

<<电子商务安全>>

图书基本信息

书名：<<电子商务安全>>

13位ISBN编号：9787505373877

10位ISBN编号：7505373870

出版时间：2002-4-1

出版时间：电子工业出版社

作者：冯矢勇,庄燕滨

页数：215

字数：365

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>

## <<电子商务安全>>

### 内容概要

编辑推荐：本书全面介绍了电子商务的安全隐患、安全技术的基础理论和实际的解决方案，内容包括：物理设备、因特网、客户机/服务器和电子商务中的种种不安全性；建立安全的电子商务流程概念、加密与密钥体系、如何实现数据完整性、数字签名、数字认证、安全协议与标准；物理设备和客户机/服务器的安全措施，防火墙的使用，对访问的认证和控制，S/MIME，SSL，SET和数字认证的使用；如何进行安全的管理等。

本书论述深入

## 书籍目录

电子商务安全隐患篇第1章 电子商务安全隐患概述1.1 信息安全的历史故事1.2 电子商务信息的价值1.3 电子商务时代安全隐患丛生1.3.1 处处有安全漏洞, 时时有安全隐患1.3.2 电子商务中的犯罪特点1.3.3 电子商务发展的关键是安全性1.3.4 安全威胁的林林总总1.4 电子商务安全的中心内容1.4.1 商务数据的机密性1.4.2 商务数据的完整性1.4.3 商务对象的认证性1.4.4 商务服务的不可否认性1.4.5 商务服务的不可拒绝性1.4.6 访问的控制性1.4.7 其他内容1.5 黑客与攻击三步曲1.5.1 黑客与攻击者1.5.2 非法使用者与过失者1.5.3 攻击者的三步曲习题一第2章 物理设备的不安全性2.1 单机硬件故障2.2 网络设备故障2.3 软件问题2.4 天灾2.5 人为事故习题二第3章 Internet的不安全性3.1 Internet的安全漏洞3.1.1 Internet各个环节的安全漏洞3.1.2 外界攻击Internet安全的类型3.1.3 局域网服务和相互信任的主机的安全漏洞3.1.4 设备或软件的复杂性带来的安全隐患3.2 TCP/IP协议及其不安全性3.2.1 TCP/IP协议简介3.2.2 IP协议的安全隐患是极严重的3.2.3 TCP协议劫持入侵3.2.4 嗅探入侵3.3 HTTP和Web的不安全性3.3.1 HTTP协议的特点3.3.2 HTTP协议中的不安全性3.3.3 Web站点的安全隐患3.4 E-mail, Telnet, 网页的不安全性3.4.1 E-mail的不安全性3.4.2 入侵Telnet会话3.4.3 网页做假3.4.4 电子邮件炸弹和电子邮件列表链接3.5 网上安全攻击实例3.5.1 病毒3.5.2 主动搭线窃听3.5.3 对不可拒绝性的安全威胁3.5.4 薄弱的认证环节3.5.5 系统的易被监视性3.6 人为过失3.6.1 工作压力引起精力不集中3.6.2 由于通信不畅3.6.3 系统管理员的失误习题三第4章 客户机 / 服务器的不安全性4.1 对Web服务器的安全威胁4.1.1 高权限的安全威胁4.1.2 服务器目录的默认设置4.1.3 CGI中的不安全性4.1.4 ASP中的不安全性4.1.5 对Web服务器其他程序的安全威胁4.1.6 服务器端嵌入4.1.7 来自FTP的安全威胁4.1.8 口令不当4.1.9 邮件炸弹4.2 UNIX系统服务器的不安全性4.2.1 攻破口令4.2.2 Web服务器软件的不安全性4.3 客户机的不安全性4.3.1 对客户机安全构成威胁的来源4.3.2 浏览器的安全4.3.3 伪装成合法网站的服务器4.3.4 在Web活动页面里的特洛伊木马4.3.5 