

<<网络安全原理与应用>>

图书基本信息

书名：<<网络安全原理与应用>>

13位ISBN编号：9787115134370

10位ISBN编号：7115134375

出版时间：2005-5-1

出版时间：人民邮电出版社

作者：沈苏彬

页数：171

字数：275000

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>

<<网络安全原理与应用>>

内容概要

本书系统地介绍网络安全原理及其典型应用。

本书共包括7章：网络安全概述、密码学导论、身份验证技术及其应用、访问控制技术及其应用、网络攻击检测与网络蠕虫、网络数据安全技术和网络应用安全技术。

本书重点讨论了网络安全的基本概念和组成，传统密码学和公钥密码学，报文身份验证、身份验证协议和Kerberos身份验证系统，访问控制模型和网络防火墙技术，网络攻击检测原理和网络蠕虫的分类方法，安全IP技术和传送层安全技术，网络应用安全体系和万维网安全技术。

本书主要作为高等院校相关专业的本科生和研究生的网络安全课程教材，也可以作为相关专业科研和工程技术人员学习、研究和开发网络安全技术的入门书籍。

<<网络安全原理与应用>>

书籍目录

| | | | | | | | |
|-----------------------------|-----------------------|----------------------------|---------------------|-------------------------------|------------------------------|------------------------------|------------------------|
| 第1章 网络安全概述 | 1.1 信息安全基本概念 | 1.1.1 密码技术 | 1.1.2 通信安全技术 | 1.1.3 计算机安全技术 | 1.1.4 数据安全技术 | 1.1.5 信息安全技术 | 1.2 网络安全基本概念 |
| 1.2.1 网络安全目标 | 1.2.2 网络安全技术组成 | 1.2.3 网络安全关键技术 | 1.3 网络安全的挑战与机遇 | 1.3.1 网络安全的挑战 | 1.3.2 网络安全的公理 | 1.3.3 网络安全的机遇 | 习题 |
| 第2章 密码学导论 | 2.1 密码学基本概念 | 2.1.1 密码学的组成 | 2.1.2 数据加密基本概念 | 2.1.3 密码破译技术 | 2.1.4 加密系统的安全性 | 2.1.5 现代密码学分类 | 2.2 传统密码学概述 |
| 2.2.1 恺撒加密法 | 2.2.2 传统密码学原理 | 2.2.3 数据加密标准(DES) | 2.2.4 高级加密标准(AES) | 2.2.5 RC4加密算法 | 2.2.6 加密操作模式 | 2.3 公钥密码学概述 | 2.3.1 公钥密码学发展动因 |
| 2.3.2 公钥密码学基本原理 | 2.3.3 RSA公钥加密算法 | 2.3.4 Diffie-Hellman密钥生成算法 | 2.3.5 公钥密码体系与密钥管理 | 习题 | 第3章 身份验证技术及其应用 | 3.1 身份验证的基本概念 | 3.1.1 身份验证的发展历史 |
| 3.1.2 身份验证的分类 | 3.1.3 身份验证的内容 | 3.1.4 身份验证的方式 | 3.2 报文身份验证 | 3.2.1 报文身份验证基本概念 | 3.2.2 报文摘要算法MD5 | 3.2.3 安全哈希算法SHA-1 | 3.2.4 哈希函数的报文验证码算法HMAC |
| 3.2.5 生日现象与生日攻击 | 3.2.6 数字签名 | 3.3 身份验证协议 | 3.3.1 身份验证协议基本概念 | 3.3.2 Needham-Schroeder身份验证协议 | 3.3.3 Needham-Schroeder协议的改进 | 3.4 Kerberos身份验证系统 | 3.4.1 基本Kerberos身份验证协议 |
| 3.4.2 完全Kerberos身份验证协议 | 3.4.3 Kerberos系统分析与应用 | 3.5 公钥基础设施(PKI)与X.509建议 | 3.5.1 PKI的必要性 | 3.5.2 PKI的结构 | 3.5.3 证书与X.509建议 | 3.5.4 PKI的实现模型 | 3.5.5 PKI设计建议 |
| 习题 | 第4章 访问控制技术及其应用 | 4.1 访问控制策略与访问控制模型 | 4.1.1 访问控制基本概念 | 4.1.2 自主访问控制策略与强制访问控制策略 | 4.1.3 Bell-LaPadula模型 | 4.1.4 “中国城墙”策略与Brewer-Nash模型 | 4.1.5 Biba完整性模型 |
| 4.1.6 商用安全策略与Clark-Wilson模型 | 4.1.7 基于角色的访问控制模型 | 4.2 网络防火墙 | 4.2.1 网络防火墙基本概念 | 4.2.2 网络层防火墙 | 4.2.3 应用层防火墙 | 习题 | 第5章 网络攻击检测与网络蠕虫 |
| 5.1 网络攻击概述 | 5.1.1 网络攻击的历史和现状 | 5.1.2 网络攻击分类 | 5.1.3 典型的网络攻击 | 5.2 网络攻击检测 | 5.2.1 网络攻击检测概述 | 5.2.2 典型的网络攻击检测系统 | 5.2.3 网络攻击检测分类 |
| 5.2.4 网络攻击的异常检测方法 | 5.3 网络蠕虫 | 5.3.1 恶意代码与网络蠕虫 | 5.3.2 电子邮件蠕虫 | 5.3.3 Windows文件共享蠕虫 | 5.3.4 传统蠕虫 | 习题 | 第6章 网络数据安全技术 |
| 6.1 安全IP及其应用 | 6.1.1 安全IP概述 | 6.1.2 身份验证报头(AH)协议 | 6.1.3 封装安全报体(ESP)协议 | 6.1.4 因特网安全关联与密钥关联协议(ISAKMP) | 6.1.5 因特网密钥交换(IKE)协议 | 6.2 传送层安全技术 | 6.2.1 SSL协议概述 |
| 6.2.2 SSL记录协议 | 6.2.3 SSL握手协议 | 习题 | 第7章 网络应用安全技术 | 7.1 网络应用安全概述 | 7.1.1 网络应用保密性和完整性解决方案 | 7.1.2 网络应用系统的可用性解决方案 | 7.2 电子邮件安全技术 |
| 7.2.1 完美保密(PGP)技术 | 7.2.2 安全MIME | 7.3 万维网(WWW)安全技术 | 7.3.1 万维网面临的安全威胁 | 7.3.2 万维网安全防范技术 | 7.3.3 万维网攻击检测技术 | 习题 | 附录1 参考文献 |
| 附录2 本书引用的RFC一览表 | 附录3 网络安全专用术语中英文对照 | 附录4 本书英文缩写词一览表 | 附录5 本书常用数学符号一览表 | | | | |

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>