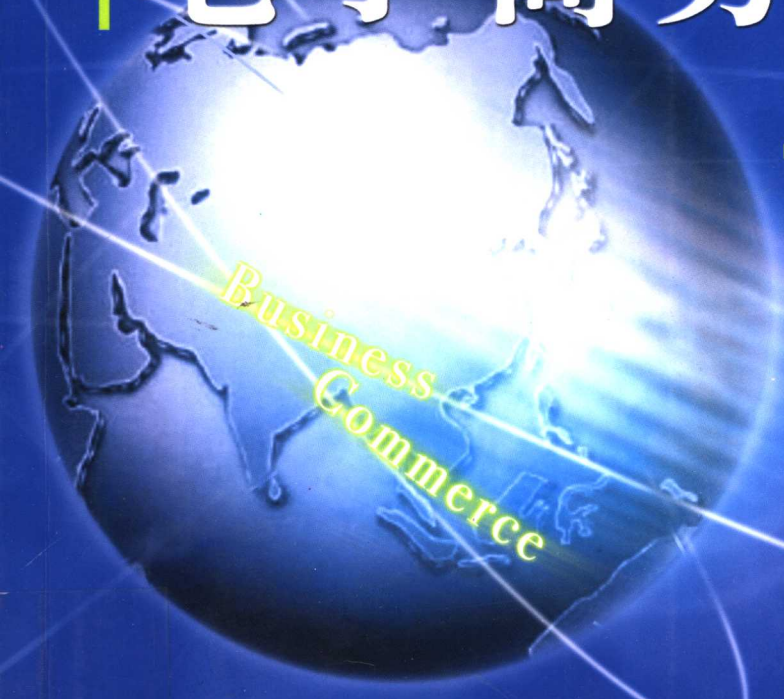
中国信息经济学会电子商务专业委员会
全国高校电子商务专业建设协作组 推荐用书

高等院校
电子商务本科系列教材

电子商务安全



▪总主编 李 琪
▪主编 钟 诚

重庆大学出版社

中国信息经济学会电子商务专业委员会
全国高校电子商务专业建设协作组 推荐用书

高等院校
电子商务本科系列教材

电子商务安全

主　编　钟　诚
副主编　吴明华

重庆大学出版社

内 容 提 要

本书从技术和管理的角度出发，讲授构建和实施安全电子商务系统所必需的基本理论、方法和技术。主要内容包括安全电子商务的体系结构、现代密码技术、数字签名技术、身份和信息认证技术、防火墙技术、虚拟专用网络、Web 安全协议、安全电子邮件系统、防治病毒技术、网络入侵检测方法、证书管理、公钥基础设施、数字水印技术、数字版权保护技术、安全电子商务支付机制、安全电子商务交易协议、在线电子银行系统和证券交易系统的安全，以及安全电子商务应用。全书强调系统性、前沿性，取材先进、科学，内容丰富、实用，图文并茂，可读性强。

本书适合作为高等学校电子商务、信息安全、管理信息系统、计算机科学技术等专业的教材，可以作为电子商务安全技术培训教材，也可供从事安全电子商务系统研究、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/钟诚主编．—重庆：重庆大学出版社，2004.6
（电子商务本科系列教材） ISBN 7-5624-3081-0

Ⅰ.电… Ⅱ.钟… 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(2004)第 031737 号

高等院校电子商务本科系列教材
电子商务安全
主 编 钟 诚
责任编辑：孙英姿 吴达周 版式设计：孙英姿
责任校对：任卓惠 责任印制：张 策
*
重庆大学出版社出版发行
出版人：张鸽盛
社址：重庆市沙坪坝正街 174 号重庆大学(A 区)内
邮编：400030
电话：(023) 65102378 65105781
传真：(023) 65103686 65105565
网址：http://www.cqup.com.cn
邮箱：fxk@cqup.com.cn (市场营销部)
全国新华书店经销
重庆升光电力印务有限公司印刷
*
开本：787×960 1/16 印张：22.25 字数：424 千
2004 年 6 月第 1 版 2006 年 5 月第 2 次印刷
印数：5 001—8 000
ISBN 7-5624-3081-0/F·330 定价：26.00 元

