

《计算机安全学》

图书基本信息

书名：《计算机安全学》

13位ISBN编号：9787111228646

10位ISBN编号：7111228642

出版时间：2008-4

出版社：Dieter Gollmann、张小松 机械工业出版社 (2008-04出版)

作者：Dieter Gollmann

页数：223

译者：张小松

版权说明：本站所提供下载的PDF图书仅提供预览和简介以及在线试读，请支持正版图书。

更多资源请访问：www.tushu000.com

《计算机安全学》

内容概要

《计算机安全学》

作者简介

Dieter Gollmann，汉堡科技大学分布式应用软件安全的教授，曾做过伦敦大学皇家豪乐威学院的访问教授。丹麦技术大学副教授。另外，他曾在剑桥大学微软研究中心担任研究信息安全的研究员。

书籍目录

目录

译者序

前言

第1章 绪论

1.1 攻击与攻击者

1.2 安全

1.3 安全管理

1.3.1 安全策略

1.3.2 测量安全

1.3.3 标准

1.4 风险与威胁分析

1.4.1 资产

1.4.2 漏洞

1.4.3 威胁

1.4.4 风险

1.4.5 对策——减轻风险

1.5 深层阅读

1.6 练习

第2章 计算机安全基础

2.1 定义

2.1.1 安全

2.1.2 计算机安全

2.1.3 机密性

2.1.4 完整性

2.1.5 可用性

2.1.6 问责性

2.1.7 不可否认性

2.1.8 可靠性

2.1.9 计算机安全定义

2.2 计算机安全进退两难的困境

2.3 数据与信息

2.4 计算机安全原则

2.4.1 控制重点

2.4.2 人一机标尺

2.4.3 复杂性与保证性

2.4.4 集中控制或分布控制

2.5 下层

2.6 深层阅读

2.7 练习

第3章 身份识别与认证

3.1 用户名与口令

3.2 口令管理

3.3 选择口令

3.4 欺骗攻击

3.5 保护口令文件

3.6 一次签到

3.7 可供选择的方法

3.8 深层阅读

3.9 练习

第4章 访问控制

4.1 背景

4.2 认证和授权

4.3 访问操作

4.3.1 访问模式

4.3.2 Bell-LaPadula模型的访问权限

4.3.3 当前的操作系统

4.4 所有权

4.5 访问控制结构

4.5.1 访问控制矩阵

4.5.2 能力

4.5.3 访问控制列表

4.6 中间控制

4.6.1 组和否定的许可

4.6.2 特权

4.6.3 基于角色的访问控制

4.6.4 保护环

4.7 偏序

4.7.1 VSTa微内核中的能力

4.7.2 安全级别的格

4.7.3 多级安全

4.8 深层阅读

4.9 练习

第5章 引用监控器

5.1 引言

5.1.1 部署引用监控器

5.1.2 执行监控器

5.2 操作系统完整性

5.2.1 操作模式

5.2.2 受控调用

5.3 硬件安全特性

5.3.1 安全基本原理

5.3.2 计算机体系结构的简单概述

5.3.3 进程和线程

5.3.4 受控调用——中断

5.3.5 Intel 80386/80486上的保护

5.4 存储器保护

5.5 深层阅读

5.6 练习

第6章 UNIX安全

6.1 引言

6.2 主角

6.2.1 用户账户

6.2.2 超级用户（根）

6.2.3 组

6.3 主体

6.3.1 登录和口令

- 6.3.2 影子口令文件
- 6.4 对象
 - 6.4.1 i节点
 - 6.4.2 默认许可位
 - 6.4.3 目录的许可
- 6.5 访问控制
 - 6.5.1 设置UID和GID
 - 6.5.2 更改许可
 - 6.5.3 UNIX访问控制的不足
- 6.6 一般安全原则的实例
 - 6.6.1 受控调用的应用
 - 6.6.2 删除文件
 - 6.6.3 设备保护
 - 6.6.4 改变文件系统的根
 - 6.6.5 挂接文件系统
 - 6.6.6 环境变量
 - 6.6.7 搜索路径
 - 6.6.8 包裹层
- 6.7 管理问题
 - 6.7.1 管理超级用户
 - 6.7.2 可信主机
