第一图书网, tushu007.com

<<计算机安全>>

图书基本信息

书名：<<计算机安全>>

13位ISBN编号：9787115118110

10位ISBN编号：7115118116

出版时间：2003-12

出版时间：人民邮电出版社

作者：戈尔曼

页数：263

字数：495000

译者：华倍

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

内容概要

这是一本侧重从技术的角度上讲授计算机安全（computer security）的教科书。
全书分成四部分：第一部分“基础知识”，介绍了身份识别和认证、访问控制、安全模型，以及安全内核；第二部分“实践”，介绍了Unix和Windows NT安全、安全问题所在，以及安全评估；第三部分“分布式系统”，介绍了分布式系统安全、Web站点安全、密码学，以及网络安全；最后是理论部分，介绍数据库安全、多级安全数据库、并发控制和多级安全，以及面向对象的安全。
本书内容丰富，深入浅出，理论与实践结合，覆盖了从基本的计算机安全概念、安全模型和安全理论，到具体的安全策略、安全实践和安全评估。
每章都有丰富的习题和进一步阅读的建议及电子资源的出处，帮助读者消化和巩固所学内容，并启发读者思考。
因此本书适合高等院校计算机科学技术相关专业的高年级本科生和研究生作选修课教材，特别适合新设信息安全专业的本科生、研究生作专业必修课教材。
本书也可供从事计算机和信息系统安全的工程技术人员作自学教材和工作参考书。

