

<<计算机系统安全原理与技术>>

图书基本信息

书名：<<计算机系统安全原理与技术>>

13位ISBN编号：9787111258568

10位ISBN编号：7111258568

出版时间：2009-2

出版时间：陈波、于冷、肖军模 机械工业出版社 (2009-02出版)

作者：陈波等著

页数：387

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>

<<计算机系统安全原理与技术>>

前言

信息安全技术的发展日新月异,新思想和新方法不断产生,教学内容必须跟踪新技术的发展。同时,信息安全是一个整体概念,解决某一个安全问题常常要综合考虑硬件、系统软件、应用软件、网络协议、评估、管理等多个层次的安全问题。

“计算机安全”是信息安全课程体系中的一门重要课程,也是一门直接面向应用、实践性很强的课程,教学中需要重视理论的讲授,使学生掌握解决问题的基本理论和技术,还要强调实验教学,培养学生解决安全问题的实践应用能力。

本书第1版自2006年出版以来,得到了许多读者的鼓励和很好的建议,因此,结合信息安全技术的发展,在第1版教材基础上,进行了认真全面的修订。

在第2章中增加了高级加密标准AES的介绍,散列函数一节删除了MD5算法,改为SHA算法的介绍;第3章中,对可信计算与安全芯片一节作了新技术的补充;第4章中修改了存储保护的内容,Windows系统安全的介绍围绕Windows XP / Vista展开,内容进行了重新组织;第5章中防火墙及入侵检测的介绍增加了实例,使得学生更加容易理解较深奥的这部分原理;第8章中删去了报文标记追踪技术这部分较深的内容;第9章围绕新的风险评估标准展开,修订了大部分内容;第10章补充了最新的法律法规,系统介绍了我国计算机知识产权的法律保护措施。

这样,基于信息保障模型(PDRR)——防护、检测、反应与恢复的理论,本书内容涉及计算机系统安全各层次可能存在的安全问题和普遍采用的安全机制,具体包括:计算机硬件与环境安全、操作系统安全、计算机网络安全、数据库系统安全、应用系统安全以及应急响应与灾难恢复、计算机系统安全风险评估、安全管理和安全立法等。

本书第2版还丰富了课后习题,增加了操作实验题、编程实验题、材料分析题,并提供了很多相关网站和参考书供读者拓展知识面和进行实践。

在一些具体章节中,例如第7章,重新编写了代码安全技术,补充了代码的静态和动态检测技术,增加了软件保护的实践方法;第8章中补充了计算机取证的操作内容。

本书第2版在注重内容全面系统的同时,力求做到叙述清晰、深入浅出。

为了方便教师利用本书教学,便于学生通过本书自学,本书提供了修订后的配套电子教案,读者可在机械工业出版社网站www.cmpedu.com上免费下载。

同时,习题中的实验指导已集结成《计算机系统安全实验教程》出版,为广大读者完成实验给予指导和提供参考,这也使得本套教材的面向应用、提高能力的特色得到更好体现。

本书由陈波、于冷和肖军模共同完成编写。

本书及配套实验教程的编写得到了南京师范大学的支持。

在此,向所有为本书做出贡献的同志致以衷心的感谢。

计算机信息系统安全仍是一个不断发展的研究领域,书中难免存在不足之处,恳请广大读者和专家提出批评和改进意见。

<<计算机系统安全原理与技术>>

内容概要

《计算机系统安全原理与技术》全面介绍了计算机系统各层次可能存在的安全问题和普遍采用的安全机制，包括计算机硬件与环境安全、操作系统安全、计算机网络安全、数据库系统安全、应用系统安全、应急响应与灾难恢复、计算机系统安全风险评估、计算机安全等级评测与安全管理等内容。

《计算机系统安全原理与技术》还对各种安全技术的实践作了指导，帮助读者理解并掌握相关安全原理，提高信息安全防护意识和安全防护能力。

《计算机系统安全原理与技术》每章附有思考与练习题，还给出了大量的参考文献以供进一步阅读。

《计算机系统安全原理与技术》可以作为信息安全专业、信息对抗专业、计算机专业、信息工程专业或其他相关专业的本科生和研究生教材，也可以作为网络信息安全领域的科技人员与信息系统安全管理员的参考书。

