

<<软件加密解密与计算机安全技术>>

图书基本信息

书名：<<软件加密解密与计算机安全技术>>

13位ISBN编号：9787508407913

10位ISBN编号：7508407911

出版时间：2001-09

出版时间：中国水利水电出版社

作者：灯芯工作室

页数：323

字数：462000

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>

<<软件加密解密与计算机安全技术>>

内容概要

随着个人电脑使用的普及和电脑教育的深化，随着网络的迅速发展，网络技术的日渐更新，网络时代的计算机信息安全越来越重要，同时许多对电脑知识和实用技术有一定了解的软件用户越来越关心软件的加密解密技术，他们迫切需要掌握一定的知识和技术手段用来保护自己的计算机和各类信息及文件。

本书将从基本的系统软件讲起，系统地讲解有关加密解密技术所需的基础知识，介绍软件加密的原理及方法，同时就常见的解密方式作个对照性分析，更为重要的是基于实例和算法的讲解会使广大读者事半功倍；本书对计算机网络安全和通信安全以及黑客攻防技术作了一个较详细的介绍；最后，还介绍几种常用的加密及解密工具。

本书配套光盘，含加/解密、系统安全、杀毒/解毒以及黑客攻防等工具和简要介绍，供学习参考。

本书主要是面对广大软件用户而编写的，也适用于计算机、通信、信息管理等有关专业的大专院校学生及专业工作者参考，也可作为相关专业的教学参考书。

书籍目录

前言 第一部分 基础知识 讲述第1章 深入操作系统 1.1 操作系统概述 1.1.1 什么是操作系统 1.1.2 操作系统的发展历程 1.1.3 操作系统的特征与功能 1.2 DOS操作系统的重要知识 1.2.1 DOS启动过程和内存分配 1.2.2 如何加载程序 1.2.3 DOS的中断系统 1.2.4 DOS的文件管理 1.3 Windows操作系统 1.3.1 Windows的发展 1.3.2 Windows的文件系统 1.4 其他操作系统 1.4.1 UNIX操作系统 1.4.2 VMS和OS/2 1.5 小结 第2章 磁盘系统 2.1 磁盘的总体结构 2.1.1 软盘的总体结构 2.1.2 硬盘的总体结构 2.2 磁盘的引导区 2.2.1 软盘的引导区 2.2.2 硬盘的主引导区 2.3 文件目录表和文件分配表 2.3.1 文件目录表 2.3.2 文件分配表 2.4 磁盘扇区信息的微观结构 2.5 软驱的工作原理 2.6 小结 第3章 计算机密码学 3.1 密码学的基本概念 3.2 古典密码 3.2.1 置换密码 3.2.2 代替密码 3.2.3 代数密码 3.3 现代密码体制 3.3.1 序列密码体制 3.3.2 分组密码体制 3.4 小结 第4章 计算机病毒 4.1 病毒的一般原理 4.1.1 病毒的产生和特点 4.1.2 病毒的一般原理 4.1.3 病毒的分类 4.1.4 病毒的主要征兆 4.2 常见病毒 4.2.1 常见病毒举例 4.2.2 病毒发展的新特点 4.3 病毒的检测原理 4.3.1 病毒的判定 4.3.2 病毒检测原理 4.4 病毒的防护和清除原理 4.4.1 病毒防护原理 4.4.2 病毒清除原理 4.5 常用病毒防治软件和硬件 4.6 小结 第5章 计算机网络安全概况 5.1 网络普及的必然性 5.1.1 计算机网络的概念 5.1.2 计算机网络的发展历史 5.1.3 计算机网络的发展前景 5.2 网络安全的脆弱性 5.3 网络安全的重要性 5.4 小结 第二部分 软件加密技术 第6章 软件加密技术概述 6.1 软件加密技术概述 6.2 软件加密的基本分类 6.2.1 依赖硬件的加密方案 6.2.2 不依赖硬件的加密方案 6.3 软件加密技术的基本要求 6.3.1 反拷贝 6.3.2 防静态分析 6.3.3 反动态跟踪技术 6.4 软件加密技术的意义 6.5 小结 第7章 磁盘反拷贝技术 7.1 软磁盘反拷贝加密技术 7.1.1 超级扇区法 7.1.2 异常ID法 7.1.3 额外扇区法 7.1.4 伪扇区法 7.1.5 扇区对齐法 7.1.6 未格式化扇区法 7.1.7 螺线型磁道法 7.1.8 磁道间距不规则变化法 7.1.9 宽磁道法 7.1.10 磁道接缝软指纹技术 7.1.11 扇区软指纹法 7.1.12 弱位方法 7.1.13 错误CRC法 7.1.14 磁道噪声法 7.1.15 FDC移花接木法 7.1.16 扇区交错保密法 7.2 硬盘加密技术 7.2.1 硬盘主引导记录的分析 7.2.2 硬盘上的软件加密 7.2.3 硬盘加锁 7.2.4 硬盘反拷贝 7.3 小结 第8章 防静态分析技术 8.1 代替密码加密技术 8.1.1 单表代替法 8.1.2 多表代替法 8.1.3 加减法 8.1.4 异或运算法 8.2 换位密码加密技术 8.2.1 以字节为单位的换位加密技术 8.2.2 以比特为单位的换位加密技术 8.3 综合加密与乘积加密 8.3.1 综合加密 8.3.2 乘积加密 8.4 小结 第9章 反动态跟踪技术 9.1 反动态跟踪技术的分类 9.2 内存翻卷技术 9.3 封锁键盘技术 9.4 显示控制技术 9.5 定时技术 9.5.1 时钟中断特性分析 9.5.2 计算加密程序执行某一模块的执行时间 9.6 变更中断技术 9.6.1 破坏中断向量 9.6.2 利用中断向量 9.7 程序自检和设计技术 9.7.1 程序自检技术 9.7.2 程序设计技术 9.8 程序运行环境的检测技术 9.9 小结 第10章 软件加密的其他技术 10.1 口令加密技术 10.1.1 口令加密 10.1.2 用口令加密起始簇号 10.1.3 可执行文件的口令加密 10.2 限制软件技术 10.2.1 设置软件使用期限 10.2.2 限制软件的运行次数 10.3 激光加密技术 10.4 自毁软件技术 10.4.1 自毁软件的基本原理 10.4.2 自毁软件的设计 10.5 逆指令流技术 10.6 伪随机数加密法 10.7 小结 第11章 密码体制与加密算法 11.1 DES密码体制 11.2 RSA加密算法 11.2.1 公开密钥秘密体制 11.2.2 RSA算法的理论基础 11.2.3 RSA算法的实施 11.2.4 素数的检测 11.2.5 RSA体制的几个有关问题 11.3 仿射变换式加密算法 11.4 割集密码与回路密码 11.4.1 割集密码 11.4.2 回路密码 11.5 小结 第三部分 软件解密技术 第12章 加密软件的解密技术 12.1 加密软件的动态跟踪工具 12.1.1 软动态跟踪工具 12.1.2 硬动态跟踪工具 12.2 动态跟踪加密软件的目标 12.3 软盘拷贝和分析工具 12.4 加密软件的解密技术 12.5 小结 第13章 强力攻击技术 13.1 穷尽密钥搜索攻击 13.2 字典攻击 13.3 查表攻击 13.4 时间-存储权衡攻击 13.5 小结 第14章 密码分析技术 14.1 差分密码分析 14.1.1 差分密码分析概述 14.1.2 DES的差分密码分析 14.2 线性密码分析 14.2.1 基本原理 14.2.2 DES的线性密码分析 14.3 小结 第四部分 网络安全 第15章 计算机网络安全 15.1 网络安全功能 15.1.1 计算机安全技术体系 15.1.2 OSI安全体系结构 15.2 网络的特点及安全问题 15.2.1 网络的特点 15.2.2 网络部件的不安全因素 15.2.3 网络软件的不安全因素 15.2.4 工作人员的不安全因素 15.2.5 环境因素 15.3 报文鉴别与数字签名 15.3.1 鉴别技术 15.3.2 数字签名 15.4 网络的数据加密 15.4.1 链路加密 15.4.2 节点加密 15.4.3 端对端加密 15.5 密钥的管理 15.5.1 密钥组织 15.5.2 密钥的产生 15.5.3 密钥的分配 15.5.4 密钥的存储与保护 15.5.5 PGP及其密钥管理 15.6 局域网 15.6.1 物理安全策略 15.6.2 流量控制 15.6.3 访问控制策略 15.6.4 信息加密策略 15.6.5 网络安全管理策略 15.7 防火墙技术 15.7.1 防火墙概述 15.7.2 防火墙的基本思想和技术 15.7.3 防火墙的类型 15.7.4 非法攻击防火墙的基本方法 15.7.5 防火墙安全技术分析 15.7.6 国内外主流防火墙产品介绍 15.8 虚

