

<<电子商务安全与认证>>

图书基本信息

书名：<<电子商务安全与认证>>

13位ISBN编号：9787040310368

10位ISBN编号：7040310368

出版时间：2011-1

出版对象：高等教育

作者：胡伟雄 编

页数：301

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>

<<电子商务安全与认证>>

内容概要

《电子商务安全与认证》是普通高等教育“十一五”国家级规划教材。

《电子商务安全与认证》从系统工程的视角来研究电子商务安全问题；以完整的框架来介绍电子商务安全的原理、技术和实施方法；从安全威胁、安全风险层面来挖掘电子商务安全需求，选择适用的安全技术来构建电子商务安全防护体系，同时重视电子商务安全管理所起到的作用。

《电子商务安全与认证》全面介绍电子商务密码技术、电子商务认证技术、电子商务认证体系、电子商务安全认证系统、电子商务网络安全、系统安全技术、电子商务安全应用、电子商务安全管理等内容，并通过电子支付、PKI/CA应用、企业网络安全防护等应用案例，帮助读者掌握基本的安全技术及其应用方法。

《电子商务安全与认证》内容丰富，深入浅出，凝聚着作者十多年从事信息网络安全工程项目的经验，可操作性强，适合作为高等学校电子商务专业本科“电子商务安全与认证”课程的教材，也可供相关专业的研究生、从事信息安全工作的研究者和从业者参考。