<<计算机系统安全原理与技术>>

书籍目录

出版说明前言第1章 计算机系统安全概论1.1 计算机信息系统安全问题1.1.1 计算机信息系统1.1.2 安全威胁1.1.3 脆弱点与安全控制1.1.4 计算机信息系统的安全需求1.2 信息安全概念的发展1.3 计算机系统安全研究的内容1.4 思考与练习第2章 密码学基础2.1 概述2.2 密码学基本概念2.2.1 现代密码系统的组成2.2.2 密码体制2.2.3 密码算法设计的两个重要原则2.2.4 密码分析学2.2.5 密码算法的安全性2.3 对称密码体制2.3.1 数据加密标准DES2.3.2 高级加密标准AES2.4 公钥密码体制2.4.1 传统密码体制的缺陷与公钥密码体制的产生2.4.2 公钥密码体制2.4.3 加密与签名的顺序问题2.4.4 基本数学概念2.4.5 RSA算法2.5 散列函数2.5.1 散列函数的概念2.5.2 SHA算法2.5.3 散列函数的应用2.6 数字签名2.6.1 数字签名的概念2.6.2 常用算法介绍2.7 信息隐藏与数字水印2.7.1 信息隐藏2.7.2 数字水印2.7.3 信息隐藏实例2.8 思考与练习第3章 计算机硬件与环境安全3.1 对计算机硬件的安全威胁3.1.1 计算机硬件安全缺陷3.1.2 环境对计算机的安全威胁3.2 计算机硬件安全技术3.2.1 PC物理防护3.2.2 基于硬件的访问控制技术3.2.3 可信计算与安全芯片3.2.4 硬件防电磁泄漏3.3 环境安全技术3.3.1 机房安全等级3.3.2 机房环境基本要求3.3.3 机房场地环境3.4 思考与练习第4章 操作系统安全4.1 操作系统的安全问题4.1.1 操作系统安全的重要性4.1.2 操作系统面临的安全威胁4.1.3 操作系统的安全性设计4.2 存储保护4.2.1 内存保护4.2.2 运行保护4.2.3 I/O保护4.3 用户认证4.3.1 口令认证4.3.2 一次性口令认证4.3.3 令牌或智能卡4.3.4 生物特征认证4.4 访问控制4.4.1 访问控制模型4.4.2 自主访问控制4.4.3 强制访问控制4.4.4 基于角色的访问控制4.4.5 新型访问控制4.5 Windows系统安全4.5.1 Windows系统安全模型4.5.2 Windows用户账户4.5.3 Windows登录验证4.5.4 Windows安全策略4.6 思考与练习第5章 网络安全5.1 网络安全威胁5.1.1 TCP/IP协议结构5.1.2 IPv4版本TCP/IP的安全问题5.1.3 网络攻击5.2 网络安全框架5.3 防火墙5.3.1 防火墙的概念5.3.2 防火墙技术5.3.3 防火墙体系结构5.3.4 防火墙的局限性和发展5.4 入侵检测5.4.1 入侵检测的概念及发展5.4.2 入侵检测通用模型及框架5.4.3 入侵检测系统分类5.4.4 入侵检测技术5.4.5 入侵检测体系结构5.4.6 入侵检测技术和产品的发展趋势5.4.7 入侵防御系统5.5 网络隔离5.5.1 网络隔离的概念5.5.2 网络隔离的技术和应用5.5.3 网络隔离的局限和发展5.6 公钥基础设施PKI5.6.1 PKI基本概念5.6.2 数字证书5.6.3 证书颁发机构CA5.6.4 证书管理中的关键过程5.6.5 PKI信任模型5.6.6 PMI基本概念5.7 网络安全协议5.7.1 应用层安全协议5.7.2 传输层安全协议SSL5.7.3 网络层安全协议IPsec5.8 IPv6新一代网络的安全机制5.8.1 IPv6的新特性5.8.2 IPv6安全机制对现行网络安全体系的新挑战5.9 思考与练习第6章 数据库安全6.1 数据库安全概述6.1.1 数据库概念6.1.2 数据库安全的重要性6.1.3 数据库面临的安全威胁6.1.4 数据库的安全需求6.1.5 数据库的安全策略6.2 数据库安全控制6.2.1 数据库的安全性6.2.2 数据库的完整性6.2.3 数据库的并发控制6.2.4 数据库的备份与恢复6.3 SQLServer数据库的安全机制6.3.1 SQLServer的安全体系结构6.3.2 SQLServer的安全管理6.3.3 SQLServer的安全策略6.4 思考与练习第7章 应用系统安全7.1 恶意程序7.1.1 计算机病毒7.1.2 蠕虫7.1.3 陷门7.1.4 特洛伊木马7.2 应用系统的编程安全7.2.1 缓冲区溢出7.2.2 格式化字符串漏洞7.2.3 安全编程7.3 Web安全7.3.1 Web安全概述7.3.2 客户端安全控制7.3.3 脚本程序安全控制7.3.4 服务器安全控制7.3.5 网络传输安全控制7.4 软件保护7.4.1 软件技术保护的基本原则7.4.2 密码保护技术7.4.3 电子注册保护技术7.4.4 结合硬件的保护技术7.4.5 基于数字签名的保护技术7.4.6 软件水印7.4.7 软件的反动态跟踪技术7.5 安全软件工程7.5.1 需求分析7.5.2 设计与验证7.5.3 编程控制7.5.4 测试控制7.5.5 运行维护管理7.5.6 行政管理控制7.6 思考与练习第8章 应急响应与灾难恢复8.1 应急响应与灾难恢复的重要性8.2 应急响应概述8.2.1 应急响应的概念8.2.2 应急响应组织8.2.3 应急响应体系研究8.3 容灾备份和恢复8.3.1 容灾备份与恢复的概念8.3.2 容灾备份的关键技术8.4 网站备份与恢复系统实例8.4.1 系统工作原理与总体结构8.4.2 系统主要功能8.4.3 系统采用的关键技术8.5 计算机取证8.5.1 计算机取证的概念8.5.2 计算机取证关键技术8.5.3 计算机取证软件8.5.4 计算机取证的发展趋势8.6 入侵追踪8.6.1 IP地址追踪8.6.2 攻击源追踪8.7 思考与练习第9章 计算机系统安全风险评估9.1 计算机系统安全风险评估的目的和意义9.2 安全风险评估途径9.3 安全风险评估基本方法9.4 安全风险评估工具9.5 安全风险评估的依据和过程9.5.1 风险评估的依据9.5.2 风险要素9.5.3 风险评估的过程9.6 信息系统安全风险评估实例9.7 思考与练习第10章 计算机系统安全管理10.1 计算机系统安全管理概述10.1.1 安全管理的重要性10.1.2 安全管理的目的和任务10.1.3 安全管理原则10.1.4 安全管理的程序和方法10.2 信息安全标准及实施10.2.1 国外主要的计算机系统安全评测准则10.2.2 我国计算机安全等级评测标准10.2.3 国外计算机信息安全管理

