

《计算机安全导论》

图书基本信息

书名：《计算机安全导论》

13位ISBN编号：9787302273359

出版时间：2012-3

作者：Michael T. Goodrich, Roberto Tama

页数：369

译者：葛秀慧, 田浩

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.tushu111.com

《计算机安全导论》

内容概要

《世界著名计算机教材精选:计算机安全导论》旨在从应用的观点来介绍计算机安全的一般原则。通过《世界著名计算机教材精选:计算机安全导论》，读者能熟悉常见的网络攻击，包括病毒、蠕虫、密码破解、按键记录器、拒绝服务、dns缓存中毒、端口扫描、欺骗和网络钓鱼等，掌握与计算机和网络脆弱性相关的鉴别和防御技术，以及用于检测和修复受感染系统的方法，学习如加密、数字签名、加密协议和访问控制模型等安全系统的基本要素，同时，还将学习如锁、手机、atm机和信用卡等相关常用物品的安全原则。

书籍目录

目录

第1章 简介

1.1 基本概念

1.1.1 机密性、完整性和可用性

1.1.2 保证、真实性和匿名

1.1.3 威胁与攻击

1.1.4 安全原则

1.2 访问控制模型

1.2.1 访问控制矩阵

1.2.2 访问控制列表

1.2.3 权能

1.2.4 基于角色的访问控制

1.3 加密的概念

1.3.1 加密

1.3.2 数字签名

1.3.3 对密码系统的简单攻击

1.3.4 加密散列函数

1.3.5 数字证书

1.4 实现和可用性问题

1.4.1 效率和可用性

1.4.2 密码

1.4.3 社会工程

1.4.4 源于编程错误的脆弱性

1.5 练习

第2章 物理安全

2.1 物理保护与攻击

2.2 锁与保险箱

2.2.1 锁技术

2.2.2 针对锁与保险箱的攻击

2.2.3 锁安全的数学知识

2.3 身份验证技术

2.3.1 条形码

2.3.2 磁条卡

2.3.3 智能卡

2.3.4 RFID

2.3.5 生物特征识别

2.4 针对计算机的直接攻击

2.4.1 环境攻击和事故

2.4.2 窃听

2.4.3 TEMPEST

2.4.4 Live CD

2.4.5 计算机取证

2.5 专用机

2.5.1 自动取款机

2.5.2 投票机

2.6 物理入侵检测

2.6.1 视频监控

2.6.2 人为因素和社会工程

2.7 练习

第3章 操作系统的安全

3.1 操作系统的概念

3.1.1 内核与输入/输出

3.1.2 进程

3.1.3 文件系统

3.1.4 内存管理

3.1.5 虚拟机

3.2 进程的安全

3.2.1 从开始到结束的传递信任

3.2.2 监控、管理与日志

3.3 内存与文件系统的安全

3.3.1 虚拟内存的安全

3.3.2 基于密码的身份验证

3.3.3 访问控制与高级文件权限

3.3.4 文件描述符

3.3.5 符号链接与快捷方式

3.4 应用程序的安全

3.4.1 编译与链接

3.4.2 简单的缓冲区溢出攻击

3.4.3 基于堆栈的缓冲区溢出

3.4.4 基于堆的缓冲区溢出攻击

3.4.5 格式化字符串攻击

3.4.6 竞争条件

3.5 练习

第4章 恶意软件

4.1 内部攻击

4.1.1 后门

4.1.2 逻辑炸弹

4.1.3 内部攻击的防御

4.2 计算机病毒

4.2.1 病毒的分类

4.2.2 病毒的防御

4.2.3 加密病毒

4.2.4 多变体病毒和变形病毒

4.3 恶意软件攻击

4.3.1 特洛伊木马

4.3.2 计算机蠕虫

4.3.3 Rootkits

4.3.4 零日攻击

4.3.5 僵尸网络

4.4 入侵隐私软件

4.4.1 广告软件

4.4.2 间谍软件

4.5 对策

4.5.1 最佳实践

4.5.2 检测所有恶意软件的不可能性

4.5.3 恶意软件检测的军备竞赛

4.5.4 恶意软件的经济

4.6 练习

第5章 网络安全I

5.1 网络安全的概念

5.1.1 网络拓扑

5.1.2 互联网协议层

5.1.3 网络安全问题

5.2 链路层

5.2.1 以太网

5.2.2 媒体访问控制 (MAC) 地址

5.2.3 ARP欺骗

5.3 网络层

5.3.1 IP

5.3.2 网际控制消息协议

5.3.3 IP欺骗

5.3.4 数据包嗅探

5.4 传输层

5.4.1 传输控制协议

5.4.2 用户数据报协议 (UDP)

