

<<电子商务安全技术>>

图书基本信息

书名：<<电子商务安全技术>>

13位ISBN编号：9787302303862

10位ISBN编号：730230386X

出版时间：2013-2

出版时间：熊平、朱平、陆安生、张爱菊 清华大学出版社 (2013-02出版)

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>

<<电子商务安全技术>>

内容概要

《21世纪高等学校电子商务专业规划教材:电子商务安全技术(第2版)》共包括10章。第1章介绍电子商务安全的基本概念、电子商务安全系统的体系结构及相关技术的介绍;第2章对密码技术及常用算法进行了介绍;第3章是认证技术,介绍了身份认证和消息认证,并对常用的认证技术进行了阐述;第4章对称密码体制和非对称密码体制中的密钥管理技术, Diffie—Hellman密钥交换协议等进行了介绍;第5章介绍计算机网络安全技术,包括防火墙、虚拟专用网、计算机病毒和入侵检测技术等;第6章介绍了公钥基础设施;第7章介绍了电子支付基本概念、我国和国外的支付系统,电子支付方式和网络银行等;第8章介绍安全套接层协议,包括认证算法、协议实现和协议安全性分析等;第9章介绍电子商务安全协议——SET协议,并和SSL协议进行了对比分析;第10章是移动电子商务安全,在这章介绍了我国的无线网络、常用的无线网络协议,移动电子商务存在的安全隐患以及目前移动电子商务中常用的安全解决方法。

书籍目录

第1章电子商务安全概论 1.1电子商务发展现状 1.2电子商务安全现状分析 1.2.1网络安全现状 1.2.2黑客常用的攻击手段 1.3电子商务安全需求及相应的安全措施 1.4电子商务安全体系结构 1.4.1电子商务安全问题分类 1.4.2电子商务的安全管理 1.4.3电子商务的法律保障 1.4.4电子商务安全体系结构 1.5电子商务安全技术 第2章信息加密技术 2.1密码技术概述 2.2密码技术的基本知识 2.3密码分析 2.4密码学的基本数学知识 2.4.1基本概念 2.4.2欧几里得算法 2.4.3欧拉函数和欧拉定理 2.4.4乘法逆元及求解 2.4.5离散对数 2.5对称密码体制 2.5.1对称密码体制的分类 2.5.2AES加密标准 2.6非对称密码体制 2.6.1非对称密码体制的理论基础 2.6.2RSA公钥密码体制 2.6.3椭圆曲线密码系统 第3章认证技术 3.1身份认证 3.1.1身份认证技术 3.1.2身份认证协议 3.2数字签名 3.2.1数字签名原理 3.2.2RSA数字签名 3.2.3DSS数字签名 3.2.4其他数字签名 3.3消息认证 3.3.1消息认证机制 3.3.2消息认证方法 第4章密钥管理 4.1密钥管理概述 4.1.1密钥管理的重要性 4.1.2密钥管理简介 4.2对称密码体制的密钥管理 4.2.1密钥分类 4.2.2密钥管理过程 4.3非对称密码体制的密钥管理 4.3.1公开密钥的分配 4.3.2秘密密钥的公开密钥加密分配 4.4Diffie—Hellman密钥交换协议 4.4.1Diffie—Hellman密钥交换协议原理 4.4.2Diffie—Hellman密钥交换协议的特性 参考文献 第5章计算机网络安全 5.1网络安全基础 5.1.1网络安全体系 5.1.2网络安全的必要性 5.1.3安全级别 5.1.4系统的访问控制 5.2防火墙 5.2.1防火墙基本知识 5.2.2防火墙的设计准则 5.2.3包过滤防火墙 5.2.4应用层网关 5.2.5线路层网关 5.2.6防火墙举例 5.3虚拟专用网 5.3.1VPN简介 5.3.2VPN协议 5.3.3VPN的安全性 5.4入侵检测系统 5.4.1入侵检测 5.4.2入侵检测系统分类 5.4.3入侵检测系统的部署 5.4.4入侵检测系统优点与缺点 5.5计算机病毒及防治 5.5.1计算机病毒概述 5.5.2网络防病毒技术 5.5.3计算机病毒类型 5.5.4计算机病毒的清除 5.5.5网络防病毒技术发展趋势 5.6电子邮件安全 5.6.1PGP 5.6.2RFC822 5.6.3MIME 5.6.4S / MIME的安全功能 5.6.5S/MIME的消息格式 5.6.6S / MIME的证书 5.7网络安全的攻防体系 5.7.1网络安全的攻防体系 5.7.2网络抓包软件Sniffer 5.7.3利用Sniffer抓包 第6章公钥基础设施 6.1PKI的功能和性能 6.2PKI的组成 6.3PKI的标准 6.4PKI的数字证书 6.4.1数字证书的格式 6.4.2数字证书的功能 6.4.3数字证书的分类 6.4.4其他类型的数字证书格式 6.4.5数字证书的扩展域 6.5证书机构 6.5.1CA的功能 6.5.2CA的组成 6.6证书管理 6.6.1证书的注册和生成 6.6.2证书的颁发 6.6.3证书验证 6.6.4证书的使用 6.6.5证书存放 6.7证书的撤销 6.7.1数字证书撤销请求 6.7.2数字证书撤销表的格式 6.7.3撤销数字证书的方法 6.7.4X.509标准的数字证书撤销表 6.8CA的证书策略和证书实施说明 6.8.1保证等级与证书等级 6.8.2CP和CPS的主题内容 6.9PKI的运行模型 6.9.1管理实体 6.9.2端实体 6.9.3证书库 6.10PKI的信任模型 6.11PKI的应用实例 6.12PKI的国内外发展情况 6.12.1我国PKI体系的发展 6.12.2国外PKI/CA体系发展状况的研究 参考文献 第7章电子支付技术 7.1电子支付系统 7.1.1电子支付 7.1.2电子支付系统概述 7.1.3我国的电子支付体系 7.1.4国际电子支付与结算系统 7.2电子支付工具 7.2.1电子货币 7.2.2信用卡支付 7.2.3电子现金支付方式 7.2.4电子支票支付 7.3移动支付 7.3.1移动支付概述 7.3.2移动支付模式 7.3.3移动支付技术标准 7.3.4移动支付安全 7.4网络银行 7.4.1网上银行概述 7.4.2网上银行的模式 7.4.3招商银行网上个人银行实例 第8章安全套接层协议 8.1SSL概述 8.1.1SSL协议的发展过程 8.1.2SSL协议提供的服务及其实现步骤 8.1.3SSL协议与电子商务 8.1.4SSL协议的分层结构 8.2SSL握手协议 8.2.1建立安全能力 8.2.2服务器认证与密钥交换 8.2.3客户端认证与密钥交换 8.2.4完成 8.3SSL记录协议 8.4SSL协议采用的加密和认证算法 8.4.1加密算法 8.4.2认证算法 8.4.3会话层的密钥分配协议 8.5SSL协议安全性分析 8.5.1安全机制分析 8.5.2脆弱性分析 8.6Windows下SSL的配置 第9章安全电子交易协议 9.1SET协议概述 9.1.1安全付费需求 9.1.2SET协议的功能及其重要特征 9.2SET交易的参与者 9.3SET协议采用的加密和认证技术 9.4SET的交易流程 9.4.1购买请求 9.4.2支付授权 9.4.3取得支付 9.5SET协议的安全性分析 9.6SSL与SET协议的比较 第10章移动电子商务安全 10.1移动电子商务概述 10.1.1移动电子商务概述 10.1.2移动电子商务交易模型 10.2无线网络 10.2.1无线网络简介 10.2.2无线局域网 10.2.3无线局域网 10.2.4无线城域网 10.2.5无线广域网 10.3移动电子商务面临的安全问题 10.3.1移动电子商务安全要素 10.3.2移动电子商务面临的安全威胁 10.4移动电子商务安全解决方案 10.4.1移动电子商务安全体系结构 10.4.2移动电子商务安全技术

