

<<信息安全原理与技术>>

图书基本信息

书名：<<信息安全原理与技术>>

13位ISBN编号：9787113099459

10位ISBN编号：7113099459

出版时间：2009-5

出版时间：蒋朝惠、武彤、王晓鹏、等 中国铁道出版社 (2009-05出版)

作者：蒋朝惠 等著

页数：437

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>

<<信息安全原理与技术>>

内容概要

《普通高等学校计算机科学与技术专业规划教材：信息安全原理与技术》以网络传输安全（线）和结点存储安全（点）为主线，重点介绍了网络安全、系统安全和应用安全等方面的基本概念、原理与技术。

主要内容包括信息安全的概念、威胁、发展过程和典型信息安全保障模型，开放系统互连（OSI）、Internet（TCP/IP）和信息系统安全体系结构，访问控制、防火墙、物理隔离、安全审计、入侵检测、虚拟专用网（VPN）、计算机病毒防治、网络攻击与防范、无线通信安全等网络安全技术，操作系统、数据库系统等系统安全技术，Web站点、电子邮件和电子商务等应用程序安全技术；数据备份与灾难恢复技术、计算机取证技术等。

《普通高等学校计算机科学与技术专业规划教材：信息安全原理与技术》内容丰富，深入浅出，既有理论方面的知识，又有实用技术，还包括一些最新的学科研究热点技术。

《普通高等学校计算机科学与技术专业规划教材：信息安全原理与技术》适合作为信息安全、计算机、通信工程、网络工程等专业的本科生教材，也可供企事业单位的网络管理人员、安全维护人员和系统管理人员以及其他相关科研与工程技术人员参考，还可供相关专业研究人员学习。

<<信息安全原理与技术>>

作者简介

蒋朝惠教授，硕士生导师，现任贵州大学计算机科学与信息学院信息系主任，贵州大学学位委员会委员，兼任“贵阳市城市数字化管理及应急指挥系统建设”项目的专家组成员。

曾在贵州工业大学软件技术研究所专职从事大型数据库Oracle和MIS / MRPII / ERP的应用研究与开发工作近10年。

曾作为中组部、科技部、教育部和中科院等单位发起并资助的“西部之光”访问学者，在北京邮电大学信息安全中心工作与学习1年，期间参与起草了教育部组织编写的“全国高校本科信息安全专业规范”和“我国信息安全学科专业发展战略研究”两个报告。