教师信息反馈表

为了更好地为教师服务，提高教学质量，我社将为您的教学提供电子和网络支持。请您填好以下表格并经系主任签字盖章后寄回，我社将免费向您提供相关的电子教案、网络交流平台或网络化课程资源。

请按此裁下寄回我社或在网上下载此表格填好后E-mail发回

<table>
<tr><td>书名：</td><td colspan="2"></td><td>版次</td><td></td></tr>
<tr><td>书号：</td><td colspan="4"></td></tr>
<tr><td>所需要的教学资料：</td><td colspan="4"></td></tr>
<tr><td>您的姓名：</td><td colspan="4"></td></tr>
<tr><td>您所在的校（院）、系：</td><td colspan="4">校（院）　　系</td></tr>
<tr><td>您所讲授的课程名称：</td><td colspan="4"></td></tr>
<tr><td>学生人数：</td><td colspan="2">____人　____年级</td><td>学时：</td><td></td></tr>
<tr><td>您的联系地址：</td><td colspan="4"></td></tr>
<tr><td rowspan="2">邮政编码：</td><td rowspan="2"></td><td rowspan="2">联系电话</td><td>（家）</td></tr>
<tr><td>（手机）</td></tr>
<tr><td>E-mail：（必填）</td><td colspan="4"></td></tr>
<tr><td colspan="3">您对本书的建议：</td><td colspan="2">系主任签字

盖章</td></tr>
</table>

请寄：重庆市沙坪坝正街174号重庆大学（A区）
重庆大学出版社市场部

邮编：400030
电话：023-65111124
传真：023-65103686
网址：http://www.cqup.com.cn
E-mail：fxk@cqup.com.cn

高等院校电子商务本科系列教材编委会

顾　问

常务编委（按姓氏笔画为序）

编委（按姓氏笔画为序）

总 序

从教育部2000年首次批准电子商务本科专业开始，到2003年底为止，已有近200所高校获得开办电子商务本科专业的资格，该专业全国在校学生也已达几万人。但纵观电子商务本科专业的教材建设，尚有不尽人意之处。虽然自2000年以来，国内不少出版社已出版了单本的或系列的电子商务本科教材，但由于教学大纲不统一，编者视角各异，许多高校在电子商务教材的选用中颇感困惑，教学效果不甚令人满意。

教育部从2001年以来，先后在南京审计学院、西安交通大学、华中师范大学和浙江大学等地，召开过全国高校电子商务专业建设工作会议和联席会议，并于第一次全国高校电子商务专业建设工作会议和联席会议上，成立了全国高校电子商务专业建设协作组，旨在通过协作组实现教育部与全国高校中开办电子商务本科专业的单位的紧密联系，在专业建设、教材建设、师资培训、学生学习和实习等多方面起到组织、引导和互助的作用。教育部高教司对电子商务本科专业的师资培训、教材建设等问题给予了极大的关注和指导。2003年3月底，全国高校电子商务专业建设协作组在福建泉州的华侨大学，召开了电子商务专业本科教学大纲研讨会，集思广益，基本形成了电子商务本科教学大纲。

重庆大学出版社在2002年的首届电子商务联席会议上，就与

协作组常务理事会联系，提出要组织力量编写一套电子商务本科专业的教材。到2003年3月，经协商决定：由全国高校电子商务专业建设协作组、中国信息经济学会电子商务专业委员会和重庆大学出版社三家，联合组织编写以讨论后的本科电子商务教学大纲为基础的电子商务本科专业系列教材丛书。

从2003年3月到2004年4月，在重庆大学出版社、全国高校电子商务专业建设协作组和中国信息经济学会电子商务专业委员会的共同努力下，成立了电子商务本科系列教材编写委员会，继而从众多自愿报名和编委会推荐的学校和教师中，选出主编，采取主编负责制，召开写作大纲研讨会，反复征求各方面意见，群策群力，逐步编写出本套电子商务专业系列教材。

