第一图书网, tushu007.com

<<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：9787560974385

10位ISBN编号：7560974384

出版时间：2011-12

出版时间：华中科技大学出版社

作者：唐德权,王六平,苗邯军,张波云

页数：252

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

内容概要

目前电子商务迅猛发展，实现电子商务的关键是要保证商务活动过程中系统的安全性，即应保证在基于Internet的电子交易转变的过程中与传统交易的方式一样安全可靠。
本书主要是围绕电子商务活动的安全性及其保障，针对与电子商务应用相关的基本安全问题，全面介绍电子商务安全的基本理论和关键技术，主要内容包括电子商务的安全问题、体系结构、密码学基础、公钥基础设施（PKD、PKI的体系与功能、认证技术、数字签名、网络安全技术、安全电子交易（SET）协议、安全套接层（SSL）协议、电子商务的主要支付机制、支付交易安全、黑客防范技术、移动电子商务安全技术及电子商务的应用安全等。

本书内容紧贴电子商务的安全技术问题，每章前面都有学习目的、工具器材和学习方式建议，后面附有实训和习题。
本书特别适合高等院校信息安全专业、计算机专业、电子商务专业、通信等专业学生使用；也适合信息管理人员、信息技术人员使用；还可作为相应层次电子商务培训班的教材。

书籍目录

第1章 电子商务安全概述
1.1 电子商务安全问题
1.1.1 安全漏洞
1.1.2 计算机病毒
1.1.3 黑客攻击
1.1.4 网页挂马
1.1.5 网页仿冒
1.2 电子商务面临的安全威胁
1.2.1 安全威胁的类型
1.2.2 电子交易过程中的安全威胁
1.3 电子商务的安全需求
1.3.1 电子交易的安全需求
1.3.2 计算机网络系统的安全
1.4 构造电子商务的安全体系
1.4.1 电子商务的安全体系
1.4.2 电子商务安全技术
1.5 电子商务安全的现状
1.5.1 法律法规
1.5.2 理论研究和技术研发
本章小结
实训一 某网上书店电子商务系统开发
习题
第2章 信息加密技术与应用
2.1 加密技术
2.1.1 数据加密概述
2.1.2 传统加密技术
2.1.3 现代加密技术
2.2 哈希函数
2.2.1 MD5算法
2.2.2 SHA-1算法
2.3 密钥管理技术
2.3.1 密钥管理技术概述
2.3.2 对称密钥的管理
2.3.3 非对称密钥的管理
2.3.4 密钥管理应用
2.3.5 密钥管理系统
2.3.6 密钥产生技术
2.3.7 密钥的分散管理与托管
2.4 安全技术的组合应用
2.4.1 MAC
2.4.2 数字信封
本章小结
实训二 DES和RSA-Tool的使用技巧
习题二
第3章 数字签名与认证技术

3.1 数字签名
3.1.1 数字签名概述
3.1.2 数字签名实现方法
3.1.3 数字签名的算法
3.1.4 数字签名的具体过程
3.1.5 数字签名标准
3.2 Hash摘要和数字时间戳
3.2.1 Hash摘要
3.2.2 数字时间戳
3.3 身份认证
3.3.1 认证的概念
3.3.2 认证方式分类
3.3.3 身份认证的概念
3.3.4 身份认证技术的分类
3.3.5 基于静态口令的身份认证
3.3.6 基于动态一次性口令的身份认证
3.3.7 基于挑战-应答协议的身份认证协议
3.3.8 指纹识别
3.4 报文认证
3.4.1 报文与报文认证
3.4.2 报文认证的分类及实现过程
3.5 认证技术的应用
3.5.1 身份认证一般应用
3.5.2 数字签名的应用示例
本章小结
实训三 安全邮件与数字签名
……
第4章 Internet安全技术与协议
第5章 数字证书及PKI
第6章 安全电子支付机制
第7章 黑客及其防范技术
第8章 安全电子商务系统应用
第9章 移动电子商务安全
参考文献

章节摘录

版权页：插图：（1）网络隐患扫描。
Internet主要采用TCP／IP协议并得到了广泛的应用，使得TCP／IP协议存在许多安全漏洞和隐患，网络隐患扫描就是对安全漏洞和隐患进行防范的技术。
（2）网络安全监控。
（3）内容识别。
（4）访问控制。
（5）防火墙技术。
防火墙是一种用于在两个网络或多个网络之间进行访问控制的技术。
保护电子交易免受非法侵犯，必须采用防火墙技术保证网络的安全。
它在基于Internet的电子交易中起着重要作用。
网络服务层是电子商务系统基本、灵活的网络服各平台。
（6）入侵检测技术。
入侵检测系统（IDS）被定义为对计算机和网络资源的恶意使用行为进行识别和相应处理的系统。
它通过对计算机系统进行监视，提供实时的入侵监测，并采取相应的防护手段。
入侵检测技术是一种主动保护自己免受黑客攻击的一种网络安全技术，能够帮助系统应对网络攻击，提高信息安全基础结构的完整性，被认为是防火墙之后的第二道安全闸门。
2.加密技术层加密技术是电子商务采取的主要安全技术手段，它不仅可以保证通信及存储数据的安全，还可以有效地用于报文认证、数字签名等，以防止种种电子欺骗。
加密技术也是认证技术及其他许多安全技术的基础，是信息安全的核心技术。
3.安全认证层安全认证层中的认证技术是信息安全理论与技术的一个重要方面，也是保证电子商务安全的重要技术之一。
采用认证技术可以直接满足身份认证、信息完整性、不可否认和不可修改等多项电子交易的安全需求，较好地避免了电子交易面临的假冒、篡改、抵赖、伪造等威胁。
4.安全协议层除了各种安全控制技术之外，电子商务的运行还需要一套完善的安全交易协议。
不同交易协议的复杂性、开销、安全性各不相同。
同时，不同的应用环境对协议目标的要求也不尽相同。
目前，比较成熟的协议如下。
（1）安全电子交易（SET，Secure Electronic Transaction）协议，是应用于Internet上的以银行卡为基础进行在线交易的安全标准。
（2）安全套接层（SSL，Secure Sockets Layer）协议，是基于传输层的安全性的一种安全策略，是国际上最早应用于电子商务的一种网络安全协议。
（3）联合电子支付联盟（JEPI，Joint Electronic PaymentInitiative），是为了解决众多协议间的不兼容性而提出来的，是现有HTTP协议的扩展，是在普遍HTTP协议之上增加了PEP（Protocol Extension Protocol）和UPP（Universal Payment Preamble）两层结构而形成的。
其目的不是提出一种新的电子支付手段，而是在允许多种支付系统并存的情况下帮助商家和顾客双方选取一个合适的支付系统。

编辑推荐

《电子商务安全》是普通高等教育“十二五”规划教材和高等院校计算机系列教材之一。

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