络上可以进行各种商务活动，大到企业和企业之间的商务合作、国际间的贸易发展，小到个人生活的各个方面，从房屋、汽车的购买，到音像制品、图书和日常用品的购买，都可以通过电子商务完成。

虽然电子商务的观念逐渐深入人心，但毕竟电子商务是在一个开放的、国际化的、社会化的虚拟网络环境中运行的，在其中难免会出现欺诈、泄密等现象。随着人们对电子商务应用的增多，有关黑客和安全问题也更多地被报道，安全问题已成为电子商务应用中一个主要的瓶颈。

要在开放的 Internet 平台上更好地进行电子商务交易，就必然要解决交易双方的身份确认、信息传输的完整性、保密性，以及交易操作的不可否认性等问题，解决这些问题需要密码学、身份认证、数字签名，以及建立在这些理论方法上的 PKI 系统、安全电子交易协议 SET、安全套接层协议 SSL 等多种技术、方法和协议的联合应用。

本书共 10 章。第 1 章为概述，主要讲述电子商务安全的现状、电子商务安全需求、电子商务安全体系结构及电子商务安全交易标准；第 2 章为密码学概述，主要讲述对称密码学、非对称密码学、哈希函数等密码学基础；第 3 章为公钥基础设施 PKI 导论，主要讲述 PKI 的概念、PKI 的定义和 PKI 的主要内容；第 4 章为 PKI 的体系与功能，主要讲述 PKI 体系结构及各实体功能、PKI 体系结构的组织方式、PKI 的功能操作、PKI 体系的互通性、PKI 的服务、X.509 标准、证书与认证过程；第 5 章为认证机构，主要讲述认证机构及其系统目标、认证机构的系统功能和系统结构。第 6 章为数字签名，主要讲述数字签名的基本原理、RSA 签名、ElGamal 签名、盲签名及其应用、多重签名及其应用、定向签名、代理签名、美国数字签名标准 DSS，以及数字签名应用系统与产品介绍；第 7 章为安全电子交易协议 SET，主要包括 SET 协议总述、SET 协议信息结构、SET 协议组成部分、SET 协议处理逻辑及 SET 协议分析；第 8 章为安全套接层协议 SSL，主要讲述 SSL 协议总述、SSL 记录层协议、SSL 握手协议、协议的安全性分析、代理协议 Proxy 以及 SET 协议与 SSL 协议的比较；第 9 章为安全电子支付机制，主要讲述电子支付系统、智能卡支付方式、电子现金支付方式微支付方式、移动支付方式及支付交易安全；第 10 章为电子商务应用安全，主要讲述网络银行安全、网络营销安全、网上购物安全及网上证券安全。

由于电子商务专业本身的交叉性，编者认为有必要将电子商务安全与传统的计算机专业的网络安全和计算机安全课程区别开来。区别的标准或者原则就在于内容是否与电子商务交易和支付方面相关，把涉及交易和支付部分的安全内容放在电子商务安全的课程中来，而将其他的内容归入常规或者传统的网络安全或者计算机安全课程中。

本书的特色就在于按照这种新的划分办法，将相应方面的内容集合到一本书中，方便读者的学习。特别是针对电子商务专业的教学来说，这种分类的方法对学生的学习有很好的效果。

本书由祝凌曦主编，刘军教授主审，孙熙安、李春艳、孙迅参与编写。在编写的过程中，有许多人给予了很多帮助，北京交通大学的电子商务实验室小组成员包括刘静、和志平、唐秀鑫、

宫素、张京伟、王华、赵剑武、李海荣、石岩、张立员等同学在文稿的录入方面付出了很多劳动，北京交通大学的邢建荣同学、范功庆同学为本书制作了很多精美的插图，北京交通大学的林冬梅、张宁同学为本书制作了全新的多媒体课件，在此表示感谢。

特别感谢北京交通大学出版社为本书的规划、编写、出版提供了宝贵的机会，没有他们的信任和支持就没有本书的出版。

另外，特别感谢我的父亲和母亲对我的教育，没有他们的培养就没有今天站在讲台上的我。在此也深深地感谢我的妻子李娜，她对我的工作给予了高度的支持，并且帮我校稿到深夜，为本书的出版付出了辛勤劳动。

本书在编写的过程中参考和引用了很多专家和学者的著作、文献，在此一并致谢，希望本书的出版能为我国的电子商务教育事业的发展作出一定的贡献。鉴于编者学术水平有限，书中可能存在错误和不妥之处，敬请各位专家和读者给予批评、指正。