该系列教材有如下几点特色：

1. 在专家、学者对教学大纲进行研讨的基础上，吸收了众多学者和学校的意见，使系列教材具有较强的普遍适用性。

2. 集中了协作组和专业委员会内外在电子商务专业教学方面有丰富经验的许多教师、研究人员的宝贵意见，使系列教材有较好的系统性、科学性和实用性。

3. 从教学大纲研讨到编写入纲的讨论，再到按主编负责制进行的编写、审核等，经过一系列较为严格的过程约束，使整套教材趋向严谨和规范。

4. 注重电子商务的理论与实践相结合，教学与科研相结合，课堂教学与实验、实习相结合，把最新的科研成果、实务发展同教学内容有机地结合起来，以促进教学水平的提高。

5. 较全面地包含了我国电子商务教学中的各种课程。不仅把电子商务教学大纲中的各门必修专业课纳入了编写计划，而且还把一些选修课程也纳入了编写计划，从而使开设电子商务本科专业的学校具有更多的选择余地。

应当承认，在全国范围组织编写电子商务新学科的教学丛书，碰到的各种困难确实不少。在各方的共同努力下，有些主要困难已被克服，作为系列教材的丛书即将面世，但仍有待于逐步完善。我

们相信各教学单位和教师们，在具体授课过程中是会根据教学大纲更好地把握教学内容的。当然，大家希望本套系列教材的出版，能给开办电子商务本科专业的学校提供尽可能好的教学用书，但这有个过程，还需得到用书单位的宝贵意见，使编者们与时俱进，不断修改和完善这套系列教材。

乌家培

2004 年 3 月 5 日于北京

前　言

随着 Internet 技术的迅速发展和深入应用，以 Internet 作为交易平台的电子商务正逐步得到人们的认同和接受。一方面，电子商务可以促进生产力进步，扩展和追求更佳的市场，降低生产和销售成本，提升产品和服务质量，改进对客户需求的响应，改善雇员的满意度，建立更好地共享信息的新的伙伴关系，提供新的商业机会；另一方面，电子商务在相当程度上改变着人们的生活方式、生产方式、工作方式和消费策略，甚至改变着人们的思想观念和思维习惯。电子商务深入和广泛的应用，将会使得网络经济进一步得到健康发展。

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金融欺诈，市场/竞争价格等秘密信息的泄露，客户或者商业伙伴关系受损，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机丢失等诸如此类的安全与信任问题。因此，要在这样开放的平台上成功地进行电子交易，必须解决包括交易网络平台的安全，交易双方机密信息的保护，交易双方身份的确认，交易信息在传输过程中的完整性以及交易操作的不可否认等问题。为了解决这些问题，需要计算机密码学、数据库安全、身份认证、数字签名、信息认证、计算机安全、操作系统安全、网络安全、安全电子支付以及安全电子交易协议等技术的支撑。

本书介绍安全电子商务系统所涉及的理论、方法、技术以及安

全电子商务的应用。全书共10章；第1章讨论安全电子商务的体系结构和电子商务的有关安全问题；第2章阐述对称密码系统DES、公钥密码系统RSA、椭圆曲线密码系统EEC、数字签名技术、密钥管理和密钥恢复技术、身份认证和信息认证技术；第3章介绍防火墙、IPsec协议和虚拟专用网、Web安全、安全电子邮件、计算机病毒防治技术和网络入侵检测方法；第4章为数字证书及其管理；第5章介绍公钥基础设施PKI的有关知识以及Windows 2000的PKI使用；第6章讨论信息隐藏技术、数字水印技术和数字版权保护技术。第7章介绍电子支付系统、智能卡支付方式、电子支票支付系统、电子现金支付系统和支付系统；第8章详细分析安全电子商务交易SET协议以及SET协议的加密和认证技术；第9章讨论在线电子银行系统和证券交易系统的安全问题；第10章为安全电子商务系统应用实例。

本书由钟诚任主编，吴明华任副主编。钟诚编写了第1章和第9章，吕皖丽编写了第2章，鲁晓明编写了第3章，陆向艳编写了第4章，杨柳编写了第5章，许亮编写了第6章和第7章，吴明华编写了第8章和第10章。全书由钟诚统稿、润色和校订。