主持完成了省部级纵向课题4项、大中型横向课题9项，发表论文近40篇(其中核心期刊16篇，EI收录2篇)。

主要研究方向：网络与信息安全、信息共享与系统集成、数字城市 / 社区。

书籍目录

第1章 信息安全概述1.1 信息安全概念1.1.1 信息安全的定义1.1.2 信息安全的基本属性1.1.3 信息安全与网络安全的区别1.2 信息安全威胁1.2.1 信息系统面临的威胁及分类1.2.2 威胁的表现形式和构成威胁的因素1.3 信息安全发展过程1.3.1 信息安全发展的3个阶段1.3.2 主流技术发展1.3.3 信息安全发展趋势1.4 信息安全保障体系1.4.1 信息安全保障体系概述1.4.2 典型的信息安全保障模型习题第2章 信息安全体系结构2.1 开放系统互连安全体系结构2.1.1 OSI安全体系概述2.1.2 OSI的安全服务2.1.3 OSI的安全机制2.1.4 OSI的安全服务与安全机制之间的关系2.1.5 在OSI层中的安全服务配置2.1.6 OSI安全体系的安全管理2.2 Internet安全体系结构2.2.1 TCP / IP协议安全概述2.2.2 Internet安全体系结构2.2.3 IPSec安全协议2.2.4 IPSec密钥管理2.2.5 IPSec加密和验证算法2.2.6 OSI安全体系到TCP / IP安全体系的影射2.3 信息系统安全体系框架2.3.1 信息系统安全体系框架2.3.2 技术体系2.3.3 组织机构体系2.3.4 管理体系习题第3章 访问控制与防火墙3.1 访问控制3.1.1 访问控制概述3.1.2 自主访问控制技术3.1.3 强制访问控制技术3.1.4 基于角色的访问控制技术3.1.5 基于任务的访问控制技术3.1.6 基于对象的访问控制技术3.2 防火墙3.2.1 防火墙技术概述3.2.2 常用的防火墙技术3.2.3 防火墙的实现技术、性能与功能指标3.2.4 防火墙的局限性和发展3.3 物理隔离3.3.1 物理隔离概述3.3.2 物理隔离的原理、分类和发展趋势3.3.3 物理隔离网闸的原理与特点习题第4章 安全审计与入侵检测4.1 安全审计4.1.1 安全审计概念4.1.2 安全审计目的4.1.3 安全审计内容4.1.4 安全审计分类和过程4.1.5 审计日志管理4.1.6 安全审计系统的组成、功能与特点4.2 入侵检测4.2.1 入侵检测概述4.2.2 入侵检测方法4.2.3 入侵检测系统的部署4.2.4 入侵检测技术的发展4.2.5 与入侵检测有关的新技术习题第5章 网络通信安全5.1 虚拟专用网5.1.1 VPN概述5.1.2 VPN的实现技术5.1.3 VPN的隧道协议5.1.4 MPLS VPN技术5.1.5 VPN应用解决方案5.2 无线通信安全5.2.1 无线通信的威胁与防范对策5.2.2 无线通信的安全机制5.2.3 无线VPN技术5.3 网络攻击与防范5.3.1 网络攻击概念及攻击者简介5.3.2 网络攻击的目的与步骤5.3.3 常见的网络攻击与防范方法5.4 计算机病毒及防治5.4.1 计算机病毒概述5.4.2 计算机病毒原理5.4.3 计算机病毒防治技术5.4.4 计算机病毒防范策略5.4.5 防病毒过滤网关系统习题第6章 系统安全6.1 操作系统安全6.1.1 操作系统安全概述6.1.2 操作系统的一般加固方法6.1.3 Windows安全6.1.4 UNIX安全6.1.5 Linux安全6.2 数据库安全6.2.1 数据库安全概述6.2.2 数据库安全技术6.2.3 数据库备份与恢复6.2.4 数据库安全实例习题第7章 应用安全7.1 Web站点安全7.1.1 Web站点的安全威胁7.1.2 Web站点的安全措施7.1.3 Web站点自动恢复技术7.2 电子邮件安全7.2.1 电子邮件安全概述7.2.2 安全的电子邮件系统7.3 电子商务安全7.3.1 电子商务安全概述7.3.2 PKI / PMI技术7.3.3 安全电子交易协议7.3.4 安全套接层协议7.3.5 SET与SSL协议比较7.4 应用程序安全7.4.1 应用程序的安全问题7.4.2 安全程序的开发7.4.3 开发工具的安全特性习题第8章 数据备份与恢复8.1 数据备份概述8.1.1 数据备份的作用与意义8.1.2 数据备份定义8.1.3 数据备份类型8.1.4 常用备份设备8.2 数据备份技术8.2.1 直接附加存储(DAS)8.2.2 网络附加存储(NAS)8.2.3 存储区域网(SAN)8.2.4 双机备份技术8.2.5 其他备份技术8.3 灾难恢复技术8.3.1 灾难恢复的作用与意义8.3.2 灾难恢复的定义8.3.3 灾难恢复计划8.3.4 灾难恢复技术8.4 企业级备份与恢复系统软件8.4.1 Symantec备份与恢复系统8.4.2 CA备份与恢复系统习题第9章 计算机取证9.1 电子证据9.2 计算机取证的概念9.3 计算机取证的原则与步骤9.3.1 计算机取证的基本原则9.3.2 计算机取证的一般步骤9.4 计算机取证技术9.4.1 基本的取证技术9.4.2 基于IDS的取证技术9.4.3 基于蜜罐的取证技术9.5 常用的取证工具习题参考文献

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>