章节摘录

版权页：插图：如果一个密码系统的加密密钥和解密密钥相同，或者虽然不相同，但由其中的任意一个密钥可以很容易地推导出另外一个，则所采用的就是对称密钥密码体制。

如A5、SEAL、DES、IDEA、RC5、AES等都是对称密码体制的加密算法。

反之，如果一个密码系统的加密和解密分别用两个不同的密钥实现，并且由加密密钥推导出解密密钥在计算上是困难的，则该系统所采用的就是非对称密码体制。

采用非对称密码体制的每个用户都有一对选定的密钥，其中一个是可以公开的，称为公钥，一个由用户自己秘密保存，称为私钥。

RSA、E1Gamal、椭圆曲线密码等都是非对称密码体制的典型代表。

对称密码体制用复杂的非线性交换来实现；非对称密钥密码体制一般使用某个数学上的难题来实现。一般来说，后者的安全程度与现实的计算能力具有密切的关系，非对称密码体制适应于开放性的使用环境，密钥管理问题相对简单，可以方便、安全地实现数字签名和验证。

(3) 根据密码算法对明文信息的加密方式，可分为流密码和分组密码。

流密码逐位地加密明文消息字符（如二进制数），本书中介绍的A5、SEAL即为流密码算法；分组密码将明文消息分组（每个分组含有多个字符），逐组地进行加密，本书所介绍的DES、IDES、RC5、AES等即为分组密码算法。

(4) 按照加密变换是否可逆，又可将密码算法分为单向函数密码以及人们通常所指的双向变换密码。

单向函数是一类特殊的密码体制，其性质是可以容易地把明文转换成密文，但再把密文转换成原来的明文却是困难的（有时甚至是不可能的）。

单向函数只适用于某种特殊的、不需要解密的情况（如密钥管理和信息完整性鉴别技术）。

典型的单向函数包括MD4、MD5、SHA—1等。

另外，关于密码体制的分类，还有一些其他的方法，例如按照在加密过程中是否注入了客观随机因素可以分为确定型密码体制和概率密码体制等。

我们最经常使用的分类方法是第二种。

2.3密码分析 密码分析主要研究如何分析和破译密码。

对于一个密码体制，如果能够根据密文确定明文或密钥，或者能够根据明文和相应的密文确定密钥，则我们说这个密码体制是可破译的；否则，称其为不可破译的。

密钥空间中不同密钥的个数称为密码体制的密钥量，它是衡量密码体制安全性的一个重要指标。

一个密码系统的实际安全性牵涉到两方面的因素。

1.所使用的密码算法的保密强度 密码算法的保密强度取决于密码设计的水平、破译技术的水平以及攻击者对于加密系统知识了解的程度。

密码系统所使用的密码算法的保密强度提供了该系统安全性的技术保证。

<<电子商务安全技术>>

编辑推荐

《21世纪高等学校电子商务专业规划教材:电子商务安全技术(第2版)》可作为电子商务、信息管理、计算机、国际贸易类专业本科生和研究生的教材,也可作为相关领域高级管理人员的培训教材或参考用书。

<<电子商务安全技术>>

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>