

<<信息安全技术及应用实验>>

图书基本信息

书名：<<信息安全技术及应用实验>>

13位ISBN编号：9787030249609

10位ISBN编号：7030249607

出版时间：2009-9

出版时间：科学出版社

作者：蔡红柳，刘海燕 主编

页数：361

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>

前言

计算机教材建设是计算机专业教学工作的重要组成部分，高质量的教材是培养高素质人才的基本保证，是体现教育特色的知识载体和教学的基本工具，直接关系到计算机专业教育能否为一线岗位培养符合要求的高级应用型人才。

教育部也把教材建设作为衡量高等院校深化教育教学改革的重要指标，作为检验各院校人才培养工作的标准。

近年来，许多院校都十分重视计算机专业教材建设工作，编写和出版了一批质量较高的精品教材，但仍然远远满足不了应用型教育发展的需要，所以我们组织了由全国高校计算机专业的专家教授组成的国家“十一五”高等院校计算机应用型规划教材课题研究组，通过对应用型本科院校和高职高专院校计算机应用技术专业全面、细致的调研和讨论，并结合我国当前的教学现状，编写了本丛书。

丛书突出系统性、科学性和实践性，以培养社会需求的计算机应用型专门人才为宗旨。

丛书特色课程体系的系统性：注重教学内容和体系的创新本丛书根据教育部颁布的应用型专门人才培养目标来编写，适合应用型本科院校和高职高专院校的教学需求和教学特色。

基础理论型课程体现以应用为目的，以必需、够用为度，以讲清概念、强化应用为教学重点；专业技术型课程强调实用性，以满足社会需求为目标，以强化实践操作为教学重点。

教学方法的先进性：加强全方位的教学配套资源建设本丛书针对计算机专业教学工作量大、课时多、讲授课程种类全的特点，注重资源和手段的改革，并逐步建立专门的论坛网站，为计算机专业教学提供一个现代化的平台，包括教材推荐和评论、学生提问和教师答疑、教师课程教学博客、教学论文发表、教学实验基地信息发布等功能。

<<信息安全技术及应用实验>>

内容概要

本书以信息安全理论与技术为基础,全面介绍信息安全的基本原理、技术及应用。

主要内容包括信息加密技术、认证技术、密钥管理与公钥基础设施、访问控制与网络隔离技术、Internet的数据安全技术、信息系统安全检测技术、恶意程序及防范技术、网络攻击与防范技术等。

本书注重理论与实践相结合,在介绍概念、原理与技术的同时,给出代表性运行方案和应用实例。每章都配有实验和习题,所有实验均给出了具体的操作过程,目的是让读者在理解、掌握基本原理和技术的基础上,巩固所学知识并快速掌握其实际应用。

本书可作为信息管理与信息系统、计算机科学、通信工程、信息工程等专业信息安全课程的教材,也可作为计算机培训学校的教材以及信息安全技术人员和自学者的参考书。

<<信息安全技术及应用实验>>

书籍目录

第1章 概述 1.1 信息安全概述 1.2 信息系统安全体系结构 1.3 信息系统安全的防御策略 1.4 安全评估标准 1.5 小结 1.6 习题第2章 信息加密技术 2.1 密码技术概述 2.2 对称密钥密码算法 2.3 非对称密钥密码算法 2.4 信息加密传输 2.5 小结 2.6 习题第3章 认证技术 3.1 概述 3.2 消息认证 3.3 认证协议 3.4 数字签名 3.5 身份认证 3.6 小结 3.7 习题第4章 密钥管理与公钥基础设施 4.1 密钥管理 4.2 公钥基础设施 4.3 Windows 2000的PKI 4.4 小结 4.5 习题第5章 访问控制与网络隔离技术 5.1 访问控制技术 5.2 防火墙技术 5.3 物理隔离技术 5.4 小结 5.5 习题第6章 Internet的数据安全技术 6.1 IPSec与网络层安全 6.2 SSL与传输层安全 6.3 Kerberos认证系统 6.4 PGP与电子邮件安全 6.5 小结 6.6 习题第7章 信息系统安全检测技术 7.1 入侵检测技术 7.2 漏洞检测技术 7.3 审计追踪 7.4 小结 7.5 习题第8章 恶意程序及防范技术 8.1 恶意程序 8.2 病毒 8.3 蠕虫 8.4 木马 8.5 小结 8.6 习题第9章 网络攻击与防范技术 9.1 网络攻击概述 9.2 常见的网络攻击技术 9.3 网络攻击技术的演变 9.4 小结 9.5 习题附录A 综合实验 附录B 习题参考答案

