

## <<电子商务信息安全技术>>

### 图书基本信息

书名：<<电子商务信息安全技术>>

13位ISBN编号：9787111323020

10位ISBN编号：7111323025

出版时间：2011-1

出版时间：沈美莉、陈孟建、郁晓红、等 机械工业出版社 (2011-01出版)

作者：沈美莉，陈孟建，郁晓红 等著

页数：268

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>

## <<电子商务信息安全技术>>

### 前言

随着互联网技术的发展,网络安全成了新的安全研究热点。

电子商务是互联网应用发展的必然趋势,也是国际金融贸易中越来越重要的经营模式。

安全是保证电子商务健康有序发展的关键因素。

由于Internet本身的开放性,使电子商务系统面临着各种各样的安全威胁。

目前安全问题已成为电子商务的核心问题。

大量的事实说明,要保证电子商务的正常运作,就必须高度重视电子商务的安全问题。

电子商务的安全涉及方方面面,不是一堵防火墙或一个电子签名就能简单解决的问题。

安全问题是电子商务成功与否的关键所在:因为电子商务的安全问题不仅关系到个人的资金安全、商家的货物安全、企业的交易安全,还关系到国家的经济安全,关系到国家经济秩序的稳定问题。

而要保证电子商务的安全,除了要充分依靠现代信息技术,尤其是信息安全技术手段来进行保护外,还需要安全管理的制度和手段来约束,需要法律、法规环境的保障。

本书从电子商务信息安全技术角度出发,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。

全书在编排上由简到繁、由浅入深和循序渐进,力求通俗易懂,简捷实用。

主要内容包括电子商务信息安全概述、电子商务网络安全基础、电子商务密码技术、电子商务安全认证技术、防火墙技术、电子交易及其安全、电子支付安全协议、移动电子商务安全、电子商务信息安全实训等。

本书观点新颖,论述深入浅出,内容丰富,可读性好,实践性强,适合作为高职高专学校电子商务、信息安全、管理信息系统、计算机科学技术等专业的教材,也可作为计算机和电子商务领域研究人员与专业技术人员的参考书。

本书由浙江工商大学沈美莉、郁晓红,浙江经贸职业技术学院陈孟建等编著。

参加编写的还有张贵君、陈奕婷、李锋之、袁志刚。

由于写作时间仓促和作者水平有限,书中不当之处敬请读者批评指正。

## <<电子商务信息安全技术>>

### 内容概要

《电子商务信息安全技术》从电子商务信息安全技术角度出发，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。

主要内容包括电子商务信息安全概述、电子商务网络安全基础、电子商务密码技术、电子商务安全认证技术、防火墙技术、电子交易及其安全、电子支付安全协议、移动电子商务安全、电子商务信息安全实训等。

本教材观点新颖，论述深入浅出，内容丰富，可读性好，实践性强。

《电子商务信息安全技术》适合作为高职高专学校电子商务、信息安全、管理信息系统、计算机科学技术等专业的教材，也可作为计算机和电子商务领域研究人员与专业技术人员的参考书。