<<计算机系统安全原理与技术>>

标准10.2.4 我国信息安全管理标准10.2.5 计算机信息系统安全等级保护管理要求10.3 安全管理与立法10.3.1 我国信息安全相关法律法规介绍10.3.2 我国有关计算机软件知识产权的保护10.4 思考与练习参考文献

<<计算机系统安全原理与技术>>

章节摘录

第1章 计算机系统安全概论1.1 计算机信息系统安全问题1.1.1 计算机信息系统 按照我国颁布的《计算机信息系统安全保护等级划分准则》的定义，“计算机信息系统是由计算机及其相关的配套设备、设施(含网络)构成的，按照一定的应用目标和规格对信息进行采集、加工、存储、传输、检索等处理的人机系统。

”实际上，人们所讨论的典型的计算机信息系统，应该是在计算机网络环境下运行的信息处理系统。一个计算机信息系统由硬件、软件系统和使用人员两部分组成。

硬件系统包括组成计算机、网络的硬设备及其它配套设备。

软件系统包括操作平台软件、应用平台软件和应用业务软件。

操作平台软件通常指操作系统和语言及其编译系统；应用平台软件通常指支持应用开发的软件，如数据库管理系统及其开发工具，各种应用编程和调试工具等；应用业务软件是指专为某种应用而开发的软件。

众多的计算机信息系统，从应用角度可分为两类：一类是以客户机/服务器模式运行的信息系统，重点是提供信息服务，如web网信息系统等；另一类是以信息交换模式运行的信息系统，重点是进行信息交换，如电子商务信息系统等。

不论是何种应用模式，计算机信息系统的最终服务对象是人。

人员是计算机信息系统的设计者、使用者，而计算机信息系统的安全问题也主要由各类使用人员引入，而且使用人员由合法使用人员和非法使用人员组成。

20世纪40年代，随着计算机的诞生，计算机安全问题也随之产生。90年代以来，随着计算机的广泛应用，以计算机网络为主体的信息处理系统迅速发展。

同以前的计算机安全保密相比，计算机信息系统的安全问题要多得多，也复杂得多，涉及到物理环境、硬件、软件、数据、传输、体系结构等多个方面。

<<计算机系统安全原理与技术>>

编辑推荐

《计算机系统安全原理与技术》由机械工业出版社出版。

<<计算机系统安全原理与技术>>

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>