我们衷心感谢重庆大学出版社为本教材的规划、编写、出版提供了宝贵机会，感谢我们的家人对本书写作给予的充分理解和热情鼓励。本教材在编写过程中参考、引用了有关专家学者的文献，在此一并致谢。

本教材的出版如能为我国电子商务教育事业的发展做出一定的贡献，我们将感到非常高兴和荣幸。鉴于编者学术水平有限，编写时间又较紧，书中可能存在错误和不妥之处，敬请专家和读者批评、指正。

编　者

2004年1月

目 录

第 1 章 绪 论 …… (1)
1.1 电子商务的安全问题 …… (1)
1.2 电子商务安全体系结构 …… (5)
1.3 电子商务安全技术的发展 …… (8)
1.4 本章小结 …… (12)
习题 1 …… (12)

第 2 章 密码技术基础 …… (13)
2.1 密码技术 …… (14)
2.2 数字签名 …… (33)
2.3 密钥管理与分发 …… (44)
2.4 身份认证技术 …… (50)
2.5 信息认证机制 …… (65)
2.6 本章小结 …… (71)
习题 2 …… (72)

第 3 章 Internet 安全 …… (73)
3.1 防火墙技术 …… (73)
3.2 IPsec 和虚拟专用网 …… (85)
3.3 Web 安全协议 …… (108)
3.4 安全电子邮件协议 …… (112)

3.5 计算机病毒及其防治 …… (123)
3.6 网络入侵检测 …… (129)
3.7 本章小结 …… (144)
习题 3 …… (144)

第 4 章 证书及其管理 …… (145)
4.1 公钥证书 …… (146)
4.2 认证机构 …… (151)
4.3 证书的发行 …… (157)
4.4 证书的更新 …… (161)
4.5 证书的分发 …… (161)
4.6 证书的撤消 …… (162)
4.7 X.509 证书撤消列表 …… (165)
4.8 X.509V3 版证书扩展域 …… (166)
4.9 本章小结 …… (169)
习题 4 …… (170)

第 5 章 公钥基础设施 PKI …… (171)
5.1 PKI 及其标准的发展 …… (171)
5.2 PKI 的组成 …… (178)
5.3 PKI 的互操作信任模型 …… (183)
5.4 PGP 协议的 PKI 使用 …… (184)
5.5 PKI 认证管理协议 …… (187)
5.6 公钥基础设施的评估 …… (189)
5.7 Windows 2000 的 PKI …… (194)
5.8 本章小结 …… (201)
习题 5 …… (202)

第 6 章 数字水印和数字版权保护技术 …… (203)
6.1 信息隐藏技术 …… (203)
6.2 数字水印技术 …… (208)

6.3 数字版权保护技术 …… (218)
6.4 本章小结 …… (227)
习题 6 …… (227)

第 7 章 安全电子商务支付机制 …… (228)
7.1 电子支付系统 …… (228)
7.2 智能卡支付方式 …… (237)
7.3 电子支票支付系统 …… (242)
7.4 电子现金支付系统 …… (246)
7.5 微支付系统 …… (249)
7.6 本章小结 …… (257)
习题 7 …… (257)

第 8 章 安全电子交易协议 SET …… (258)
8.1 安全电子交易协议 SET …… (258)
8.2 SET 的加密技术和认证技术 …… (264)
8.3 SET 协议的处理逻辑 …… (270)
8.4 SET 协议分析 …… (282)
8.5 SET 协议和 SSL 协议的比较 …… (285)
8.6 本章小结 …… (289)
习题 8 …… (290)

第 9 章 在线电子银行系统和证券交易系统的安全 …… (291)
9.1 在线电子银行系统的体系结构和安全需求 …… (291)
9.2 在线电子银行系统的通信安全和客户认证 …… (295)
9.3 在线电子银行系统的其他安全问题 …… (300)
9.4 在线网络证券交易系统的安全 …… (302)
9.5 本章小结 …… (303)
习题 9 …… (303)

