<<电子商务信息安全>>

图书基本信息

书名：<<电子商务信息安全>>

13位ISBN编号：9787563814442

10位ISBN编号：7563814442

出版时间：2010-1

出版时间：首都经济贸易大学出版社

作者：蒋汉生 编

页数：233

前言

Internet作为通信技术、网络技术和信息技术的载体与表现形式，呈现了爆炸式的增长方式，而基于Internet的电子商务应用也得到了空前的发展，电子商务从20世纪90年代中期诞生以来，已经走过了十几年的发展历程。

十几年来，安全问题始终是影响其发展的一个瓶颈，可以说电子商务信息安全是电子商务顺利发展的关键，也是难点。

电子商务作为一种全新的业务和服务方式，为全球客户提供了丰富的商务信息、简捷的交易过程和低廉的交易成本，但是电子商务在给人们带来方便的同时，也把人们引进了安全陷阱。

当进行电子商务交易、特别是网络支付的时候，在公共的Intermit网上需要传输消费者和商家的一些机密信息、如用户信用卡号、商家与用户信息和订购信息等，而这些信息一直是网络非法入侵者或黑客的攻击目标。

如何保证电子商务交易的安全性，如何对敏感的个人信息提供机密性保障，如何认证交易双方的合法身份，如何保证数据的完整性和交易的不可否认性等，已经成为制约电子商务发展的瓶颈，也成为：众多学者、研究开发人员、政府人员和管理人员关注的目标。

电子商务信息安全的相关技术既涉及信息加密解密、网络安全协议、防火墙的构建、病毒的防治等，也包括相关管理制度的建立，这是一个涉及范围相当广泛的问题，需要各方的协调配合。

本书共由15章组成，第一章介绍了电子商务信息安全的基本概念，第二章介绍了密码技术和密钥管理，第三章进一步介绍了单钥密码体制和双钥密码体制，第四章介绍了密码技术应用，第五章简单介绍了计算机病毒的基本概念和防治策略，第六章介绍了访问控制与口令认证系统，第七章介绍了防火墙技术，第八章介绍了入侵检测技术，第九章介绍了虚拟专用网技术，第十章介绍了身份证明系统和公钥证书，第十一章介绍了公钥基础设施，第十二章介绍了证书机构，第十三章介绍了个人数字证书的申请和使用，第十四章介绍了两种常见的电子商务安全协议——SSL和SET，第十五章为实验指导，比较详细地介绍了几种常见的信息安全实验。

<<电子商务信息安全>>

内容概要

如今，通过Internet进行的电子商务成为各界人士关注的焦点，由于Internet的开放性和其他各种因素的影响，安全成为电子商务诸多技术中非常重要的环节。
本书作为电子商务信息安全的入门书籍，以通俗的语言阐述了目前电子商务信息安全的主要技术，内容主要包括电子商务信息安全基础、密码学基础、密码技术的应用、计算机病毒、访问控制与口令认证系统、防火墙技术、入侵检测技术、虚拟专用网技术、身份证明系统与公钥证书、公钥基础设施、证书机构、电子商务安全协议和实验指导等。
本书内容丰富，力求以系统的观点和方法来阐述电子商务安全理论，可读性和实践性强。
本书每章开篇都配有实际的引导案例，并于章末辅之相关的班级讨论、自己动手和本章复习，以问题的方式引导读者对各章内容作更深入、广泛的思考和实践。
本书可作为高职高专电子商务专业教材使用，也适合于对电子商务信息安全和网络安全感兴趣的读者。

<<电子商务信息安全>>

书籍目录

1 电子商务信息安全基础 1.1 电子商务的发展 1.2 电子商务信息安全基础 1.3 计算机安全等级2 电子商务安全需求与密码技术 2.1 电子商务的安全需求 2.2 密码技术 2.3 密钥管理技术 2.4 密码体制的理论安全性与实际安全性3 单钥密码体制和双钥密码体制 3.1 单钥密码体制 3.2 双钥密码体制4 密码技术的应用 4.1 数据的完整性和安全 4.2 数字签名 4.3 数字信封 4.4 混合加密系统 4.5 数字时戳5 计算机病毒及其防治 5.1 计算机病毒定义 5.2 计算机病毒的特征 5.3 计算机病毒的分类 5.4 计算机病毒的主要来源 5.5 计算机病毒的防治策略6 访问控制与口令认证系统 6.1 访问控制 6.2 口令认证系统 6.3 个人特征的身份证明技术7 防火墙技术 7.1 什么是防火墙 7.2 防火墙的设计原则 7.3 防火墙的基本组成 7.4 防火墙的分类 7.5 防火墙不能解决的问题8 入侵检测技术 8.1 入侵检测的基本概念 8.2 入侵检测的信息源 8.3 入侵检测的分类 8.4 先进的入侵检测技术9 虚拟专用网（VPN）技术 9.1 什么是VPN？
9.2 VPN的优点 9.3 VPN的基础——隧道协议 9.4 隧道的基本组成 9.5 IPSec 9.6 选择VPN解决方案 9.7 VPN的适用范围 9.8 VPN的分类 9.9 组建VPN应该遵循的设计原则 9.10 VPN应用中的制约因素 9.11 VPN的几种解决方案10 身份证明系统与公钥证书 10.1 身份证明系统 10.2 公钥证书11 公钥基础设施(PKI) 11.1 PKI概述 11.2 密钥管理 11.3 不可否认业务12 证书机构 12.1 证书机构概述 12.2 国内主要证书机构13 个人数字证书的申请和使用 13.1 个人数字证书的申请 13.2 个人数字证书的使用14 电子商务的安全协议 14.1 SSL——提供网上交易安全的协议 14.2 SET——提供安全的电子商务数据交换 14.3 SET与SSL对比 14.4 SET的缺陷15 实验指导 15.1 口令攻击 15.2 数据加密与鉴别 1S.3 数字证书服务及加密认证 15.4 防火墙技术参考文献

章节摘录

插图：1.1 电子商务的发展1.1.1 从电子数据交换到电子商务电子商务可以分为以建立在专用网基础上的电子数据交换(EDI)为代表的传统电子商务和以因特网为基础的现代电子商务。
EDI时代，电子商务系统的建设多半是由大型企业或政府主导的。
现代电子商务则为大、中、小企业应用，尤其为中、小企业应用创造了几乎是相同的、平等的机会。
十几年以前，EDI还是电子商务的主要技术，但仅限于企业之间，即B2B模式。
EDI采用的是“存储一转发”信息传输方式，类似于电子邮件，再加上结构化的信息内容和功能，以保证被传送信息的可审计性和能可靠送达目的地。
EDI的规范、标准十分详尽、全面，几乎涵盖了商业往来所需资料数据的方方面面，因此也就很复杂、烦琐。
全面实现EDI，代价太大，对多数中小企业是个沉重负担，不易推广。
即使是大中型企业，往往在企业内部也只实现EDI规范的部分子集，只在进行国际贸易时，才将数据转换成标准的EDI格式。
同时，由于EDI多半是建立在专用网络上，利用率较低，网络费用昂贵，这就限制了它的广泛应用。
正因如此，传统的电子商务并未有过惊人的快速增长。

编辑推荐

《电子商务信息安全》：21世纪高职高专精品系列规划教材·电子商务专业。

<<电子商务信息安全>>

版权说明