万水网站技术丛书

软件加密解密与计算机安全技术

余东峰 策划　　孙兆林 主编　　灯芯工作室 编著

附光盘

中国水利水电出版社
www.waterpub.com.cn

万水网站技术丛书

软件加密解密与计算机安全技术

余东峰　策划

孙兆林　主编

灯芯工作室　编著

中国水利水电出版社

内 容 提 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。

图书在版编目（CIP）数据

软件加密解密与计算机安全技术 / 孙兆林主编. —北京：中国水利水电出版社，2001.9

（万水网站技术丛书）

ISBN 7-5084-0791-1

Ⅰ.软… Ⅱ.孙… Ⅲ.电子计算机－安全技术 Ⅳ.TP309

中国版本图书馆 CIP 数据核字（2001）第 062771 号

书　　名	软件加密解密与计算机安全技术
策　　划	余东峰
作　　者	孙兆林　主编　灯芯工作室　编著
出版、发行	中国水利水电出版社（北京市三里河路 6 号　100044） 网址：www.waterpub.com.cn E-mail：mchannel@public3.bta.net.cn（万水） sale@waterpub.com.cn 电话：（010）68359286（万水）、63202266（总机）、68331835（发行部）
经　　售	全国各地新华书店
排　　版	北京万水电子信息有限公司
印　　刷	北京市天竺颖华印刷厂
规　　格	787×1092 毫米　16 开本　21.5 印张　462 千字
版　　次	2001 年 9 月第一版　2001 年 9 月北京第一次印刷
印　　数	0001—5000 册
定　　价	40.00 元（含 1CD）

凡购买我社图书，如有缺页、倒页、脱页的，本社发行部负责调换

前　言

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。

本书以实践为主要目的，在讲述必要的原理和技术之外，还提供了大量的源程序和分析讲解。读者除了学习基础知识的讲解之外，可以结合后面的程序对其进行消化和理解，进而掌握设计加密解密程序的技能和方法。全书共分四部分：

第一部分是基础知识讲述，介绍了操作系统、磁盘系统、计算机密码学、计算机病毒和计算机安全技术概况，这些是软件加密和信息安全的基础。

第二部分是软件加密技术的介绍，包括磁盘反拷贝技术、防静态分析技术、反动态跟踪技术以及关于软件加密的一些其他技术，最后介绍了至关重要的现代密码体制和常见的加密算法。

第三部分是软件解密技术，包括加密软件的解密技术、强力攻击技术、密码分析技术。

第四部分是网络安全，着重介绍了计算机网络安全、通信安全和黑客。

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。

本书由余东峰策划，孙兆林、赵青松、李勇等编写，何非仔细审校了原稿，提出了许多中肯的修改意见。在本书的编著过程当中，得到了计算机学院知名教授的悉心指导，得到了相关专家的宝贵意见，在此对他们表示感谢。

由于作者水平有限，书中难免存在一些缺点和错误，衷心希望读者批评指正。

编者

2001 年 4 月

目　　录

第二部分 软件加密技术

第三部分 软件解密技术

第四部分 网络安全

第一部分　基础知识讲述

第 1 章　深入操作系统

操作系统是软件加密解密技术和计算机安全的基础。

总结目前很多加密软件所采用的技术可以看到，它们都是在充分研究操作系统及其支持软件下的一些工具软件后，采取了一系列的措施，或者是利用了工具软件的某些缺限，或者是挖掘了操作系统的一些鲜为人知的重要功能，进行了非常巧妙的程序设计，从而一方面有效地阻止了非法用户的拷贝、解密等操作，另一方面又保证了被加密软件的正常运行。

同时，操作系统的安全又是计算机安全的重要基础。操作系统能够对计算机的硬件和软件资源实行统一的管理和控制。正因为具有如此重要的功能，因而也越容易受到攻击。

所以，要想研究出一种比较有效的加密方法，或者是要保证计算机信息的安全，深入研究操作系统的组成及其工作原理是必要的。

1.1　操作系统概述

计算机的组成可由图 1-1 所示的一个层次结构表示:

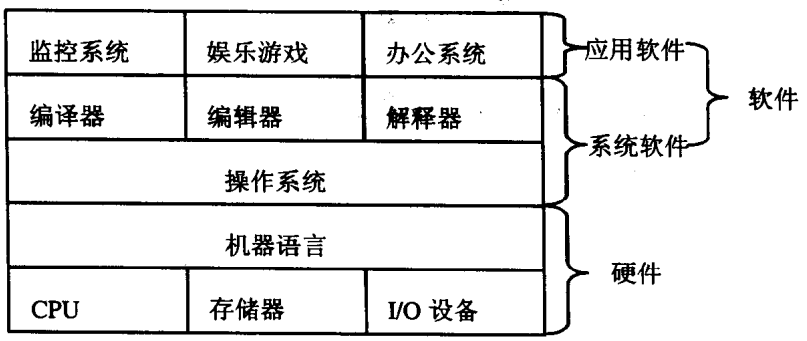

图 1-1　计算机的层次结构

操作系统是计算机一个重要的系统软件，它是计算机软件运行的基础。

在个人计算机上，经常运行的操作系统有 DOS、Windows（Windows3.1、Windows95、Windows98、WindowsNT、Windows2000）、UNIX（XENIX、SCOUNIX），等等。DOS 操作系统是 80 年代 PC 机上最常用的操作系统。Windows 是目前 PC 机上最常用的窗口多任务操作系统。而 UNIX 是多用户计算机上最常用的操作系统，可以运行在众多不同的机器上，既可以运行在个人计算机上（XENIX、SCOUNIX，等等），也可以运行在工作站上（SUNOS、Solaris，等等）。