<<信息安全技术及应用实验>>

章节摘录

插图：(1) 系统安全，即实体安全和运行安全。

实体安全。

保护计算机设备、设施（含网络）以及其他媒体免遭地震、水灾、火灾、有害气体和其他环境事故（如电磁污染等）破坏的措施、过程。

特别是避免由于电磁泄漏产生信息泄漏，从而干扰他人或受他人干扰。

实体安全包括环境安全、设备安全和介质安全3方面。

运行安全。

为保障系统功能的安全实现，提供一套安全措施（如风险分析、审计跟踪、备份与恢复、应急等）来保护信息处理过程的安全。

它侧重于保证系统正常运行，避免因系统的崩溃和损坏而对系统存储、处理和传输的信息造成破坏和损失。

风险分析是指为了使计算机信息系统能安全地运行，首先了解影响计算机信息系统安全运行的诸多因素和存在的风险，从而进行风险分析，找出克服这些风险的方法。

审计跟踪是利用计算机信息系统所提供的审计跟踪工具，对计算机信息系统的工作过程进行详尽的跟踪记录，同时保存好审计记录和审计日志，保证计算机信息系统安全可靠地运行。

这就要求系统管理员要认真负责，切实保存、维护和管理审计日志。

应急措施和备份恢复应同时考虑。

首先要根据所用信息系统的功能特性和灾难特点制定包括应急反应、备份操作、恢复措施3方面内容的应急计划，一旦发生灾害事件，就可按计划方案最大限度地恢复计算机系统的正常运行。

(2) 系统中的信息安全。

避免攻击者利用系统的安全漏洞进行窃听、冒充、诈骗等有损于合法用户的行为，即通过对用户权限的控制、利用数据加密等技术确保信息不被非授权者获取和篡改。

防止信息被故意地或偶然地非授权泄漏、更改、破坏或使信息被非法的系统辨识以及控制，即确保信息的完整性、保密性、可用性和可控性。

信息安全包括操作系统安全、数据库安全、网络安全、病毒防护、访问控制、加密与认证等方面。

(3) 管理安全，即用综合手段对信息资源和系统安全运行进行有效管理。

总之，信息安全的目的是在安全法律、法规、政策的支持与指导下，通过采用合适的安全技术与安全管理措施，维护计算机信息安全。

信息安全应当保障计算机及其相关的设备、设施（含网络）的安全，运行环境的安全，保障信息的安全，保障计算机功能的正常发挥，以维护计算机信息系统的安全运行。

<<信息安全技术及应用实验>>

编辑推荐

《信息安全技术及应用实验(第2版)》：以信息安全理论与技术为基础，全面介绍信息安全的基本原理、技术及应用。

由著名军事学院长期从事信息安全教学理论与实践研究的信息安全专家策划和编写。

“理论与实践”相结合，提供多个有针对性的实验，全面提升综合应用能力。

内容全面，通俗易懂，紧追时代前沿。

从书特色：课程体系的系统性：注重教学内容和体系的创新；教学方法的多样性：加强全方位的教学配套资源建设；教学内容的先进性：力求介绍最新的技术和方法；理论与实践并重：阐明基础理论，强调实践应用；易教易学：创新体例，合理布局，通俗易懂。

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>