21世纪高职高专电子商务系列教材

电子商务安全

主编 胡国胜

华南理工大学出版社

21世纪高职高专电子商务系列教材

电子商务安全

主　编　胡国胜
副主编　毕　娅　张　志
主　审　程玉宝

华南理工大学出版社
·广州·

内容简介

本书主要是围绕保障电子商务活动的安全性，针对与电子商务应用相关的基本安全问题解决方案进行深入的介绍与阐述。全书共分十一章，主要内容包括：电子商务安全的认识、制定安全的目标、策略的重要性、电子商务面临的威胁、网络操作系统安全、加密技术、常见的安全防御方法、电子支付及SET协议、电子商务安全策略的设计与实现和电子商务网站漏洞的检查与灾难恢复等内容。

本书的特点是不仅从技术的角度来看待电子商务安全问题，而且从项目管理和对安全的认识角度来谈论安全问题。内容通俗易懂，适合作为大专院校、高职高专院校以及中专学校学生教材；也适合企业管理人员、信息技术人员使用；还可作为相应层次电子商务培训班的教材。

图书在版编目（CIP）数据

电子商务安全/胡国胜主编. —广州：华南理工大学出版社，2003.8
（21世纪高职高专电子商务系列教材）
ISBN 7-5623-1986-3

Ⅰ.电… Ⅱ.胡… Ⅲ.①电子商务-安全技术-高等学校 ②技术学校-教材
Ⅳ.F713.36

中国版本图书馆CIP数据核字（2003）第063870号

总 发 行：华南理工大学出版社（广州五山华南理工大学17号楼，邮编510640）
发行部电话：020-87113487 87111048（传真）
E-mail:scut202@scut.edu.cn **http://www2.scut.edu.cn/press**
责任编辑：乔 丽
印 刷 者：中山市新华印刷厂有限公司
开 本：787×1092 1/16 **印张**：15.75 **字数**：380千
版 次：2003年8月第1版第1次印刷
印 数：1～3000册
定 价：25.00元

21世纪高职高专电子商务系列教材
编审委员会

序

从早期的EDI应用开始，到20世纪90年代中期基于互联网商务网站的电子商务兴起，作为对人类社会经济生活产生重大影响的事件，电子商务已经走过了近10个年头。10年来，电子商务所创造的奇迹曾一次又一次地震惊了世界。电子商务以其自身的发展，在创造巨大经济效益的同时，也从根本上改变了整个社会商务活动发展的历史进程。

在网络和电子商务环境下，没有了地域、时空等传统阻碍人类经营活动的限制；完全改变了人们利用信息从事各种经营活动的方式；经营管理的理念、市场的性态、投资者的价值观和资源观、企业的经营和营销策略、供需双方的购销行为模式等等都产生了深刻的变化。特别是在2002年以后，剔除了一些因商业炒作而形成的泡沫，电子商务开始朝着良性健康的方向快速发展。未来电子商务发展将呈现三大趋势：

- 从推动实体上：从原来的以网络公司为主，转变为以实体产业为主体；
- 从业务性质上：以B2B业务为主，技术与业务结合，为主营业务服务；
- 从技术基础上：从完全依赖互联网发展到以互联网为基础，包括：移动通信、地球卫星定位系统、地理信息系统、掌上电脑、手机、电话、视频通信、传真、计算机、各类卡证等为一体的综合网络环境。

电子商务，这种企业利用当代网络环境来从事各种商务活动的形式，终将成为人类商务活动的主要方式。这一点已经成为世人的共识。发展电子商务，成为当代企业拓展经营范围、减低外部购销和经营成本、提高整体竞争能力的必然选择。

目前，制约电子商务在我国发展的因素还有许多，但最根本的还是缺乏适应电子商务发展要求的高素质、复合型人才。早在1997年，清华等部分高校就在企业总裁研修班中开设了“电子商务”课程；从1998年起清华又在MBA教育中率先开设了“电子商务与网络营销”课程。同时，国内很多高职高专的院校也把培养电子商务应用型人才作为当前的重要任务。例如，广东科学技术职业学院从1999年开始招收第一批电子商务专业学生，随着时间的推移，招生规模在不断扩大；2001年，国家教育部正式批准开始招收第一批“电子商务”专业本科生；此外，电子商务自学考试和各种形式培训以及职业技能教育也在培养各种层次的电子商务人才。迄今为止，我国电子商务专业人才的培养已经形成了多层次的立体培养模式。但是，也应看到，目前我国