编　者

2006 年 10 月

目　录

第1章 绪 论

1.1 电子商务安全的现状与趋势

1.1.1 电子商务安全的现状

近年来,随着数字化、网络化技术的不断发展,社会信息化的程度越来越高,人类社会信息化的领域也越来越大。随着互联网在中国的日益普及,网络已经深入到人们生活的方方面面。伴随着电子商务各方面条件的不断成熟,包括信息基础设施、人们的消费观念、各大 IT 公司的努力,电子商务已经深入人心。

现在人们在网络上可以进行各种商务活动,大到企业和企业之间的商务合作,国际贸易的发展,小到个人生活的各个方面,如房屋、汽车的购买,及音像制品、图书和日常用品购买;具体的如购买电视、冰箱等家用电器,虚拟的如购买音乐、电影。金额数量从 B2B 的几十万上百万元,到下载一个铃声的一两元,购买一篇论文的三五角钱,甚至几分钱的游戏点数。

网络也深入到了工作的各个方面,如果说 20 世纪 90 年代,没有了电,没有了计算机,很多人不知该如何工作,那么到了现在的 21 世纪,如果没有了网络,同样会有很多人无法正常生活。

随着电影《天下无贼》的放映,人们感受到了人间的真情。但是随之而来铺天盖地的巨幅广告"用支付宝,天下真的无贼",才是中国历史上对于网络安全的真正的一次冲击。这不仅标志着中国的 IT 业在电子商务方面已发展到了很深的程度,而且电子商务的安全问题也第一次浮出水面,那么真实地面对普通的老百姓,而不是像以往那样面对的是西装革履的 IT 精英们。画面上傻根安心的笑容,不但体现了普通老百姓对电子商务安全的渴望,也表现出了中国 IT 人士对电子商务安全的信心。

在阻碍电子商务发展的三座大山——电子商务安全、电子支付和电子商务物流中,人们的印象是电子商务物流正在蓬勃发展,物流快递公司不断涌现,而且物流行业人们较为熟悉,容易理解。电子支付系统是银行建设的,和老百姓没有多大关系。只有安全问题是老百姓(也就是电子商务最大的收众者)深深担忧的问题,是电子商务推进中的最大路障。人们对电子商务安全的问题十分关心,但是大多数人对安全问题又缺少必要的了解,这个领域对人们充满了神秘感,人们经常在报纸上、电视上看到或听到黑客的种种消息,对电子商务的网上支付在心理上产生了畏惧感。此外,尽管政府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。因此,让更多的人了解电子商务安全的基本体系和原理是电子商务发展过程中最为重要的工作。

历史上最严重的网络安全事件发生在 2000 年 2 月 7 日、8 日、9 日这三天。在这黑色的三天里,美国许多著名的网站先后遭到计算机黑客攻击,在美国社会引起了强烈震动。黑客三天

来的袭击,造成的直接和间接经济损失达 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,其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。

最近的一次大规模的网络安全事件是发生在 2004 年 11 月 22 日的英国政府网络事故。据报道,2004 年 11 月 22 日,英国政府发生的遍及全国 1000 多个办公室,80% 的台式机的故障,使 8 万多公职人员只能"望屏兴叹,重操纸笔"。

目前网络安全的脆弱性和黑客软件和技术的普及,使得很多的黑客攻击事件已经不像以前那样是专业黑客所为,一些普通人经过一些学习,就可以进行黑客活动。发生在 2004 年的大学生黑客攻破网上银行一夜窃走 77 万元的事件,就给银行等大企业的网络安全敲响了警钟。为了应对网络的冲击,尽快给公众提供网上服务是应该的也是必要的,但前提条件是要做好安全工作,特别像政府机关和银行这些关系到国计民生的重要部门。

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计算机上,一旦某台计算机下载了此程序,那么它就成为黑客可以侵略的对象。黑客可以浏览被入侵者计算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。

即使用户不曾在公共信息场所下载软件,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,即一台计算机被感染后,病毒可通过此计算机上的地址簿向所有这些地址的计算机传播,然后按同样的方法再进一步把态势扩大。通过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,不经意间或许用户的计算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。