 - 6.7.3 审计日志与入侵检测
 - 6.7.4 安装与配置
- 6.8 深层阅读
- 6.9 练习
- 第7章 Windows 2000安全
 - 7.1 引言
 - 7.1.1 体系结构
 - 7.1.2 注册表
 - 7.1.3 域
 - 7.1.4 活动目录
 - 7.2 访问控制——组件
 - 7.2.1 主角
 - 7.2.2 主体
 - 7.2.3 对象
 - 7.2.4 访问掩码
 - 7.2.5 扩展权限
 - 7.3 访问决策
 - 7.3.1 DACL
 - 7.3.2 决策算法
 - 7.3.3 ACE继承
 - 7.4 受限上下文
 - 7.5 管理
 - 7.5.1 用户账户
 - 7.5.2 默认用户账户
 - 7.5.3 审计
 - 7.5.4 小结
 - 7.6 深层阅读
 - 7.7 练习

第8章 Bell-LaPadula模型

8.1 状态机模型

8.2 Bell-LaPadula模型

8.2.1 状态集

8.2.2 安全策略

8.2.3 基本安全定理

8.2.4 稳定性

8.2.5 BLP的各个方面及其局限性

8.3 BLP的Multics阐述

8.3.1 Multics中的主体和对象

8.3.2 转换BLP策略

8.3.3 检查内核原语

8.4 深层阅读

8.5 练习

第9章 安全模型

9.1 Biba模型

9.1.1 静态完整性级别

9.1.2 动态完整性级别

9.1.3 调用的策略

9.2 中国墙模型

9.3 Clark-Wilson模型

9.4 Harrison-Ruzzo-Ullman模型

9.5 信息流模型

9.5.1 熵和平均值

9.5.2 基于格的模型

9.6 执行监控器

9.6.1 执行属性

9.6.2 安全性和活动性

9.7 深层阅读

9.8 练习

第10章 安全评估

10.1 引言

10.2 橘皮书

10.3 虹系列

10.4 信息技术安全评估标准

10.5 联邦标准

10.6 共同标准

10.6.1 保护配置文件

10.6.2 评估保证级别 (EAL)

10.6.3 评估方法

10.7 质量标准

10.8 成果是否得到充分利用

10.9 深层阅读

10.10 练习

第11章 密码学

11.1 引言

11.1.1 旧的范例

11.1.2 新的范例

11.1.3 密钥

- 11.1.4 密码机制
- 11.2 模运算
- 11.3 完整性检查功能
 - 11.3.1 冲突和生日悖论
 - 11.3.2 操作检测码
 - 11.3.3 消息认证码
 - 11.3.4 安全哈希算法
- 11.4 数字签名
 - 11.4.1 一次性签名
 - 11.4.2 ElGamal签名和DSA
 - 11.4.3 RSA签名
- 11.5 加密
 - 11.5.1 数据加密标准
 - 11.5.2 块加密器模式
 - 11.5.3 RSA加密
 - 11.5.4 ElGamal加密
- 11.6 密码机制的强度
- 11.7 演示
- 11.8 深层阅读
- 11.9 练习
- 第12章 分布式系统中的认证
 - 12.1 引言
 - 12.2 密钥建立和认证
 - 12.2.1 远程认证
 - 12.2.2 密钥建立
 - 12.3 密钥建立协议
 - 12.3.1 认证密钥交换协议
 - 12.3.2 Diffie-Hellman协议
 - 12.3.3 Needham-Schroeder协议
 - 12.3.4 基于口令的password-based协议
 - 12.4 Kerberos
 - 12.4.1 领域
 - 12.4.2 Kerberos和Windows
 - 12.4.3 委派
 - 12.4.4 撤销
 - 12.4.5 小结
 - 12.5 公钥基础设施
 - 12.5.1 证书
 - 12.5.2 证书权威
 - 12.5.3 X.509/PKIX证书
 - 12.5.4 证书链
 - 12.5.5 撤销
 - 12.5.6 电子签名
 - 12.6 可信计算—证明
 - 12.7 深层阅读
 - 12.8 练习
- 第13章 网络安全
 - 13.1 引言
 - 13.1.1 威胁模型