《电子商务安全与认证》配套光盘中有丰富的教学资源，可以配合教材使用。

书籍目录

第1章 电子商务安全导论1.1 电子商务面临的安全问题1.1.1 信息传输过程中存在的安全问题1.1.2 交易实体的信用安全问题1.1.3 管理安全问题1.2 电子商务的安全需求1.3 电子商务安全的概念1.4 电子商务安全威胁1.4.1 安全威胁的分类1.4.2 常见的电子商务安全威胁1.5 电子商务安全服务1.5.1 常用的电子商务安全服务1.5.2 安全威胁与安全服务的关系1.6 电子商务安全机制1.6.1 网络安全机制1.6.2 电子商务的安全机制1.6.3 安全服务与安全机制的关系1.7 电子商务安全体系1.7.1 电子商务安全框架1.7.2 电子商务安全体系结构第2章 电子商务密码技术2.1 密码学概述2.1.1 密码学的基本概念2.1.2 密码学的发展历程2.1.3 密码体制的分类2.1.4 密码分析基础2.2 古典密码算法2.2.1 代替密码2.2.2 换位密码2.3 对称密钥算法2.3.1 数据加密标准2.3.2 三重数据加密标准2.3.3 国际数据加密算法2.3.4 高级加密标准2.3.5 分组密码的工作模式2.4 公开密钥算法2.4.1 RSA算法2.4.2 椭圆曲线密码算法2.4.3 其他公开密钥算法2.5 量子密码2.6 密钥管理2.6.1 密钥的种类2.6.2 密钥的生成2.6.3 对称密钥的分发2.6.4 密钥协定2.6.5 公开密钥的分发2.7 机密性服务2.7.1 机密性措施2.7.2 机密性机制2.8 网络数据加密技术2.8.1 链路加密2.8.2 节点-节点加密2.8.3 端-端加密2.9 数据加密系统PGP2.9.1 PGP简介2.9.2 PGP加密原理2.9.3 PGP密钥管理2.9.4 PGP的配置和使用第3章 电子商务认证技术3.1 认证服务3.1.1 认证与认证系统3.1.2 认证系统的分类3.1.3 认证系统的层次模型3.2 哈希函数3.2.1 哈希函数的分类3.2.2 MD-5哈希算法3.2.3 安全哈希算法3.3 数字签名3.3.1 数字签名的基本概念3.3.2 RSA签名体制3.3.3 E1Gamal签名体制3.3.4 数字签名标准3.3.5 不可否认签名3.3.6 盲签名3.3.7 双联签名3.4 时间戳3.4.1 时间戳的概念3.4.2 时间戳服务3.5 消息认证3.5.1 基于对称密钥密码体制的消息认证3.5.2 基于公开密钥密码体制的消息认证3.5.3 数据完整性服务3.6 身份认证3.6.1 身份认证的概念3.6.2 口令认证3.6.3 基于个人特征的身份认证3.6.4 基于密钥的认证机制3.6.5 零知识证明3.6.6 身份认证协议3.6.7 认证的密钥交换协议3.7 不可否认服务3.7.1 不可否认服务的类型3.7.2 可信赖的第三方3.7.3 实现不可否认服务的过程3.7.4 信源的不可否认服务3.7.5 传递的不可否认服务第4章 电子商务认证体系4.1 公钥构架体系4.1.1 公钥构架的定义4.1.2 公钥构架的组成4.1.3 公钥构架的应用4.1.4 公钥构架的标准4.2 公钥构架的安全服务4.2.1 公钥构架的核心服务4.2.2 公钥构架的支撑服务4.3 特权管理构架4.3.1 基本概念4.3.2 特权管理构架的总体框架4.3.3 特权管理构架模型4.3.4 特权管理构架与公钥构架的关系4.4 密钥/证书生命周期管理4.4.1 初始化阶段4.4.2 颁发阶段4.4.3 取消阶段4.5 信任模型4.5.1 基本概念4.5.2 交叉认证4.5.3 严格层次结构模型4.5.4 分布式信任结构模型4.5.5 Web模型4.5.6 以用户为中心的信任模型4.6 公钥构架体系结构4.6.1 典型的公钥构架体系结构4.6.2 公钥构架体系的内部组织4.6.3 公钥构架体系的互通性4.7 证书策略和认证惯例声明4.7.1 证书策略4.7.2 认证惯例声明4.7.3 证书策略和认证惯例声明的关系第5章 电子商务安全认证系统5.1 认证系统的建设原则5.2 认证系统建设方式5.2.1 自建模式5.2.2 托管模式5.3 中国金融认证中心简介5.4 中国金融认证中心的体系结构5.4.1 中国金融认证中心的整体结构5.4.2 SE了CA结构5.4.3 Non-SET CA结构5.4.4 RA系统5.5 中国金融认证中心的系统功能5.5.1 中国金融认证中心证书的种类5.5.2 证书的申领5.5.3 证书的审批5.5.4 证书的发放5.5.5 证书的撤销、归档、更新5.5.6 证书作废表的管理5.5.7 认证系统的管理功能5.5.8 认证系统的密钥管理功能5.6 户国金融认证中心的安全体系5.7 户国金融认证中心的运作策略5.8 其他常见的认证系统5.8.1 天威诚信公司5.8.2 VeriSign公司5.8.3 上海市数字证书认证中心第6章 电子商务网络安全6.1 网络安全协议6.1.1 安全套接层协议6.1.2 安全电子交易协议6.1.3 安全套接层协议与安全电子交易协议的比较6.1.4 IPsec6.2 虚拟专用网技术6.2.1 虚拟专用网概述6.2.2 虚拟专用网的安全技术6.2.3 虚拟专用网的隧道协议6.2.4 IPsec VPN与SSL VPN6.3 防火墙技术6.3.1 防火墙概述6.3.2 基本的防火墙技术6.3.3 防火墙网络部署方案6.4 入侵检测与防护6.4.1 入侵检测系统概述6.4.2 入侵检测系统的体系结构6.4.3 入侵检测系统的分类6.4.4 入侵防御系统简介6.4.5 入侵检测系统的部署与应用实例6.5 移动安全6.5.1 移动安全概述6.5.2 移动安全协议和标准6.5.3 无线公钥构架第7章 系统安全技术7.1 操作系统安全技术7.1.1 访问控制技术7.1.2 审计技术7.1.3 漏洞扫描技术7.1.4 加固技术7.1.5 Windows安全技术7.2 计算机病毒及防范技术7.2.1 计算机病毒的定义7.2.2 计算机病毒的种类和特点7.2.3 计算机病毒防范技术7.2.4 计算机病毒的防治7.3 Web安全技术7.3.1 Web传输协议7.3.2 Web服务器端安全7.3.3 Web客户端安全7.4 电子邮件安全7.4.1 电子邮件的安全威胁7.4.2 包子邮件的安全措施7.4.3 电子邮件的安全协议7.5 数据库安全技术7.5.1 数据库加密技术7.5.2 访问控制技术7.5.3 数据库审计技术7.5.4 数据备份与恢复技术第8章 电子商务安全应用8.1 电子支付安全8.1.1 电子支