在电子商务人才培养方面还存在诸多的不足，如课程设置、教材建设等方面离时代发展的要求尚存在一定差距。

这套由华南理工大学出版社和广东科学技术职业学院、武汉职业技术学院等院校联合组织编写的“21世纪高职高专电子商务系列教材”，其特色体现在以下四个方面：

1．本系列教材是为满足高职高专电子商务专业教学需要，并根据目前高职高专院校电子商务专业开设的实际状况及国家对高职应用型人才的培养目标和社会需求确定编写思路，选定编写内容。编写工作突出实用性、应用性。

2．本系列教材的课程设置较为全面，几乎涵盖了从事电子商务活动所必需知识和基本技能。目前出版的共14种，它们分别是：《计算机基础》、《网络技术和Internet应用》、《电子商务概论》、《商务数据库技术》、《电子商务网页制作》《Internet下的市场营销》、《电子商务与物流》、《电子商务安全》、《电子商务法》、《管理学概论》、《商务流通管理》、《电子商务应用与案例》、《企业信息化实施方法》和《电子商务系统设计》。这套教材既可以作为电子商务高职高专学生的教材，也适合作高级中等职业学校电子商务专业学生的教材。对后者学生来说，可以选用其中的数种，舍去一部分较难的内容。同时该教材也适合作电子商务考证方面的参考书和渴望了解电子商务的人士自学使用。

3．本系列教材的内容难易程度适中。在编写过程中，本着贴近社会，贴近学生的原则，使教材具有一定的系统性和时代性，又注重学生能力的培养和启发思维，注意实用性和可操作性，语言力求准确、简练、易懂。全套教材均为教学第一线的教师编写，充分考虑了高职高专学生的情况和培养目标。

4．本系列教材的30多位作者来自十余所大专院校。他们绝大部分是近年来活跃在电子商务教学第一线的中青年教师，具有丰富的教学经验。各院校的作者自始至终遵循着“沟通、交流、信任、创新”的原则，充分发扬团队合作和创新精神。这是系列教材质量和按时完成的重要保证。

由于学科正处于发展阶段，本套教材还存在一些疏漏和不足。参与本系列教材的所有编审人员，将秉着与时俱进的精神，充分把握学科的最新发展趋势，注意吸收国内外最新研究成果和先进技术，在修订过程中不断完善。同时也希望使用本套教材的同仁能不吝赐教，甚至加入到修订再版的作者队伍中来，共同促进电子商务人才培养事业的发展。

应编审委员会要求，欣然为丛书作序。

天道酬勤，愿各位的共同努力能对电子商务教育和发展起到一定的促进作用。

姜旭平

2003年7月2日

于北京清华园

前　言

电子商务是基于计算机技术、网络技术、通信技术和应用软件开发基础上的新兴的、充满生气的经济活动。它以 Internet/Intranet 作为通信手段，使得人们可以在网上通过建立网站树立自己企业的形象，发布自己的产品信息，宣传产品广告，提供售后服务，甚至可以进行网上谈判、电子合同签订、电子交易和资金结算。新型电子商务商业运营模式正以其全球性、高效率、低成本、高收益的特点迅速发展。特别是我国加入 WTO 后，电子商务在我国的应用将会更加快速地发展，以利于从事世界贸易。因此，电子商务的发展前景极其光明。

但是，事物的发展都存在两面性，一方面电子商务给我们带来了便利，但同时也有一部分人利用网络协议、操作系统、硬件的一些缺陷和漏洞进行各种犯罪活动。由于 Internet 的开放性以及其他各种因素的影响，安全和支付问题一直是困扰着电子商务发展的两大重要问题，包括网上传送的信息可靠性和完整性，即不被窃取、不被篡改、不被重写；还包括身份的识别、认证和交易的不可否认性。最重要的是保证电子商务系统的可用性。总之，必须保证网上从事的商务活动是安全的，尽管绝对安全是不存在的。