书籍目录

第一部分 基础知识第1章 准备 31.1 定义 31.1.1 安全 41.1.2 计算机安全 41.1.3 机密性 51.1.4 完整性 51.1.5 可用性 61.1.6 可审计性 71.1.7 可靠性和安全性 71.1.8 本书的计算机安全定义 81.2 计算机安全最根本的两难处境 81.3 数据与信息 91.4 计算机安全的原则 91.4.1 控制重点 101.4.2 人-机标尺 101.4.3 复杂性与保险性 121.4.4 集中式控制还是分布式控制 121.5 下面的层次 121.6 进一步的阅读 141.7 练习题 14第2章 身份识别与认证 162.1 用户名和口令 162.2 选择口令 172.3 欺骗攻击 192.4 保护口令文件 202.5 一次签到 212.6 可供选择的方法 222.7 进一步的阅读 232.8 练习题 23第3章 访问控制 253.1 背景 253.2 主体和客体 253.3 访问操作 263.3.1 访问方式 263.3.2 访问权限和访问属性 263.3.3 Unix 283.3.4 Windows NT 283.4 所有权 283.5 访问控制结构 293.5.1 访问控制矩阵 293.5.2 能力 303.5.3 访问控制列表 303.6 中间控制 313.6.1 组和否定的许可 313.6.2 保护环 323.6.3 VSTa微内核中的能力 323.6.4 特权 333.6.5 基于角色的访问控制 333.7 安全级别的格 343.8 进一步的阅读 363.9 练习题 37第4章 安全模型 384.1 状态机模型 384.2 Bell-LaPadula模型 394.2.1 安全策略 394.2.2 基本安全定理 404.2.3 稳定 414.2.4 BLP的各个方面及其局限性 414.3 Harrison-Ruzzo-Ullman模型 424.4 中国墙模型 444.5 Biba模型 454.5.1 静态完整性级别 464.5.2 动态完整性级别 464.5.3 调用的策略 464.6 Clark-Wilson模型 474.7 信息流模型 484.8 进一步的阅读 494.9 练习题 49第5章 安全内核 515.1 基本原理 515.2 操作系统完整性 525.2.1 操作模式 535.2.2 受控调用 535.3 硬件安全特性 535.3.1 计算机体系结构的简单概述 545.3.2 进程和线程 555.3.3 受控调用——中断 555.3.4 Motorola 68000上的保护 565.3.5 Intel 80386/80486上的保护 575.4 引用监视器 595.4.1 存储器保护 605.4.2 Multics操作系统 615.4.3 BLP的Multics解释 625.4.4 核心原语 635.5 进一步的阅读 645.6 练习题 65第二部分 实 践第6章 Unix的安全 696.1 概述 696.2 Unix安全体系结构 706.3 登录和用户账号 716.3.1 用户和超级用户 716.3.2 属组 726.3.3 设置UID和GID 736.4 访问控制 736.4.1 Unix文件结构 736.4.2 改变许可 756.4.3 缺省许可位 766.4.4 目录的许可 776.5 一般安全原则的实例 776.5.1 受控调用 776.5.2 删除文件 786.5.3 设备的保护 786.5.4 挂接文件系统 796.5.5 改变文件系统的根 796.5.6 搜索路径 806.6 审计日志和入侵检测 806.7 包裹层 826.8 安装和配置 836.9 进一步的阅读 836.10 练习题 84第7章 Windows NT安全 857.1 概述 857.2 注册 867.3 身份识别和认证 887.3.1 Windows NT口令方案 887.3.2 登录 897.3.3 绕过SAM API 907.4 访问控制--特性 907.4.1 域 907.4.2 登录缓存--一个潜在的攻击点 917.4.3 用户账户 917.4.4 安全标识符 927.4.5 Windows NT对象的访问 927.4.6 NTFS文件系统 937.4.7 共享 947.5 访问控制--管理 947.5.1 本地组和全局组 957.5.2 用户权限 957.5.3 内置组 967.5.4 Windows NT中的信任关系 967.5.5 强制配置文件 987.6 审计 987.7 动态链接库DLL的安全考虑 997.7.1 DLL欺骗 997.7.2 通知包 997.8 进一步的阅读 997.9 练习题 100第8章 问题是怎样产生的 1018.1 概述 1018.2 环境的变化 1028.2.1 疯狂的黑客 1028.2.2 CTSS 1038.3 边界和语法检查 1038.3.1 Finger漏洞 1038.3.2 VMS登录 1048.3.3 rlogin漏洞 1048.3.4 一个Java漏洞 1058.4 方便的特性 1058.5 受控调用 1068.5.1 VMS用户授权功能 1068.5.2 登录的一个潜在问题 1068.6 旁路 1068.6.1 AS/400机器接口模板 1068.6.2 at漏洞 1078.6.3 Sidewinder 1078.6.4 攻击智能卡 1088.7 有缺陷协议的实现 1098.7.1 TCP认证 1098.7.2 Java的DNS漏洞 1108.8 病毒攻击 1118.8.1 病毒分类 1128.8.2 PC启动过程 1128.8.3 自引导病毒 1138.8.4 寄生病毒 1148.8.5 伴生病毒 1148.8.6 宏病毒 1158.8.7 中断的重定向 1158.8.8 伪装 1168.9 反病毒软件 1168.9.1 物理控制和行政控制 1168.9.2 加密的校验和 1178.9.3 扫描器 1178.10 进一步的阅读 1188.11 练习题 118第9章 安全评估 1209.1 概述 1209.2 橙皮书 1229.3 TNI—可信网络说明 1259.3.1 红皮书策略 1269.3.2 完整性 1269.3.3 标签 1269.3.4 其他安全服务 1279.3.5 评估分类和合成规则 1289.4 信息技术安全评估准则 1289.4.1 评估过程 1299.4.2 安全功能性 1299.4.3 有效性保证 1309.4.4 正确性的保证 1319.5 通用准则 1319.6 质量准则 1329.7 成果充分利用了吗 1329.8 进一步的阅读 1339.9 练习题 133第三部分 分布式系统第10章 分布式系统安全 13710.1 概述 13710.1.1 安全策略 13810.1.2 授权 13810.1.3 安全执行 13910.2 认证 13910.2.1 Kerberos协议 13910.2.2 DSSA/SPX 14210.2.3 个人加密设备 14410.3 安全API 14510.3.1 GSS-API 14510.3.2 API和安全 14810.4