<<电子商务安全与认证>>

付安全概述8.1.2 电子支付交易安全8.1.3 安全电子支付方式8.2 PKI/CA系统的应用8.2.1 网上银行8.2.2 移动商务8.2.3 B2B交易8.3 企业网络安全实例8.3.1 网络现状与需求分析8.3.2 网络安全设计思路8.3.3 网络安全整体解决方案8.3.4 外联网安全解决方案第9章 电子商务安全管理9.1 电子商务风险管理9.1.1 电子商务风险管理概述9.1.2 电子商务风险评估9.1.3 电子商务风险应对9.2 电子商务安全管理制度9.2.1 电子商务安全管理规章9.2.2 电子商务安全操作规范9.2.3 应急事件及响应9.2.4 电子商务安全培训机制9.3 电子商务法律法规9.3.1 国外电子商务管理立法9.3.2 国内电子商务管理立法9.3.3 电子签名相关法律法规9.4 电子商务安全标准9.4.1 ISO / IEC 270019.4.2 TCSEC9.4.3 ITSEC9.4.4 ISO / IEC 15408 (CC) 9.4.5 ITIL9.4.6 SSE-CMM9.4.7 国内信息安全标准

章节摘录

版权页：插图：假客户是指假扮合法客户来订购产品或服务的那些客户。

例如，用伪造信用卡来骗取免费服务和免费产品；或者提交订单，客户拒不执行订单；或者在收到货物后，客户却拒绝付款。

(2) 拒绝服务拒绝服务是指商家的计算机和网络资源被黑客攻击和消耗殆尽，从而导致无法提供正常的销售服务。

(3) 数据安全问题数据安全问题包括数据被窃取、篡改、丢失和伪造。

其中，数据被窃取是商家面临的一种常见的安全问题。

黑客可以随时、随地作案，而且很难被追踪到。

被窃取的数据则包括商家的商业机密信息、客户的个人信息等。

1.1.2 交易实体的信用安全问题交易实体的信用安全问题主要来自以下3个方面。

1.来自买方的信用安全问题对于个人消费者来说，在进行网络支付时，有可能恶意透支信用卡，或者使用伪造的信用卡来骗取商品和服务；对于集团消费者来说，有可能拖延货款。

以上风险都必须由卖方来承担。

2.来自卖方的信用安全问题卖方不能按质、按量、按时提供消费者所购买的货物，或者不能完全履行与集团消费者签订的合同，造成买方的货款存在风险。

3.抵赖行为买卖双方中的一方或双方对某项交易的全部或部分内容事后抵赖，拒不执行交易中的约定，带来一定的信用风险。

1.1.3 管理安全问题所谓“三分技术、七分管理”，这句话真实地说明了管理在电子商务活动中的重要性。

在电子商务的各个环节中，都必须制定严格的管理制度和规范，并在实施过程中严格执行这些管理制度和规范，才能保证交易的安全、可靠，保护各参与方的利益。

网上交易的管理安全问题是指由于交易流程管理、人员管理、网络系统管理等方面尚不完善所带来的安全风险。

1.交易流程管理安全问题在C2C（Customer to Customer，客户对客户）交易过程中，交易平台（网络商城）不仅要监督买方按时付款，同时还要监督卖方按时提供符合买方要求的货物。

在这些具体的环节上，都存在着大量的管理问题。

如果管理不善，势必造成较大的交易风险。

2.人员管理安全问题人员管理是电子商务管理安全中最为薄弱的环节。

近年来，我国一些单位中出现了内部计算机犯罪，其主要原因是部分工作人员的职业道德修养不高，所在单位的安全教育和管理松懈。

一些单位还存在向竞争对手派出商业间谍或者收买竞争对手的内部管理人员的不良行为，以此窃取对方的账号、密码、机密文件等信息。

<<电子商务安全与认证>>

编辑推荐

《电子商务安全与认证》：普通高等教育“十一五”国家级规划教材·高等学校电子商务专业系列教材。

<<电子商务安全与认证>>

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>