5.4.3 网络地址转换

5.4.4 TCP会话劫持

5.5 拒绝服务攻击

5.5.1 ICMP攻击

5.5.2 SYN洪水攻击

5.5.3 优化的TCP ACK攻击

5.5.4 分布式拒绝服务

5.5.5 IP 回溯

5.6 练习

第6章 网络安全II

6.1 应用层与DNS

6.1.1 应用层协议示例

6.1.2 域名系统

6.1.3 DNS攻击

6.1.4 DNSSEC

6.2 防火墙

6.2.1 防火墙策略

6.2.2 无状态和有状态防火墙

6.3 隧道

6.3.1 安全的Shell (SSH)

6.3.2 IPSec

6.3.3 虚拟专用网络

6.4 入侵检测

6.4.1 入侵侦测事件

6.4.2 基于规则的入侵检测

6.4.3 统计入侵检测

6.4.4 端口扫描

6.4.5 蜜罐

6.5 无线网

6.5.1 无线技术

- 6.5.2 有线等效保密
- 6.5.3 Wi-Fi保护访问
- 6.6 练习
- 第7章 Web安全
 - 7.1 万维网
 - 7.1.1 HTTP与HTML
 - 7.1.2 HTTPS
 - 7.1.3 动态内容
 - 7.1.4 会话和cookie
 - 7.2 针对客户端的攻击
 - 7.2.1 会话劫持
 - 7.2.2 网络钓鱼
 - 7.2.3 点击劫持
 - 7.2.4 媒体内容的脆弱性
 - 7.2.5 隐私攻击
 - 7.2.6 跨站点脚本
 - 7.2.7 跨站请求伪造
 - 7.2.8 防御客户端的攻击
 - 7.3 服务器的攻击
 - 7.3.1 服务器端的脚本
 - 7.3.2 服务器端脚本包含的脆弱性
 - 7.3.3 数据库和SQL注入攻击
 - 7.3.4 拒绝服务攻击
 - 7.3.5 Web服务器权限
 - 7.3.6 防御服务器端的攻击
 - 7.4 练习
- 第8章 加密
 - 8.1 对称加密
 - 8.1.1 攻击
 - 8.1.2 替换密码
 - 8.1.3 一次一密
 - 8.1.4 伪随机数发生器
 - 8.1.5 希尔密码与置换密码
 - 8.1.6 高级加密标准 (AES)
 - 8.1.7 操作模式
 - 8.2 公钥加密
 - 8.2.1 模运算
 - 8.2.2 RSA密码系统
 - 8.2.3 Elgamal密码系统
 - 8.2.4 密钥交换
 - 8.3 加密散列函数
 - 8.3.1 性质与应用
 - 8.3.2 生日攻击
 - 8.4 数字签名
 - 8.4.1 RSA签名方案
 - 8.4.2 Elgamal签名方案
 - 8.4.3 使用Hash函数的数字签名
 - 8.5 AES和RSA加密细节
 - 8.5.1 AES的细节

8.5.2 RSA的细节

8.6 练习

第9章 安全模型与实践

9.1 策略、模型与信任

9.1.1 安全策略

9.1.2 安全模型

9.1.3 信任管理

9.2 访问控制模型

9.2.1 Bell-La Padula模型

9.2.2 其他的访问控制模型

9.2.3 基于角色的访问控制

9.3 安全标准与评价

9.3.1 橘皮书和通用标准

9.3.2 政府管治及标准

9.4 软件的脆弱性评估

9.4.1 静态测试与动态测试

9.4.2 漏洞开发与脆弱性披露

9.5 管理和测试

9.5.1 系统管理

9.5.2 网络测试与渗透测试

9.6 Kerberos

9.6.1 Kerberos票据与服务器

9.6.2 Kerberos身份验证

9.7 安全存储

9.7.1 文件加密

9.7.2 磁盘加密

9.7.3 可信平台模块

9.8 练习

第10章 分布式应用程序的安全

10.1 数据库安全

10.1.1 表和查询

10.1.2 更新和两阶段提交协议

10.1.3 数据库访问控制

10.1.4 敏感数据

10.2 电子邮件安全

10.2.1 电子邮件的工作原理

10.2.2 加密和身份验证

10.2.3 垃圾邮件

10.3 支付系统和拍卖

10.3.1 信用卡

10.3.2 数字现金

10.3.3 网上拍卖

10.4 数字版权管理

10.4.1 数字媒体版权技术

10.4.2 数字媒体版权实践

10.4.3 软件许可方案

10.4.4 法律问题

10.5 社交网络

10.5.1 作为攻击载体的社交网络

10.5.2 私隐

10.6 投票系统

10.6.1 安全目标

10.6.2 ThreeBallot

10.7 练习

参考文献

《计算机安全导论》

精彩短评

- 1、我读到第三章，有些概念书上讲的极差，感觉完全是机器翻译过来的。如果懂了就知道书上在说啥。如果不懂，语句都不通顺
- 2、导论嘛。。。
- 3、仅适合学生看看

《计算机安全导论》

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.tushu111.com