拟专网技术 (VPN) 15.8.1 虚拟专网的功能 15.8.2 虚拟专网的处理流程 15.9 入侵检测系统 15.9.1 什么是入侵检测 15.9.2 入侵检测的评价标准 15.9.3 攻击检测技术 15.9.4 几种典型的入侵检测系统 15.10 小结
第16章 通信安全 16.1 基本术语 16.2 通信特性 16.2.1 信号的谐波 16.2.2 电话通信 16.2.3 多路复用 16.2.4 数字信号传输 16.2.5 专用线路与交换线路 16.2.6 传输设备和公共载体 16.3 通信媒体 16.3.1 电缆 16.3.2 微波 16.3.3 卫星 16.3.4 光纤 16.4 真实性的丧失 16.4.1 噪声 16.4.2 模拟通信中的噪声 16.4.3 数字噪声 16.5 搭线窃听 16.5.1 物理连接 16.5.2 感应搭线窃听 16.6 通信安全技术 16.6.1 物理安全 16.6.2 加密 16.6.3 用户身份鉴别 16.7 通信安全小结 第17章 走近黑客 17.1 认识黑客 17.1.1 黑客来了 17.1.2 “黑客”是什么 17.1.3 黑客守则 17.1.4 黑客文化背景分析 17.2 黑客手法 17.2.1 黑客攻击的步骤 17.2.2 网络攻击概览 17.2.3 黑客攻击工具举例 17.3 小结 附录A 网络黑客大事记 附录B Internet上的安全资源 附录C 光盘内容介绍 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>