- 13.1.2 通信模型
- 13.1.3 TCP会话劫持
- 13.1.4 TCP-SYN洪泛攻击
- 13.2 协议设计原则
- 13.3 IP安全
 - 13.3.1 认证报头
 - 13.3.2 封装安全有效载荷
 - 13.3.3 安全关联
 - 13.3.4 因特网密钥交换协议
 - 13.3.5 IPsec策略
 - 13.3.6 小结
- 13.4 SSL/TLS
- 13.5 域名系统DNS
- 13.6 防火墙
 - 13.6.1 包过滤
 - 13.6.2 状态包过滤器
 - 13.6.3 电路级代理
 - 13.6.4 应用层代理
 - 13.6.5 防火墙策略
 - 13.6.6 边界网络
 - 13.6.7 局限性和问题
- 13.7 入侵检测
 - 13.7.1 漏洞评估
 - 13.7.2 误用检测
 - 13.7.3 异常检测
 - 13.7.4 基于网络的入侵检测系统
 - 13.7.5 基于主机的入侵检测系统
 - 13.7.6 蜜罐
- 13.8 深层阅读
- 13.9 练习
- 第14章 软件安全
 - 14.1 引言
 - 14.1.1 安全性和可靠性
 - 14.1.2 恶意程序分类
 - 14.1.3 黑客
 - 14.1.4 环境的改动
 - 14.2 字符和数字
 - 14.2.1 字符（UTF-8编码）
 - 14.2.2 整数溢出
 - 14.2.3 数组
 - 14.3 规范表示
 - 14.4 内存管理
 - 14.4.1 缓冲区溢出
 - 14.4.2 虚拟内存系统（VMS）登录
 - 14.4.3 finger漏洞
 - 14.4.4 栈溢出
 - 14.4.5 不可执行的栈
 - 14.4.6 堆溢出
 - 14.4.7 类型混淆

- 14.4.8 疯狂的电脑黑客
- 14.4.9 AS/400机器接口模板
- 14.5 数据和代码
- 14.5.1 远程登录漏洞
- 14.5.2 脚本
- 14.5.3 SQL插入
- 14.6 竞争条件
- 14.7 防御
- 14.7.1 防止：硬件
- 14.7.2 防止：类型安全
- 14.7.3 预防：更安全的函数
- 14.7.4 检测：代码检查
- 14.7.5 检测：测试
- 14.7.6 缓和：最低权限
- 14.7.7 反应：紧跟时代步伐
- 14.8 深层阅读
- 14.9 练习
- 第15章 新的访问控制范例
- 15.1 引言
- 15.1.1 访问控制范例的改变
- 15.1.2 修订的有关访问控制的术语
- 15.2 基于代码的访问控制
- 15.2.1 堆栈检查
- 15.2.2 基于历史的访问控制
- 15.3 Java安全
- 15.3.1 执行模型
- 15.3.2 Java 1安全模型
- 15.3.3 Java 2安全模型
- 15.3.4 字节码校验器
- 15.3.5 类加载器
- 15.3.6 策略
- 15.3.7 安全管理器
- 15.3.8 小结
- 15.4.NET安全框架
- 15.4.1 通用语言运行库
- 15.4.2 基于代码身份的安全
- 15.4.3 证据
- 15.4.4 强名称
- 15.4.5 许可
- 15.4.6 安全策略
- 15.4.7 堆栈遍历
- 15.4.8 小结
- 15.5 cookie
- 15.6 简单公钥基础设施
- 15.7 信任管理
- 15.8 数字版权管理
- 15.9 深层阅读
- 15.10 练习
- 第16章 移动