## 书籍目录

前言第1章 电子商务信息安全概述1.1 电子商务概念1.1.1 电子商务案例1.1.2 电子商务定义1.1.3 电子商务模型1.1.4 电子商务基本框架结构1.1.5 电子商务购物流程1.2 电子商务信息概念1.2.1 数据的概念1.2.2 信息的概念1.2.3 信息系统的概念1.2.4 电子商务信息安全要素1.3 电子商务信息安全概念1.3.1 电子商务信息安全的重要性1.3.2 电子商务面临的挑战1.3.3 电子商务面临的安全威胁1.3.4 电子商务安全问题采取的对策1.4 电子商务信息安全保障1.4.1 电子商务安全控制要求\_1.4.2 电子商务安全技术1.4.3 电子商务安全保障体系\_1.4.4 我国电子商务法律法规1.5 电子商务信息安全体系结构1.5.1 电子商务安全体系结构框架1.5.2 网络服务层与加密技术层1.5.3 安全认证层与交易协议层习题第2章 电子商务网络安全基础2.1 电子商务网络安全概述2.1.1 网络安全概念2.1.2 影响网络安全的因素2.1.3 网络安全的威胁2.1.4 威胁网络安全的主要方法2.1.5 网络安全威胁的来源2.2 电子商务网络安全模型2.2.1 网络安全基本模型2.2.2 PDRR网络安全模型2.2.3 PDRR网络安全模型术语2.3 电子商务网络体系结构2.3.1 网络体系结构的基本概念2.3.2 OSI网络安全体系2.3.3 网络安全协议2.3.4 OSI网络层2.4 电子商务网络安全保障机制2.4.1 硬件安全保障机制2.4.2 软件安全保障机制2.4.3 电子商务网络安全体系2.4.4 我国网络安全形势及应对措施习题二第3章 电子商务密码技术3.1 密码学3.1.1 密码学的起源与发展3.1.2 密码学概述3.1.3 密码体制分类3.1.4 密码系统设计原则3.2 传统密钥密码体制3.2.1 传统密码数据的表示3.2.2 置换密码3.2.3 替代密码3.2.4 移位密码和其他'3.3 对称密钥密码体制3.3.1 对称密钥密码体制概念3.3.2 数据加密标准3.3.3 高级数据加密标准3.4 非对称密钥密码体制3.4.1 非对称密钥密码体制概念3.4.2 RSA加密算法3.4.3 其他非对称加密算法3.5 密钥管理3.5.1 密钥管理概述3.5.2 密钥的种类和作用3.5.3 密钥的生成3.5.4 密钥的管理习题三第4章 电子商务安全认证技术4.1 身份认证与认证体系4.1.1 身份认证概念4.1.2 身份认证方法4.1.3 数字证书4.1.4 认证中心4.2 身份认证构架体系4.2.1 身份认证构架方案4.2.2 SecurID4.2.3 ACE / Server4.2.4 ACE / Agent4.3 PKI体系4.3.1 PKI体系概述4.3.2 PKI安全服务功能4.3.3 PKI系统功能4.3.4 PKI客户端软件4.4 身份认证协议4.4.1 Kerberos认证协议4.4.2 x.509标准4.4.3 PKCS标准4.5 生物特征身份认证4.5.1 生物特征身份论证概述4.5.2 生理特征身份论证4.5.3 行为特征身份论证习题四第5章 防火墙技术5.1 防火墙概述5.1.1 防火墙概念5.1.2 防火墙的功能5.1.3 防火墙的类型5.1.4 企业如何选购防火墙5.2 防火墙体系结构5.2.1 包过滤型结构5.2.2 双宿网关结构5.2.3 屏蔽主机结构5.2.4 屏蔽子网结构5.3 防火墙的应用5.3.1 控制来自互联网对内部网络的访问5.3.2 控制来自第三方网络对内部网络的访问5.3.3 控制内部网络的几种方法5.3.4 中小企业防火墙的典型应用5.4 分布式防火墙5.4.1 分布式防火墙概述5.4.2 分布式防火墙特点5.4.3 分布式防火墙的体系结构5.4.4 分布式防火墙的应用5.5 防火墙安装、配置与天网防火墙5.5.1 防火墙安装与配置5.5.2 防火墙与路由器的区别5.5.3 天网个人防火墙概述5.5.4 天网个人防火墙设置习题五第6章 电子交易及其安全6.1 电子货币6.1.1 电子货币概述6.1.2 电子货币的表现形式6.1.3 电子货币支付方式发展6.1.4 电子货币发展战略6.2 电子交易技术6.2.1 电子交易概述6.2.2 电子交易模型6.2.3 电子交易支付模型6.2.4 电子交易中买卖双方当事人的权利6.2.5 电子交易的发展6.3 EDI技术6.3.1 EDI概述6.3.2 EDI系统结构和特点6.3.3 EDI系统的组成6.4 网络金融6.4.1 网络银行概述6.4.2 网络银行服务6.4.3 网络证券交易6.4.4 网络保险习题六第7章 电子支付安全协议7.1 电子支付概述7.1.1 传统支付方式7.1.2 电子支付方式7.1.3 电子支付体系结构7.1.4 电子支付的风险7.2 安全套接层协议7.2.1 安全套接层协议概述7.2.2 安全套接层协议结构7.2.3 安全套接层协议应用7.3 安全电子交易协议7.3.1 安全电子交易概述7.3.2 安全电子交易协议工作原理7.3.3 安全电子交易协议应用习题七第8章 移动电子商务安全8.1 移动电子商务安全概述8.1.1 移动商务定义8.1.2 移动商务的实现技术8.1.3 移动商务的主要商务模式8.1.4 移动商务的安全威胁8.2 移动电子商务安全协议8.2.1 无线应用协议8.2.2 wPKI体系8.2.3 蓝牙技术8.2.4 3G系统的安全体系8.3 移动支付系统安全8.3.1 移动支付概述8.3.2 移动支付框架及安全8.3.3 移动支付的实现习题八第9章 电子商务信息安全实训9.1 实训一路由器的接口及连接9.2 实训二文件安全与保护9.3 实训三黑客攻击与防范9.4 实训四古典密码与破译9.5 实训五数字证书9.6 实训六防火墙9.7 实训七病毒机制分析参考文献

