

<<计算机系统安全>>

图书基本信息

书名：<<计算机系统安全>>

13位ISBN编号：9787040220735

10位ISBN编号：7040220733

出版时间：2007-11

出版范围：高等教育

作者：曹天杰

页数：324

字数：470000

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>

<<计算机系统安全>>

前言

计算机在政治、军事、金融、商业等部门的应用越来越广泛，社会对计算机网络信息系统的依赖也越来越大，安全可靠的网络空间已经成为支撑国民经济、关键性基础设施以及国防的支柱。

随着全球安全事件的逐年增多，确保网络信息系统的安全已引起世人的关注，信息安全在各国都受到了前所未有的重视。

“9·11”之后，美国联邦调查局所属的关键性基础设施保护中心发布了《关于网络空间安全的国家战略》的报告，明确地将信息安全提升到了关系国家安全的战略高度，“信息安全+国土安全=国家安全”正逐渐得到社会的认同。

我国正逐步形成一个完善的统一的安全保障体系，成立了国家计算机网络应急处理协调中心、国家计算机病毒应急处理中心、国家计算机网络入侵防范中心、信息安全国家重点实验室等一批国家级机构。

信息安全、信息对抗、密码学等专业已开始在许多高校及科研院所招生，并开设了“计算机系统安全”、“密码学”等相关课程，但目前我国信息安全人才依然缺乏，内容系统全面反映最新进展的优秀本科信息安全教材还不多见。

根据“计算机系统安全”的教学需要，我们从2000年开始编写讲义，在多年讲授该课程的基础上，不断充实改进，完成了本教材。

安全的概念是与时俱进的，历经了可靠性、保密、保护，而发展到今天的信息保障。

本书从技术的角度介绍了信息安全保障体系，从管理的角度介绍了风险管理，并进一步强调系统安全是一个动态的整体的安全。

本书内容全面、系统，涉及了计算机系统安全的主要方面，如物理安全、运行安全（风险分析、审计跟踪、备份与恢复、应急）、信息安全（网络安全、访问控制、认证等）。

全书分十三章：计算机系统安全概述、计算机系统的物理安全、计算机系统的可靠性、密码学基础、消息认证与数字签名、公开密钥基础设施PKI、身份认证、访问控制、防火墙、攻击与应急响应、入侵检测、IP安全、安全套接层（SSL）协议。

<<计算机系统安全>>

内容概要

本书为普通高等教育“十一五”国家级规划教材，面向应用型本科层次的高校。

本书在第一版的基础上进行了细致和严谨的修改，全书分14章，涵盖了密码学、网络安全和系统安全的主要内容。

本书从三个层次讲述计算机系统安全的知识：第一层次是理论知识，这一层次主要包括信息安全相关的基本概念、密码学与安全协议的基本知识、网络攻防的原理、访问控制模型等。

第二层次是安全应用，包括攻防工具的使用、安全管理与配置。

第三层次是安全编程，主要是利用编程技术编写攻防工具，实现信息系统的安全。

本书可作为计算机科学与技术、电子信息科学与技术等专业“计算机系统安全”、“网络安全”课程的教材，也可供从事信息安全管理、开发、服务等工作的人员参考。

本书有配套的多媒体课件、网络攻防案例库供读者下载。

<<计算机系统安全>>

书籍目录

第一章 计算机系统安全概述 1.1 计算机系统安全的概念 1.1.1 世界范围内日益严重的安全问题 1.1.2 计算机系统安全的概念 1.1.3 国内外计算机系统安全标准 1.2 安全威胁 1.2.1 安全威胁的概念及分类 1.2.2 威胁的表现形式 1.3 安全模型 1.3.1 P2DR安全模型 1.3.2 PDRR安全模型 1.4 风险管理 1.4.1 风险管理的基本概念 1.4.2 风险管理的生命周期 1.5 安全体系结构 1.5.1 安全策略的概念 1.5.2 安全策略的组成 1.5.3 安全体系结构 习题一第二章 计算机系统的物理安全 2.1 物理安全概述 2.2 环境安全 2.3 设备安全 2.3.1 设备安全的保护内容 2.3.2 TEMPEST技术 2.3.3 电子战系统 2.4 介质安全 习题二第三章 计算机系统的可靠性 3.1 计算机系统可靠性的概念 3.2 容错系统的概念 3.2.1 容错的概念 3.2.2 容错系统工作过程 3.3 硬件容错 3.3.1 硬件备份 3.3.2 数据备份 3.3.3 双机容错系统 3.3.4 双机热备份 3.3.5 三机表决系统 3.3.6 集群系统 3.4 软件容错 3.5 磁盘阵列存储器的编码容错方案 习题三第四章 密码学基础 4.1 密码学概述 4.1.1 加密和解密 4.1.2 对称算法和公开密钥算法 4.1.3 随机序列与随机数 4.1.4 密码分析 4.1.5 密码协议 4.2 传统密码学 4.2.1 置换密码 4.2.2 代换密码 4.2.3 一次一密密码 4.3 分组密码 4.3.1 代换—置换网络 4.3.2 数据加密标准 4.3.3 高级加密标准 4.3.4 工作模式 4.4 公钥密码 4.4.1 单向陷门函数 4.4.2 RSA算法 4.5 密钥管理 习题四第五章 消息认证与数字签名第六章 公钥基础设施第七章 身份认证第八章 访问控制第九章 防火墙第十章 攻击与应急响应第十一章 入侵检测第十二章 计算机取证第十三章 IPSec第十四章 TLS协议参考实验参考文献

<<计算机系统安全>>

章节摘录

插图：

<<计算机系统安全>>

编辑推荐

<<计算机系统安全>>

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>