本书围绕着如何保护电子商务网站安全以及电子商务活动的安全性问题进行展开。全书共分为十一章，主要内容简介如下：

第一章和第二章主要讲述对电子商务安全的认识。包括电子商务安全的含义，电子商务系统构成，电子商务安全隐患、技术、国际规范和法律要素，电子商务安全原则、目标、策略及实现，电子商务面临的安全威胁。

第三章至第七章主要讲述电子商务安全的技术问题。包括电子商务网站常见的攻击（IP 欺骗、Sniffer 技术、Port Scanner 技术、Torjan Horse、DDOS 技术、病毒、WWW 中的安全问题），Win2000 和 UNIX/LINUX 两种网络操作系统的安全问题，加密技术（对称、非对称、单向散列函数、身份验证和数字签名、SSL 协议），电子商务网站常用防御方法（防火墙、非军事区、虚拟专业网、入侵检测系统、认证），数据库系统安全以及生物特征识别等。

第八章和第九章讲述了电子商务活动最重要的问题之一，即电子支付和相关的 SET 协议问题。包括电子支付系统、电子支付工具、电子支付交易步骤、电子支付安全、SET 协议的认证和证书问题、电子支付流程等。

第十章内容主要包括电子商务安全策略设计、实现以及系统总体的强化。

第十一章讲述了网站漏洞的检查和恢复。

附录中列出了与计算机信息安全、域名管理等相关的法律、法规条文。

本书的第一章和第二章由胡国胜编写，第三章和第八章由胡胜红编写，第四章和第五章由毕娅编写，第六章由张志编写，第七章由张志、胡国胜编写，第九章由毕娅、胡胜红编写，第十章和第十一章由吴瑞明、邓宁编写。

本书适合大专院校、高职高专院校、中专学校学生使用，同时也适用于相应水平的电子商务培训班学员以及对电子商务安全感兴趣的爱好者使用。

由于电子商务是一门正在发展的学科，它的技术和应用涉及范围广、内容多、技术更新快、商务模式尚未成熟，加之编者水平所限，书中难免有疏漏和不妥之处，敬请广大读者和专家批评指正。

编　者

2003 年 6 月

目　录

第一章　电子商务安全基础

Internet 是一种用于传输数据的巨大而便利的网络，它为电子商务提供了理想的基础设施。然而，Internet 同时也是一种公开而极不安全的基础设施。因此，Internet 中传输的电子商务数据必须得到某种形式的信息安全保护。事实上，安全问题已成为电子商务发展的瓶颈。如何正确地认识电子商务安全，如何正确地应付电子商务可能出现的安全问题，是本章讨论的内容。

本章主要内容：

- 电子商务安全的正确认识
- 电子商务系统构成
- 电子商务原则、目标、策略和实现

一、电子商务安全的认识

有一个流传很广的故事，故事的寓意是教育小孩要诚实。说的是，一个小孩和一群小伙伴在河边游泳。小孩为了戏弄同伴，装出溺水的样子，“救命呀，救命呀……”，小伙伴们做出迅速反应，却发现只是一个玩笑。一次、两次、三次……小伙伴们对他的救命请求信号麻木、迟钝了。有一次，小孩真的遭遇危险，发出“救命”的呼叫声时，谁也不当一回事，最终悲剧发生。

有趣的是，这个简单的故事在军事上得到了很好的应用。一军事基地四周有铁丝网和运动传感器保护，攻击者带上一只兔子，将它扔到铁丝网上，然后离去。运动传感器报警，卫兵做出反应，没有发现异常就返回了哨所。攻击者又如法来了一遍，卫兵再次做出反应。这样经过几个晚上之后，卫兵关掉了运动传感器。攻击者驾着吉普车直闯铁丝网。这种事在俄罗斯驻阿富汗的军事基地发生过多次。对几个美军基地曾做过试验，结果都取得惊人的成功。

据称，曾经针对前苏联驻华盛顿大使馆进行过类似的攻击。美国人向窗户发射了一粒加拿大薄荷糖（一粒糖丸）。振动触发了报警器，但糖丸碎掉了，找不到报警原因。随后又一粒，砰！报警，不知原因。最后报警器经过修改，窗户振动也不再报警了。

