

<<电子商务的安全技术>>

图书基本信息

书名：<<电子商务的安全技术>>

13位ISBN编号：9787508432007

10位ISBN编号：7508432002

出版时间：2005-9

出版时间：中国水利水电出版社

作者：劳帼龄

页数：292

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>

<<电子商务的安全技术>>

前言

电子商务从20世纪90年代中期诞生以来，已经走过了十年的发展历程。

十年来，安全问题始终是影响其发展的一个瓶颈。

这在中国互联网络信息中心所作的历次调查和发布的《中国互联网络调查统计报告》中可见一斑，历次调查，安全问题一直是电子商务用户特别关注的主题。

可以这么说，电子商务安全是电子商务顺利发展的一个关键，也是一个难点。

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。

电子商务是利用计算机通过网络来实现的。

<<电子商务的安全技术>>

内容概要

《注册电子商务工程师（CEBE）认证培训教材·电子商务的安全技术》介绍了电子商务安全防范措施，通过对信息加密技术与应用、数字签名技术与应用、TCP / IP服务与WWW安全、防火墙的构造与选择计算机病毒及其防治、系统评估准则与安全策略以及计算机信息系统安全保护制度的详细介绍，使读者掌握目前先进的电子商务安全技术。

书籍目录

序前言第1章 电子商务安全的现状和趋势1.1 电子商务安全问题1.1.1 安全漏洞1.1.2 病毒感染1.1.3 黑客攻击1.1.4 网络仿冒1.2 触发电子商务安全问题的原因1.2.1 先天原因1.2.2 后天原因1.3 电子商务安全的概念与基本要求1.3.1 电子商务系统安全的构成1.3.2 电子商务安全的需求1.4 电子商务安全的现状1.4.1 法律法规建设1.4.2 理论研究和技术开发1.4.3 网络安全的十大不稳定因素1.5 电子商务安全防治措施1.5.1 技术措施1.5.2 管理措施1.6 电子商务安全举措1.6.1 未来电子商务安全工作1.6.2 加强网络安全的10条建议本章小结复习题第2章 信息加密技术与应用2.1 网络通信中的加密方式2.1.1 链路—链路加密2.1.2 节点加密2.1.3 端—端加密2.1.4 ATM网络加密2.1.5 卫星通信加密2.1.6 加密方式的选择方法2.2 分组加密与高级加密标准2.2.1 密码体制的分类2.2.2 对称加密模式2.2.3 分组密码体制2.2.4 数据加密标准2.2.5 高级加密标准AES2.3 公开密钥加密体制2.3.1 公钥加密模式2.3.2 RSA加密体制2.3.3 背包加密体制2.3.4 ElGamal加密体制2.4 复合型加密体制PGP2.4.1 PGP加密体制简介2.4.2 PGP的加密算法2.4.3 PGP的广泛应用2.4.4 PGP商务安全方案2.5 非密码的安全技术2.5.1 基于信息隐藏的传递技术2.5.2 基于生物特征的鉴别技术2.5.3 基于量子密码的密钥传输技术本章小结复习题第3章 数字签名技术与应用3.1 数字签名的基本原理3.1.1 数字签名的要求3.1.2 数字签名的分类3.1.3 数字签名的使用3.1.4 数字签名与手写签名的区别3.2 常规数字签名方法3.2.1 RSA签名3.2.2 ElGamal签名3.3 特殊数字签名方法3.3.1 盲签名3.3.2 多重签名3.3.3 代理签名3.3.4 定向签名3.3.5 双联签名3.3.6 团体签名3.3.7 不可争辩签名3.4 美国数字签名标准3.4.1 DSS简介3.4.2 数字签名算法 (DSA) 3.5 数字证书技术3.5.1 数字证书简介3.5.2 数字证书的类型3.5.3 利用数字证书实现信息安3.5.4 数字证书的格式3.5.5 数字证书的申请与发放3.5.6 数字证书的分发3.5.7 公钥基础设施PKI3.5.8 CA的结构3.6 电子签名法律3.6.1 电子签名法律概述3.6.2 电子签名法的主要特点3.6.3 电子签名国际立法状况3.6.4 我国数字签名法律本章小结复习题第4章 TCP / IP服务与WWW安全4.1 TCP / IP服务4.1.1 电子邮件4.1.2 文件传输4.1.3 Ljsetnet新闻组4.1.4 远程终端访问4.1.5 万维网访问4.1.6 域名查询4.2 WWW的安全4.2.1 HTTP协议4.2.2 安全套接层协议4.2.3 SET协议4.2.4 WWW服务器的安全漏洞4.2.5 CGI程序的安全性问题4.2.6 Plug-in的安全性4.2.7 ActiveX的安全性4.2.8 cookie的安全性4.3 Java的安全性4.3.1 Java的特点4.3.2 Java的安全性4.3.3 JavaScript的安全性问题本章小结复习题第5章 防火墙的构造与选择5.1 防火墙概述5.1.1 防火墙的概念5.1.2 防火墙设计的基本原则5.2 防火墙的原理5.2.1 防火墙设计的基本准则5.2.2 防火墙的组成5.2.3 防火墙不能对付的安全威胁5.2.4 防火墙的分类5.3 防火墙的选择和使用5.3.1 防火墙的选择原则5.3.2 防火墙产品的分类5.3.3 防火墙产品的介绍5.4 分布式防火墙技术5.4.1 分布式防火墙的产生5.4.2 传统边界式防火墙的固有欠缺5.4.3 分布式防火墙的主要特点5.4.4 分布式防火墙的主要优势5.4.5 分布式防火墙的基本原理5.4.6 分布式防火墙的主要功能5.4.7 肯德基 (KFC) 中国连锁经营店防火墙应用案例本章小结复习题第6章 计算机病毒及其防治6.1 计算机病毒的概念6.2 计算机病毒的分析6.3 计算机病毒的防范6.4 网络病毒的防治6.5 常用的防杀毒软件本章小结复习题第7章 系统评估准则与安全策略第8章 计算机信息系统安全保护制度附录1 参考答案附录2 国际注册电子商务工程师 (CEBE) 认证考核大纲参考文献