Java、Java小应用程序与JavaScript4.3.6 ActiveX控件4.3.7 图形文件、插件和电子邮件的附件4.3.8 Cookie的安全威胁4.4 无法估计主机的安全性习题四第5章 电子商务中的不安全性5.1 电子商务数据库的不安全5.1.1 篡改数据库数据5.1.2 窃取数据库数据5.2 从事电子商务人员的管理5.3 密切注意未来的安全威胁5.3.1 电子支付手段5.3.2 EDI要利用Internet5.3.3 B to B的发展5.3.4 电子商务法律漏洞习题五电子商务安全基础篇第6章 电子商务安全基础概述6.1 电子商务的安全要求6.1.1 电子商务安全基础要求6.1.2 电子商务安全要求的特殊性6.2 电子商务安全与其他领域的交融6.3 安全风险与安全保护6.3.1 认识安全风险6.3.2 安全风险的特点6.3.3 风险管理习题六第7章 电子商务流程的安全事务7.1 建立认证中心CA和其他各种第三方公证机构7.1.1 建立认证中心CA等的必要性7.1.2 建立认证中心CA等概述7.2 电子支付系统7.2.1 支付系统的特点7.2.2 卡的安全体系和卡的安全7.2.3 电子信用卡系统7.3 安全电子商务的主要流程7.3.1 安全电子商务系统的组成7.3.2 电子商务各参与单位的作用习题七第8章 加密与密钥体系8.1 加密概念与基本方法8.1.1 替代密码法8.1.2 转换密码法8.1.3 网络上数据的加密方式8.1.4 文件加密8.1.5 密钥体系8.2 单钥密码体制8.2.1 流密码体制8.2.2 分组密码体制8.2.3 DES加密标准8.2.4 IDEA加密算法8.2.5 RC-5加密算法8.2.6 单钥密码体制的特点8.3 双钥密码体制8.3.1 RSA密码体制8.3.2 ElGamal密码体制8.4 加密算法和标准8.5 密钥的管理习题八第9章 数据的完整性和安全9.1 数据完整性和安全概述9.1.1 数据完整性被破坏的严重后果9.1.2 散列函数的概念9.1.3 散列函数应用于数据的完整性9.1.4 数字签名使用双钥密码加密和散列函数9.2 应用散列函数保证完整性的方案9.2.1 应用散列函数的基本方式9.2.2 MD-4和MD-5散列算法9.2.3 安全散列算法 (SHA) 9.2.4 其他散列算法习题九第10章 数字鉴别10.1 数字签名10.1.1 数字签名的基本概念10.1.2 数字签名的必要性10.1.3 数字签名的原理10.1.4 数字签名的要求10.1.5 数字签名的作用10.1.6 单独数字签名的安全问题10.1.7 RSA签名体制10.1.8 ElGamal签名体制10.1.9 无可争辩签名10.1.10 盲签名10.1.11 双联签名10.2 身份证书与数字认证10.2.1 身份认证证书的概念10.2.2 身份认证证书的类型10.2.3 身份认证证书的内容10.2.4 身份认证证书的有效性10.2.5 身份认证证书的使用10.2.6 数字证书的发行10.2.7 身份证明10.2.8 口令认证系统10.3 公钥数字证书10.3.1 公钥证书的基本概念10.3.2 公钥/私钥对的生成和要求10.3.3 公钥证书的申请、更新、分配10.3.4 公钥的格式10.3.5 公钥证书的吊销10.3.6 证书的使用期限10.3.7 公钥证书的授权信息10.4 公钥基础设施、证书机构和证书政策10.4.1 公钥基础设施10.4.2 认证系统10.4.3 中国电子商务认证中心10.5 数字时间戳及其业务10.5.1 数字时间戳仲裁方案要点10.5.2 数字时间戳链接协议10.6 不可否认业务10.6.1 不可否认业务的概念10.6.2 不可否认业务类型和业务活

