

<<网络信息安全技术>>

图书基本信息

书名：<<网络信息安全技术>>

13位ISBN编号：9787560613048

10位ISBN编号：7560613047

出版时间：2003-11

出版时间：西安电子科技大学出版

作者：周明全

页数：260

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>

<<网络信息安全技术>>

内容概要

全书共分为11章，介绍了计算机网络安全的基本理论和关键技术。

主要内容包括：网络安全、密码技术基础、密钥管理技术、数字签名和认证技术、网络入侵检测原理与技术、Internet的基础设施安全、防火墙技术、电子商务的安全技术及应用、包过滤技术原理及应用、代理服务技术原理及应用、信息隐藏技术。

通过对本书的学习，使读者能够对计算机网络安全有一个系统的了解，掌握计算机网络特别是计算机互联网安全的基本概念，了解设计和维护安全的网络体系及其应用系统的基本手段和常用方法。

本书可作为高等学校计算机软件工程、计算机网络工程、计算机科学与技术、商务信息等有关专业本科生和研究生的教材，也可作为从事网络信息方面人员的参考书。

书籍目录

第1章 网络安全	1.1 网络安全的基础知识	1.1.1 网络安全的基本概念	1.1.2 网络安全的特征
	1.1.3 网络安全的目标	1.1.4 网络安全需求与安全机制	1.2 威胁网络安全的因素
1.2.1 网络的安全威胁	1.2.2 网络安全的问题及原因	1.3 网络安全防护体系	1.3.1 网络安全策略
1.3.2 网络安全体系	1.4 网络安全的评估标准	1.4.1 可信任计算机标准评估准则简介	
1.4.2 国际安全标准简介	1.4.3 我国安全标准简介	习题 第2章 密码技术基础	2.1 密码技术的基本概念
2.2 古典加密技术	2.2.1 置换密码	2.2.2 代换密码	2.3 现代加密技术
习题第3章 密钥管理技术	3.1 密钥的管理内容	3.2 密钥的分配技术	3.2.1 密钥分配实现的基本方法
3.2.2 密钥分配实现的基本工具	3.2.3 密钥分配系统实现的基本模式	3.2.4 密钥的验证	3.3 公钥密码
3.3.1 公钥密码体制的基本概念	3.3.2 公钥密码体制的原理	3.4 RSA算法	3.4.1 RSA算法描述
3.4.2 RSA算法中的计算问题	3.4.3 RSA算法的安全性	3.4.4 RSA的实用性及数字签名	
3.4.5 RSA算法和DES算法	3.5 椭圆曲线密码体制	3.5.1 椭圆曲线	3.5.2 有限域上的椭圆曲线
3.5.3 椭圆曲线上的密码	习题第4章 数字签名和认证技术	4.1 数字签名的基本概念	4.1.1 数字签名概念
4.1.2 数字签名技术应满足的要求	4.1.3 直接方式的数字签名技术	4.1.4 具有仲裁方式的数字签名技术	4.1.5 利用公钥实现数字签名技术原理
4.1.6 其它数字签名技术	4.2 认证及身份验证技术	4.2.1 相互认证技术	4.2.2 单向认证技术
4.2.3 身份验证技术	4.2.4 身份认证系统实例——Kerberos系统	4.3 数字签名标准及数字签名算法	4.3.1 数字签名算法DSS
4.3.2 数字签名算法DSA	4.3.3 数字签名算法HASH	4.3.4 数字签名算法RSA	4.4 其它数字签名体制
4.4.1 基于离散对数问题的数字签名体制	4.4.2 基于大数分解问题的签名体制	4.5 数字证明技术	习题 第5章 网络入侵检测原理与技术
5.1 黑客攻击与防范技术	5.1.1 网络入侵及其原因	5.1.2 黑客攻击策略	5.1.3 网络入侵的防范技术
5.2 入侵检测原理	5.2.1 入侵检测概念	5.2.2 入侵检测模型	5.2.3 IDS在网络中的位置
5.3 入侵检测方法	5.3.1 基于概率统计的检测	5.3.2 基于神经网络的检测	5.3.3 基于专家系统
5.3.4 基于模型推理的攻击检测技术	5.3.5 基于免疫的检测	5.3.6 入侵检测的新技术	5.3.7 其它相关问题
5.4 入侵检测系统	5.4.1 入侵检测系统的构成	5.4.2 入侵检测系统的分类	5.4.3 入侵检测系统的介绍
5.5 入侵检测系统的测试评估	5.5.1 测试评估概述	5.5.2 测试评估的内容	5.5.3 测试评估标准
5.5.4 IDS测试评估现状以及存在的问题	5.6 几种常见的IDS系统	5.7 入侵检测技术发展方向	习题 第6章 Internet的基础设施安全
6.1 Internet安全概述	6.2 DNS的安全性	6.2.1 目前DNS存在的安全威胁	6.2.2 Windows下DNS欺骗
6.2.3 拒绝服务攻击	6.3 安全协议IPSec	6.3.1 IP协议简介	6.3.2 下一代IP-IPv6
6.3.3 IP安全协议IPSec的用途	6.3.4 IPSec的结构	6.4 电子邮件的安全性	6.4.1 PGP
6.4.2 S/MIME	6.5 Web的安全性.....	第7章 防火墙技术	第8章 电子商务的安全技术及应用
第9章 包过滤技术原理及应用	第10章 代理服务技术原理及应用	第11章 信息隐藏技术	附录A 《中华人民共和国计算机信息网络国际联网管理暂行办法》 251
附录B 《中华人民共和国计算机信息网络国际联网安全保护管理办法》 253	附录C 《中华人民共和国计算机信息系统安全保护条例》	参考文献	

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>