

<<网络信息安全>>

图书基本信息

书名：<<网络信息安全>>

13位ISBN编号：9787111128922

10位ISBN编号：7111128923

出版时间：2003-8

出版时间：机械工业出版社

作者：肖军模 编

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>

<<网络信息安全>>

内容概要

本书详细地论述了访问控制、信息流控制和推理汇漏控制等信息安全的基本理论，系统地分析了计算机硬件、操作系统、网络及其安全设备、数据库系统和应用系统的安全机制的原理及其可能存在的安全缺陷。

书中比较详细地介绍了常用的加密技术、安全信息系统的安全模型和评价标准，同时介绍了安全操作系统和安全应用系统的设计与开发方法。

本书可以作为信息安全专业、信息对抗专业、计算机、信息工程专业或相近专业的本科和研究生教材，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。

书籍目录

第1章 信息安全概述1.1 信息安全与信息对抗1.1.1 信息的安全需求1.1.2 网络信息安全的层次性1.1.3 信息对抗的阶段1.2 信息安全概念与技术的发展1.2.1 单机系统的信息保密阶段1.2.2 网络信息安全阶段1.2.3 信息保障阶段习题一第2章 密码技术2.1 密码技术简介2.1.1 密码学基本概念2.1.2 对称密钥密码系统2.1.3 公钥密码系统2.1.4 散列函数2.2 密码技术的应用2.2.1 数据加密2.2.2 鉴别协议2.2.3 消息完整性协议2.3 公开密钥分发习题二第3章 访问控制原理3.1 访问控制3.1.1 保护系统的访问矩阵模型3.1.2 访问控制策略3.1.3 安全策略的形式描述3.1.4 访问控制机制综述3.1.5 访问的等级结构3.1.6 授权表与权利撤销问题3.1.7 能力机制3.2 基于状态变换的安全系统理论3.2.1 一般性保护系统3.2.2 若干受限制的保护系统3.2.3 获取-授予系统3.3 安全模型的构建3.3.1 建模的方法步骤3.3.2 模型构建实例3.3.3 从模型到系统的映射习题三第4章 信息流控制原理4.1 信息流的格模型4.1.1 格与信息流动策略4.1.2 系统的信息安全性状态4.1.3 状态转换与信息流4.1.4 格的性质的应用4.2 基于格的多级安全模型4.2.1 军用安全模型4.2.2 Bell-Lapadula安全模型4.2.3 Biba安全模型4.3 信息流控制机制综述4.3.1 安全性与精确性4.3.2 流的信道4.4 基于执行的机制4.4.1 流安全的访问控制4.4.2 基于执行机制的模型4.4.3 动态安全性检查4.5 基于编译的机制。4.5.1 关于流的说明4.5.2 各种语句的安全性要求4.5.3 流语义安全性证明4.5.4 任意控制结构的顺序程序4.5.5 同步信息流4.5.6 不正常终止4.6 实际系统的流控制4.6.1 有关流的安全性证明4.6.2 与流控制有关的问题4.7 安全模型的应用4.7.1 安全模型的特点与用途4.7.2 模型的类型4.7.3 模型的应用习题四第5章 信息系统的安全性评价标准5.1 可信计算机系统评价标准5.1.1 评价准则主要概念5.1.2 计算机系统的安全等级5.2 计算机网络安全等级评价标准5.2.1 网络系统的安全等级5.2.2 网络安全服务5.3 我国信息系统安全评价标准5.3.1 各安全级别的主要特征5.3.2 对标准的讨论5.4 通用评估准则(CC)5.4.1 CC的由来与特色5.4.2 安全功能要求5.4.3 安全保证要求5.4.4 AMA类: 保证维护5.4.5 TOE的评估保证级别习题五第6章 计算机硬件与环境安全6.1 对硬件与环境的安全威胁与安全需求6.1.1 计算机硬件安全缺陷6.1.2 环境对计算机造成的安全问题6.2 