

<<网络安全技术及应用>>

图书基本信息

书名：<<网络安全技术及应用>>

13位ISBN编号：9787121091957

10位ISBN编号：712109195X

出版时间：2009-8

出版时间：电子工业出版社

作者：郑秋生 主编

页数：266

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>

## <<网络安全技术及应用>>

### 内容概要

随着信息技术与通信网络技术的迅猛发展，计算机网络正面临着前所未有的安全性挑战，网络安全的攻击、防御、保障技术也日新月异。

本书主要从网络安全基础理论、典型攻击技术、安全防御技术及网络安全新技术四个方面，系统地阐述密码学基础理论与公钥基础设施体系，网络攻击方法及计算机病毒，防火墙应用与入侵检测，以及近年来涌现的可信计算与安全风险评估等新理论、新技术、新方法。

本书以网络安全技术的应用性为主要特色，内容阐述深入浅出、问题分析清晰透彻，除了系统地介绍相关技术与理论外，每章还有具体的应用实例及实验环节部分，可进一步加深读者对内容的理解和掌握。

本书可以作为高等院校计算机科学与技术、信息安全、网络工程等相关专业本科生和专科生的教材或参考书，也可作为从事网络安全工程系统设计、应用开发、部署与管理工作的技术人员的高级技术人员的培训参考书。

## &lt;&lt;网络安全技术及应用&gt;&gt;

## 书籍目录

第1章 网络安全概述 1.1 网络安全的内涵和属性 1.1.1 网络安全的内涵 1.1.2 网络安全的属性 1.2 网络安全的威胁 1.2.1 网络系统软件漏洞 1.2.2 典型恶意攻击方法 1.3 网络安全策略、安全服务与安全机制 1.3.1 网络安全策略 1.3.2 网络安全服务 1.3.3 网络安全机制 1.4 网络安全体系结构 1.4.1 OSI安全体系结构 1.4.2 OSI安全服务的分层配置 1.4.3 OSI安全服务与安全机制的关系 1.5 网络信息安全的评价标准 1.5.1 可信计算机系统评估准则 1.5.2 信息技术安全性评估准则 1.5.3 信息技术安全性评估通用准则 1.5.4 我国国家标准《计算机信息系统安全保护等级划分准则》 1.6 我国网络信息安全的相关法规 1.7 小结 习题第2章 密码学应用基础 2.1 概述 2.1.1 密码学发展历史 2.1.2 密码学基本术语 2.1.3 密码体制分类 2.2 私钥密码体制 2.2.1 简化DES(S-DES) 2.2.2 DES简介 2.2.3 高级加密标准AES 2.2.4 分组密码工作模式 2.3 公钥密码体制 2.3.1 概述 2.3.2 RSA加密体制 2.3.3 RSA签名体制 2.4 杂凑函数 2.4.1 消息认证码 2.4.2 一般杂凑函数 2.4.3 SHA-1算法 2.5 密码算法应用实例——PGP 2.5.1 PGP提供的安全服务简介 2.5.2 PGP密钥管理机制简介 2.5.3 PGP加密实例 2.6 实验：PGP加密并签名邮件 2.7 小结 习题第3章 公钥基础设施PKI 3.1 概述 3.1.1 什么是PKI 3.1.2 为什么需要PKI 3.1.3 PKI的发展与应用 3.2 PKI组成 3.2.1 PKI系统结构 3.2.2 认证中心 3.2.3 注册中心 3.2.4 最终实体 3.3 数字证书及管理 3.3.1 证书格式 3.3.2 证书的申请 3.3.3 证书生成 3.3.4 证书发布 3.3.5 证书撤销 3.3.6 证书更新 3.3.7 证书归档 3.3.8 用户证书存储 3.3.9 数字证书的使用 3.4 密钥管理 .....第4章 网络攻击技术第5章 计算机病毒及恶意代码第6章 操作系统安全第7章 防火墙及其应用第8章 入侵检测系统第9章 网络安全新技术及应用参考文献

章节摘录

第1章 网络安全概述 1.1 网络安全的内涵和属性 1.1.1 网络安全的内涵 21世纪是信息时代，网络已经成为人们快速、全面获取信息的主要渠道，成为人们日常生活和工作不可或缺的组成部分。

人们在充分享受网络带来巨大便利的同时，也深刻感受到网络安全事件和黑客攻击的烦恼。

网络安全（Network Security）涉及计算机科学、通信技术、密码理论、信息论等多个学科，因此迄今为止，学术界对网络安全仍没有一个统一的定义。

要了解网络安全的内涵，首先要了解计算机网络的概念。

计算机网络是地理上分散的多台自主计算机互联的集合。

从该定义中我们可以了解到计算机网络安全涉及的内容，包括计算机主机软硬件系统安全、通信系统安全，以及各种网络应用和服务的安全。

计算机是网络的基本组成元素，现代数据处理系统都是建立在计算机网络基础上的。

因此，网络安全的研究内容也包括计算机信息系统安全。

国际标准化组织（ISO）将计算机信息系统安全定义为：“为数据处理系统建立和采用的技术和管理的安全保护，保护计算机硬件、软件和数据不因偶然和恶意的原因遭到破坏、更改和泄露。

”网络是信息的重要载体，因此从信息系统特点和运行过程出发，网络安全的研究内容可大致分为四个方面：实体安全、运行安全、数据安全和管理安全。

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>