1.1.2 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,不仅会使上网企业、机构及用户蒙受巨大经济损失,而且也会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。在现实世界中,黑客是最能吸引人们目光的焦点。从1998年的三少年入侵五角大楼,到著名黑客"分析家"的弟子破坏印度的核研究中心,直至我国的数学硕士以"破坏计算机信息系统"的罪名成为刑法修订后首个以该罪名被逮捕的罪犯。关于黑客的报道、新闻或电影很多,只要在网络上进行一下简单的搜索就可以得到很多这方面的信息。

为了应对黑客的威胁,人们甚至开设了"黑客保险"。为了避免"证券大盗"病毒给用户带来的损失,专家们呼吁应该开设"黑客保险"来为网上的交易保驾护航。

(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。如2003年12月至2004年1月,一黑客利用微软的漏洞盗窃了18万元的充值卡,这固然是网络的问题,但也在一个方面体现出了管理上的欠缺。

(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的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"

早在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。

1.1.3 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,菲律宾一名计算机高手制造出一种称为"爱虫"的计算机病毒,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"等计算机病毒不断兴风作浪,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、一个调制解调器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现成软硬件,加大了网络战争的防御难度。信息系统在防不胜防的破坏性活动面前,显得苍白无力。对网络的非法渗透或操纵,正以令人震惊的速度蔓延。

一些黑客和上网成瘾的人在日以继夜寻找信息系统缺陷。一个每90亿次运算才可能发生一次的错误,被一些关注英特尔产品的人在因特网上公布出来,造成英特尔公司5亿美元的损失。美国国家航空航天局花了100万美元所做的信息安全系统,自以为固若金汤,他们请来因特网安全系统公司董事长克劳斯进行安全演示,结果仅2分钟就被偷走了一大串口令。值得警惕的是,在互联网所营造的无疆界电子空间中,国家主权的概念也正经受到前所未有的冲击。

1995年,美国就提出了"战略信息战"的概念,就是指通过侵袭和操纵计算机网络的办法,对国防和基础设施实施破坏,从而达到战略目的的作战手段。他们把这种"不费一枪一弹的战争"与核战和生化战并列为对国家安全最具威胁的三大挑战。

1. 网络安全无保障,如何踏进信息社会

随着网络经济和网络社会时代的到来,我国的军事、经济、社会、文化各方面都越来越依赖于网络。与此同时,计算机网络上出现了利用网络盗用他人账号上网,窃取科技、经济情报进行经济犯罪等现象。

2000年春天,我国有人利用新闻组这一普通技术手段,轻而易举地从多个商业站点窃取到8万个信用卡号和密码,并标价26万元出售。

与传统的金融管理方式相比,金融电子化如同金库建在计算机里,把钞票存在数据库里,资金在计算机网络里流动。金融计算机系统已经成为犯罪活动的新目标。据有关资料,美国金融界每年由于计算机犯罪造成的经济损失近百亿美元。我国金融系统发生的计算机犯罪也有逐年上升趋势。近年来最大一起犯罪案件造成的经济损失高达人民币2 100万元。

到目前,我国已发生了200多起利用计算机进行金融犯罪的案件,老百姓普遍关注的证券市场近期也受到"黑客"的攻击。

专家指出,电子攻击可分为三个层次。低层次威胁是局部的威胁,包括消遣性黑客、破坏公共财产者;第二个层次是有组织的威胁,包括一些机构黑客、有组织的犯罪、工业间谍;最高层次是国家规模上的威胁,包括敌对的外国政府、恐怖主义组织发起的全面信息战。

据公安部门介绍,仅2000年就破获了黑客案件数百起。目前我国发生的"黑客"事件,大多属于低层次的攻击事件。面对着最低层次的攻击行为,现在基本上还是无能为力,无从防范。那么,又如何防范高层次的黑客呢?完成了我国首次全国范围大规模信息产业调查的专家张爱国认为,如果不注意信息安全的话,"黑客"或敌国很可能利用网络对我国各个核心行业进行攻击,从而令整个社会处于瘫痪状态。信息安全问题,严重影响我国大步迈向网络时代,制约了国家电子商务向纵深发展。

2. "看家护院"式防卫,无法实现超时空的防御

中国90%的互联网站都极易受到攻击,这一调查表明,网络经济包括电子商务的繁荣必须建立在安全的基础上,一旦安全屏障被破坏,所有的努力就可能毁于一旦。

信息业调查专家分析认为,当前国内大多数管理者对网络安全不甚了解,在管理上存在巨