动10.6.3 源的不可否认性及实现方法10.6.4 递送的不可否认性及实现方法10.6.5 可信赖第三方10.6.6 解决纠纷10.7 数字签名和证书应用举例习题 十第11章 安全协议与标准11.1 安全协议种类11.1.1 仲裁协议11.1.2 裁决协议11.1.3 自动执行协议11.1.4 密钥建立协议11.1.5 认证协议11.1.6 消息认证11.1.7 实体认证协议11.1.8 认证的密钥建立协议11.1.9 Internet业务提供者协议11.1.10 IKP协议11.2 IPSEC——IP安全协议11.2.1 IPsec的概念11.2.2 IPsec的应用11.2.3 IPsec的优势11.2.4 路由应用11.3 安全超文本传输协议S-HTTP11.3.1 S-HTTP是HTTP的安全扩展11.3.2 S-HTTP和SSL的异同11.3.3 S-HTTP的应用11.4 有关安全技术标准11.4.1 密码技术的国际标准11.4.2 ANSI和ISO的银行信息系统安全标准11.4.3 ISO安全结构和安全框架标准11.4.4 美国政府标准(FIPS) 11.4.5 Internet标准和RFC11.4.6 PKCS11.4.7 其他标准11.5 INTERNET消息安全性协议11.5.1 消息安全性的基本概念11.5.2 保密强化邮件PEM11.5.3 X.400国际电子消息协议11.5.4 消息安全协议MSP11.5.5 各种消息安全协议比较11.6 EDI的安全协议11.7 安全等级习题 十一电子商务安全解决篇第12章 物理设备的安全措施12.1 做好损坏的应对策略12.2 实体安全措施12.2.1 建立物理安全的环境12.2.2 维护良好的环境12.2.3 建立定期检测和日常检查制度12.2.4 容错技术和冗余系统12.3 保护数据的完整性12.3.1 网络备份系统12.3.2 数据文件的备份12.3.3 归档12.3.4 提高数据完整性的预防性措施习题 十二第13章 客户机/服务器的安全措施13.1 客户机的保护措施13.1.1 Web浏览器信息泄漏的防止13.1.2 使用内容协商禁止PostScript危险操作13.1.3 监测活动内容13.1.4 处理Cookie13.1.5 使用防病毒软件13.1.6 网上的安全购物——识别SSL联机13.2 服务器的安全措施13.2.1 UNIX系统正确配置主机的操作系统13.2.2 Web服务器安全配置原则13.2.3 认证和访问控制机制13.2.4 口令的使用和管理13.2.5 注意ASP漏洞13.2.6 商家使用SSL建立安全的商务网站13.3 使用杀毒软件13.3.1 杀毒软件使用综述13.3.2 KV系列杀毒软件13.3.3 瑞星杀毒软件13.3.4 金山毒霸杀毒软件13.3.5 杀毒服务网站13.3.6 国外有名杀毒产品习题 十三第14章 INTERNET上的安全措施和使用安全协议14.1 INTERNET上的安全措施概述14.1.1 网络安全14.1.2 应用安全14.1.3 系统安全性14.1.4 对付一些攻击14.2 使用防火墙14.2.1 防火墙的基本概述14.2.2 防火墙的配置14.2.3 防火墙的类型14.2.4 防火墙的选择14.2.5 防火墙软件14.2.6 防火墙不能对付的安全威胁14.2.7 包过滤技术的概念14.2.8 代理服务技术的概念14.3 对访问的认证和控制14.3.1 对访问的认证14.3.2 对访问的控制14.3.3 入侵的审计、追踪与检测技术14.4 KERBEROS身份验证应用14.4.1 用Kerberos通信过程说明14.4.2 用Kerberos实现认证的NetCheque电子支票系统14.4.3 防止网络上的嗅探入侵14.5 免费加密软件14.5.1 使用RSA算法的SecurPC14.5.2 信息摘要软件14.5.3 其他加密程序14.6 认证证书的发放14.6.1 证书发放政策14.6.2 认证机构之间的相互关系14.6.3 证书中名字的约束14.6.4 认证通路的查找和确认14.6.5 证书管理协议习题 十四第15章 两大安全电子邮件的实用技术15.1 PGP完美的加密程序的使用15.1.1 PGP的概念15.1.2 PGP的原理15.1.3 PGP的作用15.1.4 PGP的安装与设置15.1.5 PGP软件的使用15.1.6 PGP使用的注意事项15.2 S/MIME安全的电子邮件标准15.2.1 Secure-MIME标准15.2.2 S/MIME如何满足电子邮件的安全要求15.2.3 Secure-MIME特点15.2.4 收发S/MIME的操作15.3 PGP与S/MIME比较习题 十五第16章 电子商务的安全协议16.1 SSL——提供网上购物安全的协议16.1.1 安全套接层SSL协议概念16.1.2 SSL提供的安全内容16.1.3 SSL体系结构16.1.4 服务器和浏览器对SSL的支持16.1.5 传输层安全TLS16.2 SET——提供安全的电子商务数据交换16.2.1 网上信用卡安全交易必须用SET16.2.2 SET的认证过程16.2.3 SET协议的安全技术16.2.4 SET交易中的电子钱包16.2.5 商店服务器和支付网关16.2.6 SET网上购物实例16.2.7 SET实际操作的全过程16.3 SET与SSL对比及SET的缺陷16.4 目前国内应用SSL和SET的情况16.4.1 SSL已经开始普及16.4.2 出现同时使用SSL和SET的网站16.4.3 认证中心的涌现及各自的特色16.4.4 电子商务“专业银行”的出现16.5 SET公钥基础设施习题 十六第17章 安全的管理17.1 安全策略制定的目的、内容和原则17.1.1 制定安全策略的目的17.1.2 安全策略的内容17.1.3 制定安全策略的基本原则17.2 安全策略17.2.1 要定义保护的资源17.2.2 要定义保护的威胁17.2.3 要吃透电子商务安全的法律法规17.2.4 建立安全策略和确定一套安全机制17.3 关于版权和知识产权的安全管理17.4 网上安全求援习题 十七附录附录一 加密中的数学知识附录二 电子商务安全名词术语附录三 电子商务安全英语词汇和缩略词

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>