第 10 章　安全电子商务系统应用 …… (305)
10.1　网络银行在中国的应用与发展 …… (305)
10.2　中国银行电子钱包及其网上购物 …… (309)
10.3　招商银行网上支付 …… (319)
10.4　本章小结 …… (331)
习题 10 …… (331)

附　录 …… (332)
附录 1　发表电子商务安全方面文献的部分相关期刊 …… (332)
附录 2　电子商务安全部分相关会议名录 …… (334)
附录 3　电子商务安全部分相关网站 …… (334)

参考文献 …… (336)

第1章 绪 论

随着 Internet 在全世界的广泛应用，近几年来人们纷纷兴办了网上商城、网上书店、网上影院、数字图书馆、网络银行等，于是自然而然地产生了一种新兴的商贸模式——电子商务。有别于传统的商务模式，电子商务借助于开放的 Internet 网络环境和现代信息技术，完成商品（服务）发布、商品选购、发货通知、货款支付、收货确认等工作。这些工作必然涉及到客户和商家身份的验证、客户和商家隐私信息的保护、交易过程中机密信息的安全传输、交易行为的确认等问题。为此，电子商务的应用必须解决好数据加密、身份认证、信息认证、网络安全、交易协议安全等问题。本章将从电子商务安全问题的提出开始，给出电子商务的安全体系结构，阐述支撑电子商务系统安全的相关技术，并且讨论电子商务安全技术的发展趋向。

1.1 电子商务的安全问题

当今的世界已经是数字化的信息社会。在许多城市里，几乎人人都拥有移动电话，并且以前被认为是奢侈品的计算机也日益成为家庭中常用的商品，有些家庭甚至拥有三四台计算机：父母小孩每人一台笔记本电脑或者台式计算机。运用计算机和借助于 Internet，人们可以通过电子邮件、短信（即时消息 IM，Instant Messages）、聊天室和电话相互交流，也可以通过电脑传真文件、听音乐、看电影、购物、存款和付账，等等。

Internet 被设计成为一个高度开放的信息交换的媒介。人们可以在任何时候、任何地点通过 Web 访问他们所需的信息，获取他们所需求的服务。Internet 不仅深刻地影响了个人的生活和工作方式，而且对商业的运作也产生了巨大的冲击。

将传统的贸易活动移植到 Internet 平台上而产生的电子商务正逐渐发展成为人们在 21 世纪进行商务活动的一种有效模式。基于 Internet 的电子商务正成为世界工业和商业一个重要的组成部分。可以说，所有可以买卖的东西都能在 Internet 上进行交易。据 Gartner 组织的研究报告称，2000 年全球电子商务销售额超过 4 330亿美元，比 1999 年销售额增长 189%。电子商务的发展形势喜人、前景诱人。

B2C 的电子商务方式被迅速接受的一个原因是其方便性，人们可以坐在家里方便地购买东西并享受送货上门服务；对于行动不方便的人来说，购物变得容易多了；对于想寻找更好交易的人来说也简单多了（因为不再需要到处逛商店来货比三家）；所有一切只需轻轻按一下鼠标就可以完成，不会再腰酸脚痛。不算运费，考虑一下到处寻找商店和比较商品所花的交通费用，事实上电子购物也能省钱。对于 B2B 领域，电子商务削减了传统商业意义上的商品展示费、场地租用费、仓储费，以及销售人员工资等商业运作成本。其实，Internet 本身就是一个巨大的电子商务展台，它显著地降低了商业运作成本。

基于 Internet 进行的电子商务活动主要有：商务信息通过计算机网络进行传输，在网络上传输的信息是加密数据并保持完整性，贸易双方进行身份认证和确保交易的安全性。安全问题在电子商务的发展和应用中显得越来越突出，如何建立一个安全、便捷的电子商务应用环境，对信息提供足够安全的保护，已经成为商家和用户都十分关心的话题。目前，大多数用户端使用的计算机操作系统基本上都是微软的 Windows 系统和苹果的 Macitosh 操作系统。不像 Unix 操作系统，Windows 和 Macitosh 操作系统的基本设计并不针对安全性，也不保护大多数用户的个人信息。更让人惊慌的事是黑客使用一些病毒进行拒绝服务（DoS）攻击，而大多用户根本没有意识到自己的计算机已经被攻击。DoS 病毒利用多个系统发送大量请求信息包轰击网站，造成目标站点“死机”。2003 年 8 月，冲击波（MSBlaster）和冲击波杀手（Nachi）病毒利用 Windows 2000/XP 操作系统等的远程过程调用 RPC 漏洞，大量感染 Internet 的电脑，使得系统不断被要求重启，无法进行正常的操作和使用，危害面极广，危害后果极为严重。

