第一图书网, tushu007.com

<<电子商务安全与支付>>

图书基本信息

书名：<<电子商务安全与支付>>

13位ISBN编号：9787508471105

10位ISBN编号：7508471105

出版时间：2009-12

出版时间：水利水电出版社

作者：宋少忠，颜辉 主编

页数：295

版权说明：本站所提供下载的PDF图书仅提供预览和简介，请支持正版图书。

更多资源请访问：http://www.tushu007.com

前言

随着经济全球化和我国加入“ WTO ”、改革开放的进一步深化，商业市场逐步向国际化的方向发展，我国电子商务技术和物流产业也有了迅速的发展，已成为极具活力的产业。
由于高新技术和现代管理方法的应用，我国传统的商务、物流活动在管理理念、组织方式、管理制度、业务流程、信息处理手段及作业方式等诸多方面已不能适应现代商务、物流行业发展的需要，由此引发了对电子商务、现代物流等行业专业技术人才和管理人才的竞争。
这些人才应具有现代管理思维方式、组织管理方法和现代技术手段。
这就对教育部门提出了新的要求：如何培养出适合现代商务、物流等行业急需的专门人才。
本套教材是为了配合培养电子商务、现代物流行业专门人才的需要而组织编写的。
现在，有许多高等院校为了适应人才市场的需要，已经或正在准备成立电子商务、物流管理或物流工程专业。
为此，我们组织在这方面具有较高教学水平和教学经验的一线教师精心编写了这套教材，为培养电子商务、现代物流行业的专门人才尽一份力量。
本套《21世纪电子商务与现代物流管理系列教材》具有如下特点：（1）面向21世纪电子商务与物流人才培养的需求，结合本专业学生的培养特点，针对性强。
本套教材的作者都是长期在第一线从事教学的教授、副教授，有的还是硕士生导师、博士生导师，他们都有丰富的教学经验，对学生的基本情况、特点和认知规律等有深入的了解。
（2）本套教材以基本的理论知识为主，阐述相关的实用技术和方法。
在写法上，为了激发学生的兴趣，采用以案例教学的方式，用典型的实例讲解有关的理论与技术的具体操作方法，使学生易于接受。
（3）每本书的编写注重以“ 深入浅出 ”、“ 言简意明 ”为原则，论述基本原理与使用方法，以实例分析的形式阐述具体的分析、操作过程，使读者从一般理论知识到实际运用有一个全面的认识。
（4）书中每章前面有：知识点、难点提要与本章的要求、需要熟练掌握的内容和一般了解的内容；每章结尾有“ 小结 ”。
为了方便学生自学自查，各章配有较多数量的练习题，习题的形式多种多样，有选择题、判断题、填空题、简答题、论述题和思考题等。

内容概要

电子商务安全与支付是电子商务运作中密切联系的两个关键环节。
本书系统介绍了电子商务安全与支付的基本理论、技术以及安全电子商务的应用。
全书共包括电子商务安全理论（网络信息安全、计算机信息安全）、网络安全中涉及的攻防技术、金融支付安全3部分。
　本书内容丰富、层次清晰、讲解深入浅出，可作为高等院校电子商务、信息安全、信息管理、计算机应用和金融等专业的教材，也可作为有关电子商务企业和企事业单位开展电子商务活动的参考书。