- 16.1 引言
- 16.2 GSM
 - 16.2.1 部件
 - 16.2.2 临时移动用户标识
 - 16.2.3 加密算法
 - 16.2.4 用户身份认证
 - 16.2.5 加密
 - 16.2.6 基于位置的服务
 - 16.2.7 小结
- 16.3 通用移动通信系统
 - 16.3.1 假基站攻击
 - 16.3.2 加密算法
 - 16.3.3 UMTS认证和密钥协议
- 16.4 移动IPv6的安全性
 - 16.4.1 移动IPv6
 - 16.4.2 安全绑定更新
 - 16.4.3 地址所有权
- 16.5 无线局域网
 - 16.5.1 无线对等加密
 - 16.5.2 WPA
 - 16.5.3 IEEE 802.11i-WPA2
- 16.6 蓝牙
- 16.7 深层阅读
- 16.8 练习
- 第17章 数据库安全
 - 17.1 引言
 - 17.2 关系数据库
 - 17.2.1 数据库的关键字
 - 17.2.2 完整性规则
 - 17.3 访问控制
 - 17.3.1 SQL安全模型
 - 17.3.2 特权的授予和撤销
 - 17.3.3 通过视图的访问控制
 - 17.4 统计数据库的安全
 - 17.4.1 聚集和推断
 - 17.4.2 跟踪攻击
 - 17.4.3 对策
 - 17.5 操作系统的完整性
 - 17.6 隐私
 - 17.7 深层阅读
 - 17.8 习题
- 参考文献

第1章 绪论 一些涉及新的信息技术(IT)的文章中常常以如下评论开头：对安全的关注是阻止新信息技术使用的主要原因，但这样一来也妨碍了普通用户和公司享受到这些技术可能带来的所有好处。这类观点见诸于安全方面的学术专著，见诸于试图说服用户相信其提供服务价值的咨询人员，见诸于安全产品销售人员或负责安全计划的政府官员。安全方面的故事在媒体中炒得很热，并且总是带有强烈的动机，例如IT巨人(微软)在安全方面的漏洞或者对看不见的危害的担心(例如肆虐于因特网上的病毒、蠕虫)。一些别有用心的人自然会找出一些原因来夸大我们面临的威胁，而要获取有力的证据来评估问题的严重程度常常也很困难。同时，在另一方面，任何遭到某种蠕虫或病毒攻击的人都能证实，威胁确实存在。的确，开放式的通信网络如因特网、移动电话系统的广泛使用，让数量巨大的用户群暴露在安全的威胁下。因此，IT专业人员必须要了解这些网络的潜在漏洞、核心保护机制及其局限性。这本书主要讲述计算机安全。计算机安全最初的关注点是多用户系统。用户必须相互隔离，非授权用户必须被禁止修改系统软件。目前的关注点放在被认为是网络终端系统的计算设备上。许多安全问题都源于这些设备连在网络上这一事实，或多或少都可能受到“非信任节点”的攻击。传统的网络安全服务保护节点间的信号，当信息被安全地送达对方，保护的任务就完成了。我们要讨论的是终端系统接收信息后在处理信息的过程中发生的问题。在进入此书技术内容的讨论之前，本章将纵览一些在实战中试图实现安全措施时必须说明的重要问题。部署安全措施(以及通常的IT技术)是个管理决策的问题，必须有组织、按部就班地实施技术安全措施才能奏效。管理决策应依据对当前风险和威胁的分析来作出。因此，我们将给出安全管理及风险和威胁分析的简短综述。

精彩短评

1、安全理论

《计算机安全学》

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:www.tushu000.com