章节摘录

2.2 分组加密与高级加密标准密码体制从原理上可分为两大类，即单钥体制（One—key System）和公钥体制（Two-key System）。

单钥体制的加密密钥和解密密钥相同，也称对称加密体制。

本节所介绍分组密码是一种重要的对称加密体制，它是将明文按一定的位长分组，输出也是固定长度的密文。

它的优点十分突出，应用非常广泛。

本节在详细介绍了密码体制以及对称加密模式后，将介绍分组密码加密算法中最具典型意义的数据加密标准DES和高级加密标准AES。

2.2.1 密码体制的分类密码是实现秘密通信的主要手段，是隐蔽语言、文字、图像的特殊符号。

凡是用特殊符号按照通信双方约定的方法把电文的原型隐蔽起来，不为第三者所识别的通信方式称为密码通信。

在计算机通信中，采用密码技术将信息隐蔽起来，再将隐蔽后的信息传输出去，使信息在传输过程中即使被窃取或截获，窃取者也不能了解信息的内容，从而保证信息传输的安全。

密码体制是指密钥空间与相应的加密运算结构，同时还包括了明文和密文的结构特征。

密码体制一般可分为传统密码和现代密码，传统密码包括换位密码、代替密码、转轮机密码等，现代密码又包括序列密码、分组密码、公钥密码、量子密码体制等，现代密码已经广泛应用于军事、商业经济、网络间的通信、电子商务、电子政务等领域。

从不同的角度根据不同的标准，可以把密码分成若干类。

1.按密钥方式划分（1）对称式密码。

收发双方使用相同密钥的密码，叫做对称式密码。

传统的密码都属此类，现代密码中的分组码和序列密码也属于这一类。

（2）非对称式密码。

收发双方使用不同密钥的密码，叫做非对称式密码。

如现代密码中的公开密钥密码就属此类。

2.按应用技术或历史发展阶段划分（1）手工密码。

以手工完成加密作业，或者以简单器具辅助操作的密码，叫做手工密码。

第一次世界大战前的密码主要是这种作业形式。

（2）机械密码。

以机械密码机或电动密码机来完成加解密作业的密码，叫做机械密码。

这种密码从第一次世界大战出现到第二次世界大战中得到普遍应用。

（3）电子机内乱密码。

通过电子电路，以严格的程序进行逻辑运算，以少量制乱元素生产大量的加密乱数，因为其制乱是在加解密过程中完成的而不需预先制作，所以称为电子机内乱密码。

从20世纪50年代末期出现到70年代广泛应用。

（4）计算机密码。

是以计算机编程进行算法加密为特点，适用于计算机数据保护和网络通信等广泛用途的密码。

从20世纪70年代出现到现在广泛应用。

<<电子商务的安全技术>>

编辑推荐

《注册电子商务工程师(CEBE)认证培训教材·电子商务的安全技术》可作为注册电子商务工程师(CEBE)认证考试的教材,也可以作为电子商务专业的概论性课程教材,或作为计算机专业、信息管理与信息系统专业有关电子商务课程的教材,还可供一般工程技术人员、工商管理和社会大众,系统了解和学习电子商务的有关知识。

<<电子商务的安全技术>>

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>