<<网络安全与保密>>

图书基本信息

书名：<<网络安全与保密>>

13位ISBN编号：9787560613031

10位ISBN编号：7560613039

出版时间：2003-1

出版时间：西安电子科技大学出版社

作者：胡建伟 主编

页数：359

字数：546000

<<网络安全与保密>>

内容概要

网络安全和密码学是当今通信与计算机领域的热门课题。
本书内容新颖而丰富，主要讲述了基本的密码学原理，各种加／解密算法及其应用，网络协议的安全漏洞和防护措施，系统安全技术，程序代码安全，无线通信网络安全以及欺骗网络等内容。
各章节都提供了大量的参考资料和习题，以供读者进一步学习、研究。
　本书可作为高等院校信息对抗、通信、电子或计算机相关专业的教材，也可作为相关领域的研究人员和专业技术人员的参考书。

<<网络安全与保密>>

书籍目录

第一部分 网络安全综述　第1章 网络安全综述　1.1 网络安全的基本概念和术语　1.2 网络拓扑与安全性　1.2.1 总线网（Bus Network）　1.2.2 拨号网（Dial up Network）　1.2.3 局域网（Local Area Network）　1.2.4 网状网（Mesh Network）　1.2.5 环型网（Ring Network）　1.2.6 星型网（Star Network）　1.3 网络安全的层次结构　1.3.1 物理安全　1.3.2 安全控制　1.3.3 安全服务　1.4 网络安全威胁　1.4.1 网络威胁的类型　1.4.2 威胁的动机（Motives）　1.5 网络攻击　1.5.1 网络攻击的定义　1.5.2 攻击的一般目标　1.5.3 攻击的一般过程　1.5.4 攻击的主要方式　1.6 网络安全模型　1.7 基本安全技术　1.7.1 防火墙（Firewall）　1.7.2 加密（Encryption）　1.7.3 身份认证（Authentication）　1.7.4 数字签名（Digital Signature）　1.7.5 内容检查（Content Inspection）　1.8 网络安全漏洞　1.8.1 物理安全性　1.8.2 软件安全漏洞　1.8.3 不兼容使用安全漏洞　1.8.4 选择合适的安全哲理　1.8.5 寻找漏洞简述　参考资料第二部分 密码学基础　第2章 对称密码学　2.1 前言　2.1.1 密钥加／解密系统模型　2.1.2 古典密码　2.2 数据加密标准（DES）　2.2.1 分组密码简介　2.2.2 DES的历史　2.2.3 DES算法的描述　2.2.4 DES工作模式　2.2.5 三重DES　2.3 A5算法　2.3.1 序列密码简介　2.3.2 A5算法　2.4 其它对称密码算法　2.4.1 IDEA　2.4.2 Blowfish算法　2.4.3 GOST算法　2.4.4 RC5算法　2.4.5 PKZIP算法　习题　参考资料　第3章 单向散列函数　3.1 MD5算法　3.1.1 算法　3.1.2 举例　3.2 安全散列函数（SHA）　3.2.1 算法　3.3.2 举例　3.2.3 SHA-1与MD5的比较　3.3 消息认证码（MAC）　习题　参考资料　第4章 公钥密码系统　4.1 RSA密码系统　4.2 Diffie-Hellman密钥交换　4.2.1 Diffie-Hellman算法　4.2.2 中间人攻击　4.2.3 认证的Diffie-Hellman密钥交换　4.2.4 三方或多方Diffie-Hellman　4.3 数字签名　4.3.1 基本概念　4.3.2 数字签名算法　4.3.3 RSA签名方案　4.3.4 其它数字签名方案　习题　参考资料 第三部分 网络安全应用　第5章 因特网与TCP／IP安全　5.1 TCP／IP协议栈　5.2 互联网地址　5.3 协议封装　5.4 IP协议　5.5 TCP协议　5.5.1 端口号　5.5.2 TCP安全缺陷　5.5.3 IP欺骗攻击　5.5.4 TCP状态转移图和定时器　5.5.5 网络攻击签名检测　5.5.6 总结　5.6 UDP协议　5.7 ARP／RARP协议　5.8 ICMP协议　5.8.1 ICMP报文类型　5.8.2 Smurf攻击　5.9 网络服务的安全性　5.9.1 远程登录　5.9.2 文件传输协议　5.9.3 域名系统（DNS）　习题　参考资料　第6章 VPN与IPSec　6.1 VPN定义　6.2 VPN优势　6.3 VPN的安全考虑　6.4 常见VPN应用环境　6.5 VPN安全策略　6.6 VPN数据安全性　6.6.1 认证（Authentication）　6.6.2 加密（Encryption）　6.6.3 完整性（Integrity）　6.7 VPN协议　6.7.1 PPTP　6.7.2 L2TP　6.7.3 IPSec　6.8 IPSec协议　6.8.1 安全关联（Security Association）　6.8.2 SA管理的创建和删除　6.8.3 SA参数　6.8.4 安全策略　6.8.5 选择符　6.8.6 IPSec模式……　第7章 SSL和TLS第四部分 系统安全机制　第8章 身份认证及其应用　第9章 访问控制和系统审计　第10章 防火墙技术　第11章 入侵检测系统第五部分 代码安全　第12章 安全编程　第13章 移动代码安全　第14章 病毒与数据安全第六部分 其它安全主题　第15章 无线通信网的安全　第16章 蜜罐主机和欺骗网络

<<网络安全与保密>>

编辑推荐

《面向21世纪高等学校信息工程类专业规划教材•网络安全与保密》可作为高等院校信息对抗、通信、电子或计算机相关专业的教材，也可作为相关领域的研究人员和专业技术人员的参考书。

版权说明