书籍目录

序前言第1章 电子商务系统安全与支付概述 1.1 电子商务及其发展 1.1.1 什么是电子商务 1.1.2 电子数据交换(EDI)的发展 1.1.3 Internet的发展 1.1.4 电子商务的发展 1.2 网络信息安全 1.2.1 网络信息安全的目标 1.2.2 电子商务系统安全层次 1.3 电子商务安全规范 1.4 电子商务和支付系统第2章 电子商务系统的安全需求 2.1 安全问题的产生 2.2 交易环境的安全性 2.2.1 WWW简介 2.2.2 客户机的安全性 2.2.3 通信信道的安全性 2.2.4 服务器的安全性 2.3 交易对象和交易过程的安全性 2.4 网上支付的安全需求 2.4.1 支付的发展 2.4.2 电子商务系统中的支付 2.4.3 网上支付系统的安全需求第3章 加密技术 3.1 数据加密概述 3.2 对称密钥密码体制 3.2.1 流密码 3.2.2 分组密码 3.2.3 DES算法 3.2.4 其他分组密码算法 3.2.5 AES算法 3.3 非对称密钥密码体制 3.3.1 RSA密码体制 3.3.2 其他非对称密钥密码体制 3.4 密钥管理 3.4.1 密钥的生存周期 3.4.2 保密密钥的分发 3.4.3 公钥的分发 3.5 数字信封技术第4章 操作系统的安全 4.1 操作系统安全性概述 4.1.1 操作系统安全性设计的原则 4.1.2 操作系统的安全服务 4.1.3 操作系统安全级别的划分 4.2 UNIX系统的安全性 4.2.1 口令与账号安全 4.2.2 文件系统安全 4.2.3 系统管理员的安全策略 4.3 Windows系统的安全性 4.3.1 WindowsNT的安全性 4.3.2 Windows2003的安全性 4.4 常见的操作系统安全漏洞 4.4.1 影响所有系统的漏洞 4.4.2 最危险的Windows系统漏洞 4.4.3 UNIX系统漏洞第5章 电子商务通道的安全 5.1 TCP／IP的基础知识 5.2 网络层的安全性 5.2.1 网络层的安全性 5.2.2 IPSec 5.3 传输层的安全性 5.3.1 传输层的安全性介绍 5.3.2 SSL协议 5.4 应用层的安全性 5.4.1 应用层的安全 5.4.2 安全超文本传输协议(S.HTTP)第6章 服务器的安全 6.1 对服务器的安全威胁 6.1.1 对WWW服务器的安全威胁 6.1.2 对数据库的安全威胁 6.1.3 对公用网关接口的安全威胁 6.1.4 对其他程序的安全威胁 6.2 访问控制和认证 6.2.1 入网访问控制 6.2.2 权限控制 6.2.3 目录级安全控制 6.2.4 属性安全控制 6.2.5 服务器安全控制 6.3 常见企业级防火墙介绍 6.3.1 选择防火墙的要求 6.3.2 选购防火墙应该注意的问题 6.3.3 防火墙的局限 6.3.4 常见企业级防火墙产品介绍 6.4 常见企业级防火墙的使用方法 6.4.1 FireWall－1 6.4.2 CiscoPIX防火墙 6.5 常见的入侵检测系统 6.5.1 概述 6.5.2 常见的企业级网络入侵检测系统第7章 客户机的安全 7.1 对客户机的安全威胁 7.1.1 对客户机的安全威胁介绍 7.1.2 内置的客户机安全机制 7.2 电子邮件的安全 7.2.1 基本概念 7.2.2 电子邮件反病毒 7.2.3 电子邮件内容安全 7.3 使用个人防火墙 7.3.1 为什么要使用个人防火墙 7.3.2 常见的个人防火墙 7.3.3 几种个人防火墙的使用方法 7.4 使用反病毒软件第8章 电子商务网站常见的攻击 8.1 TCP／IP协议简介 8.1.1 传输控制协议(TCP) 8.1.2 网际协议(IP) 8.1.3 差错与控制报文协议(ICMP) 8.1.4 用户数据报文协议(UDP) 8.2 IP欺骗技术 8.2.1 IP欺骗原理 8.2.2 IP欺骗的防范 8.3 Sniffer技术 8.3.1 Sniffer的工作原理 8.3.2 Sniffer的防范 8.4 PortScanner技术 8.4.1 常用的网络相关命令 8.4.2 PoltScanner定义 8.4.3 PortScanner的工作原理和功能 8.5 TorjanHorse 8.5.1 TorianHorse的概念 8.5.2 TorianHorse的特点 8.5.3 TotianHorse的实现 8.5.4 TorianHorse的发现和清除 8.6 DDoS技术 8.6.1 DDoS的原理 8.6.2 DDoS的防范 8.6.3 电子商务网站是DDoS的主要攻击目标 8.7 计算机病毒 8.7.1 病毒的定义 8.7.2 病毒的危害 8.7.3 病毒的分类 8.7.4 病毒的传播途径 8.8 WWW中的安全问题 8.8.1 现代恶意代码 8.8.2 ActiveX的安全性 8.8.3 URL破坏 8.8.4 Cookies 8.8.5 DNS安全 8.9 移动安全第9章 电子商务网站常用防御方法 9.1 防火墙 9.1.1 防火墙的工作原理 9.1 防火墙规则集 9.2 非军事区域 9.2.1 DMZ的概念 9.2.2 非军事区域的设置 9.2.3 电子商务非军事区域的实现 9.2.4 多区网络存在的问题 9.3 虚拟专用网 9.3.1 VPN技术 9.3.2 IPSee协议 9.4 入侵检测系统 9.4.1 入侵检测概念 9.4.2 基于主机的IDS 9.4.3 基于网络的IDS 9.4.4 入侵检测技术发展方向 9.5 认证 9.5.1 第三方认证 9.5.2 PKI的组成 9.5.3 证书认证机构CA 9.5.4 PKI应用第10章 电子商务安全常见技巧 10.1 数据库系统安全 10.1.1 数据库系统安全的重要性 10.1.2 数据库系统安全的含义 10.1.3 数据库中数据的完整性 10.1.4 数据库并发控制 10.1.5 数据库的备份与恢复 10.1.6 数据库攻击常用方法 10.2 生物特征识别 10.2.1 隐写术 10.2.2 数字水印 10.3 潜信道 10.4.外包安全第11章 电子交易与支付 11.1 电子交易 11.1.1 电子交易模式 11.1.2 电子商务流程 11.1.3 电子商务平台介绍 11.2 支付活动及其发展 11.2.1 电子支付基本模式 11.2.2 电子支付基本流程 11.2.3 国内外网络支付发展情况 11.3 电子商务支付系统 11.3.1 电子商务支付系统的构成 11.3.2 电子商务支付系统的功能 11.3.3 电子支付系统的安全要求 11.4 电子支付系统应用 11.4.1 ATM系统 11.4.2 POS系统 11.4.3 电子汇兑系统 11.4.4 网上支付系统第12章 电子支付工具 12.1 电子货币