一波未平，另一波又起。2003 年 9 月中旬，另一个 Windows 操作系统的远程过程调用 RPC 接口又发现存在多个远程安全漏洞。这些漏洞是由于不正确处理畸形消息所造成的，漏洞的实质影响了使用 RPC 的 DCOM 接口（此接口处理由客户端机器发送给服务器的 DCOM 对象激活请求，如 UNC 路径）。攻击者通过 135（UDP/TCP），137/UDP，138/UDP，139/TCP，445（UDP/TCP）和 593/TCP 端口进行攻击，而对于启动了 COM Internet 服务和 RPC over HTTP 的用户来说，攻

击者还可通过 80/TCP 和 443/TCP 端口进行攻击。由于 Windows 的 DCOM 实现在处理参数的时候没有检查长度，所以通过提交一个超长（数百字节）的文件名参数可以导致堆溢出，从而使 RPC 服务崩溃。这样，攻击者向目标发送畸形 RPC DCOM 请求来利用这些漏洞取得本地系统权限，在系统上执行任意操作（如安装程序、查看或更改、删除数据或创建系统管理员权限的账户），严重影响 Windows NT/2000/XP/Server 2003 系统的正常运行。可以想象，在这些被病毒感染的计算机网络和电脑上进行电子商务操作是很难保证其安全性的。

电子商务应用的另一个风险是有效性和实用性问题。对于一个运用 Internet 作为交易手段的商业组织，它需要投资数十亿美元进行信息基础建设。据有关公司发布的市场调查报告估计，黑客（Hacker）的攻击使得一些诸如 Yahoo 和 eBay 这样的热门网站出现暂时性“死机”，从而使它们的损失超过了 12 亿美元，严重影响了 Internet 上电子商务的应用和发展。著名的美国在线公司由于人为操作和技术上的失误，使其 600 多万用户陷入瘫痪 10 小时。美国另一家网络在线通信服务公司的主干网出现重大故障，其后果是 40 万用户被迫中断联络 40 小时。因此，电子商务网站的访问无效或者网络瘫痪，将会促使顾客另外寻找新的供应商，或者回到更传统的一家一家商店地逛的老办法进行交易。

在 Internet 上进行电子交易自然需要有安全、快捷的网络银行来支撑其运作。然而，如果金融计算机网络系统缺乏安全防护，传输网络缺乏安全保障，转账支付缺乏安全通道，授权认证缺乏安全措施，个人私有信息和单位敏感信息缺乏保密措施，那么就会在现代化的 Internet 上出现好比使用“不加锁的储柜”存放资金，“公共汽车”运送钞票，“邮寄托寄”方式传送资金，“商店柜台”方式存取资金和“平信”邮寄机密信息的不安全局面，用户运用 Internet 进行电子交易的热情就会大打折扣。

为了保证基于 Internet 的电子商务的安全性，必须解决如下问题：

①信息的机密性。要求系统存储的信息（用户个人资料、企业或者部门商业机密等）不泄露给非授权的人或实体，并且保证这些加密信息在网络传输过程中只有合法接收者才能获取和读懂，防止攻击者通过互联网、搭线、电磁波辐射范围内安装截收装置，或者在数据包经过的网关和路由器上截获数据以获取用户的银行账号、密码以及企业商业机密等信息。

②信息认证。要求检验信息的完整性，保证数据在传输过程中没有被非授权建立，没有在消息中插入信息以使得接收方读不懂或接收错误的信息，没有删除某条消息或者消息的某部分，没有改变信息流的次序或者更改替换信息的内容（如更