## 章节摘录

插图：5.证书的获取在验证信息的数字签名时，用户必须事先获取信息发送者的公钥证书，以对信息进行解密验证，同时还需要CA对发送者所发的证书进行验证，以确定发送者身份的有效性。

证书的获取可以有以下几种方式。

- 1) 发送者发送签名信息时，附加发送自己的证书。
- 2) 单独发送证书信息的通道。
- 3) 可从访问发布证书的目录服务器获得。
- 4) 或者从证书的相关实体（RA）处获得。

在PKI体系中，可以采取上述的某种或几种方式获得证书。

在发送数字签名的证书的同时，可以发布证书链。

这时，接收者拥有证书链上的每一个证书，从而可以验证发送者的证书。

检验过程是，通过检查发送者证书的发放机构CA，从CA中的目录服务器取得该CA证书，并重复这证书链上的CA根证书的验证。

6.证书和目录查询因为证书都存在周期问题，所以进行身份验证时要保证当前证书是有效而没过期的；另外，还有可能密钥泄露，证书持有者身份、机构代码改变等问题，证书需要更新。

因此在通过数字证书进行身份认证时，要保证证书的有效性。

为了方便对证书有效性的验证，PKI系统提供对证书状态信息的查询，以及对证书撤销列表的查询机制。

CA的目录查询通过LDAP协议，实时地访问证书目录和证书撤销列表，提供实时在线查询，以确认证书的状态。

这种实时性要求是由金融业务或其他电子政务应用的高度敏感性和安全性的高要求所决定的。

7.证书撤销证书在使用过程中可能会因为各种原因而被废止，例如，密钥泄露，相关从属信息变更、密钥有效期中止或者CA本身的安全隐患引起废止等。

因此，证书撤销服务也必须是PKI的一个必需功能。

该系统提供成熟、易用、标准的证书列表作废系统，供有关实体查询，对证书进行验证。

8.密钥备份和恢复密钥的备份和恢复是PKI中的一个重要内容。

因为可能有很多原因造成丢失解密数据的密钥，那么被加密的密文将无法解开，会造成数据丢失。

为了避免这种情况的发生，PKI提供了密钥备份与解密密钥的恢复机制，即密钥备份与恢复系统。

在PKI中密钥的备份和恢复分为CA自身根密钥的备份和恢复和用户密钥。

CA根密钥由于其是整个PKI安全运营的基石，其安全性关系到整个PKI系统的安全及正常运行，因此对于根密钥的产生和备份要求很高。

根密钥由硬件加密模块中加密机产生，其备份由加密机系统管理员启动专用的管理程序执行备份过程。

备份方法是将根密钥分为多块，为每一块生成一个随机口令，使用该口令加密该模块，然后将加密后的密钥块分别写入不同的IC卡中，每个口令以一个文件形式存放，每人保存一块。

恢复密钥时，由各密钥备份持有人分别插入各自保管的IC卡，并输入相应的口令才能恢复密钥。

## <<电子商务信息安全技术>>

### 编辑推荐

《电子商务信息安全技术》：21世纪高职高专规划教材系列

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>