12.1.1 电子货币的概述　12.1.2 电子货币的分类　12.1.3 电子货币的职能与作用　12.1.4 中国电子货币的发展现状 12.2 银行卡　12.2.1 银行卡概述　12.2.2 信用卡　12.2.3 借记卡　12.2.4 IC金融卡　12.2.5 中国主要银行卡　12.2.6 国外信用卡及国际卡组织 12.3 网络货币　12.3.1 信用卡型网络货币　12.3.2 电子现金　12.3.3 电子支票　12.3.4 电子钱包第13章 网上金融 13.1 网上银行　13.1.1 网上银行服务　13.1.2 中国网上银行的现状及发展 13.2 网上证券交易　13.2.1 网上证券交易的发展现状　13.2.2 网上证券交易模式和系统　13.2.3 网上证券交易的基本方法　13.2.4 网上证券交易的资金支付 13.3 网上保险　13.3.1 网上保险的主要内容　13.3.2 网上保险系统　13.3.3 网上保险经营模式第14章 网站漏洞的检查和灾难恢复 14.1 对站点进行风险分析　14.1.1 什么是风险　14.1.2 企业资产与风险　14.1.3 攻击威胁与风险　14.1.4 网站漏洞与风险 14.2 检查自己站点的安全漏洞　14.2.1 研究网站漏洞　14.2.2 决定检查技术　14.2.3 使用自动扫描工具 14.3 雇用一个入侵检测小组 14.4 拟订灾难恢复计划　14.4.1 拟订灾难恢复计划的目的　14.4.2 灾难恢复计划的目标　14.4.3 灾难恢复计划的内容 14.5 信息数据库备份和恢复　14.5.1 数据库备份的实例　14.5.2 数据库恢复 14.6 防范自然灾害　14.6.1 自然灾害及引起的灾难　14.6.2 防范措施 14.7 事件反应、跟踪和法规　14.7.1 事件反应策略　14.7.2 建立事件反应小组　14.7.3 制定事件反应程序　14.7.4 事件跟踪　14.7.5 司法调查与适用法律第15章 电子商务支付与安全的法律保障 15.1 电子商务参与各方的法律关系　15.1.1 买卖双方当事人的权力和义务　15.1.2 网络交易中心的法律地位　15.1.3 关于网站经营者侵权的法律责任　15.1.4 网络交易客户与网上银行间的法律关系　15.1.5 认证机构在电子商务中的法律地位 15.2 电子商务交易安全保护法　15.2.1 联合国电子商务交易安全的法律保护　15.2.2 中国电子商务交易安全的法律保护 15.3 中华人民共和国《电子签名法》参考文献

章节摘录

插图：（2）违反授权原则：一个授权进入系统做某件事的用户，在系统中进行未经授权的其他事情，表面看来这是系统内部的误用或滥用问题，但这种威胁与外部穿透有关联。
一个攻击者可以通过猜测口令接入一个非特许用户账号，进而可揭示系统的薄弱环节，取得特许接入系统权限，从而严重危及系统的安全。
（3）植入：一般在系统穿透或违反授权攻击成功后，入侵者常要在系统中植入一种能力，为以后攻击提供方便条件，如向系统中注入病毒、蛀虫、特洛伊木马、陷阱、逻辑炸弹等来破坏系统正常工作。
特洛伊木马为攻击者服务，例如一种表面上合法的字处理软件能将所有编辑文档复制存入一个隐蔽的文件中，供攻击者检索。
（4）通信监视：这是一种在通信过程中从信道进行搭线窃听的方式，通过搭线和电磁泄漏等对机密性进行攻击，造成泄密，或对业务流量进行分析，获取有用情报。
侦察卫星、监视上层、预警卫星、间谍飞机、隐身飞机、预警飞机、装有大型综合孔径雷达的高空气球、无数微型传感器均可用于截获和跟踪信息。
（5）通信干扰：攻击者对通信数据或通信过程进行于预，对完整性进行攻击，篡改系统中数据的内容；修改消息次序、时间（延时和重放），注入伪造消息。
（6）中断：对可用性进行攻击，破坏系统中的硬件，包括硬盘、线路、文件系统等，使系统不能正常工作，破坏信息和网络资源。
高能量电磁脉冲发射设备可以摧毁附近建筑物中的电子器件，正在研究中的电子生物可以吞噬电子器件。
（7）拒绝服务：指合法接入信息、业务或其他资源受阻，例如一个业务口被滥用而使其他用户不能正常接入，又如Internet的一个地址被大量信息垃圾阻塞等。

编辑推荐

《电子商务安全与支付》：电子商务与现代物流管理系列教材

第一图书网, tushu007.com

版权说明

本站所提供下载的PDF图书仅提供预览和简介，请支持正版图书。

更多资源请访问:http://www.tushu007.com