计算机硬件安全技术6.2.1 硬件访问控制技术6.2.2 防复制技术6.2.3 硬件防辐射6.3 环境安全技术6.3.1 环境干扰防护6.3.2 机房安全6.3.3 灾难后的恢复习题六第7章 安全操作系统及其设计7.1 操作系统安全技术概述7.1.1 威胁系统资源安全的因素7.1.2 系统安全措施7.1.3 系统提供的保护方式7.2 内存保护技术7.2.1 单用户内存保护问题7.2.2 多道程序的保护7.2.3 标记保护法7.2.4 分段与分页技术7.3 客体的访问保护与控制7.3.1 客体的各种保护机制7.3.2 文件的保护机制7.4 自主访问控制与强制访问控制7.4.1 DAC的实现机制7.4.2 MAC的实现机制7.5 用户认证7.5.1 通行字认证方法7.5.2 其他认证方法7.6 实际操作系统中的安全机制7.6.1 Windows NT操作系统7.6.2 UNIX操作系统7.7 可信操作系统的设计7.7.1 可信操作系统的开发过程7.7.2 可信操作系统的设计原则7.7.3 操作系统中的安全功能与技术7.7.4 安全核的设计与实现技术7.7.5 分层结构设计技术7.7.6 环型结构设计技术习题七第8章 网络安全问题8.1 网络安全框架8.2 网络安全机制8.3 IPv4的安全问题8.3.1 网络安全目标8.3.2 IPv4版本TCP/IP的缺陷8.4 Internet网络服务的安全问题8.4.1 Web服务的安全问题8.4.2 FTP服务的安全问题8.4.3 Telnet的安全问题8.4.4 电子邮件的安全问题8.4.5 DNS的安全问题8.5 网络安全的增强技术8.5.1 Kebo阳系统8.5.2 SSL安全协议8.5.3 IPsec8.5.4 虚拟专用网8.6 网络多级安全技术8.6.1 可信网络基8.6.2 安全通信服务器8.6.3 多级安全信道8.7 IPv6新一代网络的安全机制8.7.1 加密和认证8.7.2 密钥的分发8.7.3 IPv6安全机制的应用习题八第9章 数据库安全9.1 数据库的安全问题9.1.1 数据库特点概述9.1.2 数据库的安全威胁9.1.3 数据库的安全要求9.1.4 数据库的安全技术9.2 推理泄露问题9.2.1 敏感数据的泄露问题概述9.2.2 推理控制模型*9.3 数据库的多级安全问题9.3.1 数据库的安全模型9.3.2 数据库多级安全问题研究习题九第10章 程序系统安全10.1 程序对信息造成的危害10.1.1 陷阱10.1.2 缓冲区溢出10.1.3 特洛伊木马10.1.4 零碎敛集10.1.5 隐蔽信道10.1.6 开放敏感信息10.2 危害服务的程序10.2.1 耗时程序10.2.2 死锁问题10.2.3 病毒程序10.2.4 蠕虫程序10

. 2 . 5 网络上其他服务拒绝问题10 . 3 JAVA语言的安全性简介10 . 3 . 1 JAVA简介10 . 3 . 2 JAVA语言的安全问题10 . 4 CGI与PERL语言的安全性简介10 . 4 . 1 CGI与PERL语言10 . 4 . 2 CGI的工作原理10 . 4 . 3 CGI的脆弱性10 . 4 . 4 保护CGI的一些安全措施10 . 5 HTML语言的安全性简介10 . 5 . 1 HTML语言简介10 . 5 . 2 HTML的安全问题10 . 6 安全软件工程10 . 6 . 1 需求分析控制10 . 6 . 2 设计与验证10 . 6 . 3 编程控制10 . 6 . 4 测试控制10 . 6 . 5 运行维护管理10 . 6 . 6 行政管理控制10 . 7 操作系统对程序安全的支持10 . 7 . 1 可信软件10 . 7 . 2 互不信任的程序10 . 7 . 3 受限访问10 . 7 . 4 信息分隔习题十参考文献

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>