CORBA安全 14910.4.1 对象请求代理 15010.4.2 CORBA安全模型 15110.4.3 认证 15210.4.4 保证的安全还是保证的安全服务 15210.5 进一步的阅读 15310.6 练习题 153第11章 WWW安全 15511.1 背景 15511.2 Web浏览器 15611.3 CGI脚本 15711.4 Cookie 15911.5 认证码 16011.6 沙盒 16111.6.1 字节码检验程序 16211.6.2 Applet类加载程序 16311.6.3 安全管理器 16311.6.4 目前的Java安全 16311.7 知识产权保护 16411.7.1 拷贝保护 16411.7.2 使用限制 16511.7.3 指纹和水印 16511.8 进一步的阅读 16611.9 练习题 166第12章 密码学介绍 16812.1 概述 16812.1.1 老的范型 16812.1.2 新的范型 16912.1.3 密码的密钥 17012.1.4 模运算 17112.2 密码机制 17212.2.1 完整性检查功能 17212.2.2 数字签名 17512.2.3 加密 17712.3 密钥建立协议 18212.3.1 Diffie-Hellman协议 18212.3.2 Needham-Schroeder协议 18312.4 证书 18312.5 密码机制的强度 18412.6 进一步的阅读 18612.7 练习题 186第13章 网络安全 18813.1 概述 18813.1.1 分层模型 18913.1.2 嗅探和欺骗 19013.1.3 ISO/OSI安全体系结构 19113.2 TCP/IP安全 19113.2.1 IPSEC 19213.2.2 SSL/TLS 19513.3 网络边界 19813.4 防火墙 19913.4.1 报文分组过滤 19913.4.2 代理服务器 20013.4.3 双宿主主机防火墙 20013.4.4 屏蔽主机防火墙 20113.4.5 屏蔽子网防火墙 20213.5 进一步的阅读 20313.6 练习题 203第四部分 理 论第14章 数据库安全 20714.1 概述 20714.2 关系数据库 20914.2.1 数据库关键字 21114.2.2 完整性规则 21114.3 访问控制 21214.3.1 SQL的安全模型 21314.3.2 优先权的颁发与撤销 21314.3.3 通过视图的访问控制 21414.4 统计数据库的安全性 21614.4.1 聚集和推断 21714.4.2 跟踪攻击 21714.4.3 对策 21914.5 结合操作系统的完整性 22014.6 进一步的阅读 22114.7 练习题 221第15章 多级安全数据库 22315.1 基本原理 22315.2 关系数据库中的MAC 22415.2.1 标识对象 22415.2.2 一致的寻址 22515.2.3 可见数据 22515.2.4 导出关系 22615.2.5 自主访问控制 22715.2.6 干净数据 22715.3 多重实例 22715.4 低端插入 22915.5 实现方面的问题 23115.6 进一步的阅读 23215.7 练习题 232第16章 并发控制和多级安全 23416.1 目的 23416.2 并发控制 23516.2.1 积极的和保守的调度器 23616.2.2 两阶段锁 23616.2.3 多版本时间戳排序 23716.3 MLS并发控制 23816.3.1 总体观察 23916.3.2 最佳MLS并发控制 24016.3.3 单级调度器的MVTO 24116.3.4 MVTO-SS的正确性 24316.4 非串行的并发控制 24316.5 进一步的阅读 24616.6 练习题 247第17章 面向对象安全 24817.1 基本原理 24817.2 对象模型 24817.3 对象模型中的安全 25017.4 在面向对象系统中的强制访问控制 25117.4.1 标识对象 25117.4.2 消息流的控制 25217.4.3 MLS操作系统下的面向对象的安全 25317.5 进一步的阅读 25517.6 练习题 255参考文献 257

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