窃车贼在凌晨 2 点、2 点 10 分、2 点 20 分、2 点 30 分……触发汽车报警，直到车主关掉报警器以平息邻居的怒气。早晨醒来，车不见了。

上述几例所用的技巧具有相同的特点，也是目前电子商务网站遭受攻击的最主要的工

具，它就是在第三章被称作的拒绝服务攻击（DOS）。

随着 Internet 时代慢慢演变到 GRID 时代，网络犯罪现象和电子商务安全问题非但没有解决，反而愈演愈烈。仅从下面几则报道中，我们可以看出问题多么严重。

实例 1

今年 27 岁的俄罗斯车里雅宾斯克人瓦西里·戈尔什科夫，最近被美国 FBI 逮捕并指控他利用计算机网络欺诈达 20 次。戈尔什科夫被判刑 3 年，还得赔偿西雅图 Speakeasy Network 公司和加利福尼亚 PayPal of Palo Alto 公司 69 万美元，以补偿他借助 Internet 犯罪给这两家公司造成的损失。他在车里雅宾斯克用自己的计算机上网时，找到了业务系统有薄弱环节的美国公司，入网后盗取了重要的信息。根据 FBI 掌握的情况，有黑客还盗取了几十个信用卡号。美国情报机构证实，受损失的除了上述两家公司以外，还有 CTF 公司等商业机构。2000 年 6 月，FBI 在西雅图成立了一家虚构的公司，成功地诱使戈尔什科夫来美。2000 年 11 月 10 日，在“会谈”结束后，戈尔什科夫立刻被逮捕。（2002 年 10 月 5 日俄罗斯《晨报》报道）

实例 2

英国一名“黑客”因传播电脑病毒导致全球数十万台计算机瘫痪而被伦敦当地法院判处两年徒刑。这名 22 岁的英国人西蒙·瓦洛尔在伦敦萨瑟克法庭上承认，他在 2001 年 12 月至 2002 年 1 月期间制造并传播了电脑病毒。西蒙·瓦洛尔是一名网页设计师。他在自己位于兰迪德诺的家中制造了被称为“通过邮件大量传播型病毒”的系列电脑病毒。这种病毒伪装成无害邮件进入 Internet，内容多为情书或网络安全提示等。在一个月内，瓦洛尔通过电子邮件向全球传播这种能够破坏网络数据库的病毒，直到被美国 FBI 查获，并于 2002 年 2 月被伦敦警察厅信息技术科逮捕。瓦洛尔共导致了 46 个国家的用户数十万台电脑“中毒”。（埃菲社伦敦 2003 年 1 月 21 日报道）

实例 3

巴西一法院 12 日下令逮捕 3 名美国人，罪名是以一个环境基金会的名义通过 Internet 出售亚马逊土地。一对美国夫妇以及美籍巴西人若昂·维洛佐通过 Internet 上森林基金会的网址出售地契。该基金会保证说，出钱者可以得到亚马逊地区的土地。11 日，在接到一名已付出 100 万美元的美国企业家有关诈骗的举报后，警方在帕拉州逮捕了那 3 名嫌疑犯。警察局长热拉尔多·阿劳若说，那 3 人是因被指控犯有诈骗罪而被捕的，他们“出售”的土地属国有财产。（埃菲社巴西贝伦 2002 年 9 月 15 日报道）

实例 4

专家担心恐怖分子以 Internet 发动袭击。情报专家担心，恐怖分子对美国发动的下一轮袭击可能是他们所谓的“分路袭击”———场爆炸事件或自杀性袭击，再加在电脑上发难，那将使执法人员和应急人员更加难以招架。为了应付这一威胁，布什政府正在制定一项防范电脑空间恐怖袭击的策略。白宫网络空间安全特别顾问理查德·克拉克说：“网络袭击比造一种大规模杀伤性武器容易得多，它是一种制造大规模混乱的武器，它们的花费少得多，也容易得多。”利用 Internet 可能造成什么破坏？克拉克和另一些专家列举了一个熟练的电脑黑客可能做到的事情：①改变控制电话服务的电脑软件，切断整个地区的通