1.1.1　什么是操作系统

可以简单总结操作系统的工作如下：

（1）负责启动并执行每个程序，并负责完成每个程序的结束处理工作。如在 DOS 系统提示符下键入所要执行的程序名，在 WINDOWS 系统中用鼠标双击可执行程序的图标或名称执行程序。

（2）在任何应用程序中，负责完成应用程序在使用硬件及硬件中的信息时所用的与硬件相关并与应用无关的基本工作。这主要是通过操作系统的系统调用来完成，如在汇编语言中的 INT 调用。

（3）为用户对硬件及所存放信息的基本操作提供现成的实用程序和相应的管理，以使这些操作能很方便和有效地进行。如 DOS 中的 COPY、DIR、FORMAT、XCOPY 等，WINDOWS 系统中的资源管理器等。

（4）改善上述 3 个方面基本工作的效率和安全问题，使计算机系统的各部分和整个计算机系统得到高效安全的利用。

以上 4 个工作似乎相互无关，但它们都具有这样的共性：与硬件相关和与应用无关。

在这里，一个工作是硬件相关的，是指这个工作的实现代码中包含内外存及设备的物理地址，包含对设备接口寄存器和设备接口缓冲区的读写等等。硬件相关的代码必然随硬件的变化而变化。这样的硬件变化包括内外存物理存储空间大小的变化，程序和数据在内外存物理存储空间中的存放位置的变化，设备数量和类型的变化，等等，但不包括 CPU 指令集的变化。操作系统承担硬件相关工作，使其上运行的程序都是硬件无关的，当程序所使用的硬件发生变化（除 CPU 指令集以外）时，程序不必改变，人的操作更不必改变，即使是 CPU 指令集发生改变时，代码的改变也是最小的。

一个工作是应用无关的，是指不管用计算机来做什么，不管在计算机上运行什么程序，只要使用相应硬件或相应信息就要涉及到的工作。它是用户共需的，工作过程相同，有共性可循，却又与应用本身的问题没有直接关系。

操作系统为用户操作和用户程序完成所有硬件相关和应用无关的工作，目的和益处是什么呢？硬件相关，必然意味着复杂烦琐、代码量很大（大到经常占代码比例份量的大部分）、代码不通用和变化大，需要用户投入大量的精力来以了解相应的硬件细节知识实现设计和维护修改，因此有必要统一管理，使用户摆脱负担。应用无关，就意味着有必要统一管理（因为很普遍和频繁地涉及，且与具体应用无直接关系）和能够统一管理（因为工作过程都是相同的）。越是对计算机硬件和信息的使用中的底层的、基本的工作，越具有硬件相关和应用无关的特点，对用户和系统的方便、效率、安全影响也越大，越需要、也值得由操作系统来完成这些工作并解决其中的效率和安全问题。从而使用户程序成为硬件无关的，即独立于硬件，不包括硬件相关的代码。当硬件改变时程序不必改变，这样用户不必考虑这些底层基本使用过程并了解相关的硬件细节知识，避免频繁重复编制（或编译）与应用问题本身关系不大的

大量复杂烦琐的底层代码，从而专心于应用本身，更好地达到最终的具体应用目标。总之，操作系统为保证用户操作和用户程序最终使用的方便、效率、安全，而承担了所有硬件相关和应用无关的工作，从最底层提供统一帮助和管理。

操作系统为用户完成所有应用无关且硬件相关的工作，但这并不意味着操作系统本身的所有功能部分都是硬件相关的。操作系统分为实用程序层、命令解释层、核心层，其中只有核心层才是硬件相关的，甚至在核心（层）内部也做了进一步的隔离，只有核心中最底层的一些模块（例如 Windows NT 中的硬件抽象层，设备驱动程序等）才是硬件相关的。

还可以将上面所讲的操作系统的四个工作进一步归纳为两个方面：

（1）操作系统扩展了计算机硬件系统，提供用户与计算机硬件之间的接口。

在机器语言一级上，多数计算机的体系结构（指令集、存储器、I/O 和总线结构）是原始的，而且编程困难。在裸机上覆盖一层管理软件，提供一个简明的、面向文件的接口，将诸如定时器、存储管理等低层硬件的特性隐藏起来。从这个角度看，操作系统的作用是为用户提供一台等价的扩展机器（Extended Machine），或称为虚拟机（Virtual Machine），它比低层硬件更容易交流。操作系统主要提供两种方式：

命令方式：由操作系统提供一组联机命令（语言），用户可以通过键盘、鼠标等输入设备，直接操作计算机系统。

系统调用方式：由操作系统提供一组系统调用，用户可以在应用程序中通过调用相应的系统调用来操作计算机。

（2）操作系统是计算机的资源管理器。

在计算机系统中通常包含了各种各样的硬件和软件资源。归纳起来可以分为四类：处理器、存储器、I/O 设备以及作为数据或程序载体的文件。操作系统主要针对这四类资源进行有效管理，并协调多个用户对这些资源的共享使用。例如可能有多个程序同时在一台打印机输出计算结果，如果没有操作系统的协调，那么头几行可能是程序 1 的输出，下几行可能是程序 2 的输出，然后又是程序 1 或者程序 3 的输出，结果会一团糟。利用操作系统可以建立打印机的缓冲区来解决这个问题。总之，操作系统作为计算机的资源管理器主要任务是跟踪谁在使用什么资源、满足用户对资源的请求、记录资源的使用情况，以及协调各个用户或程序之间对资源使用请求的冲突。

结合操作系统进行工作的两个基本方面，可以将操作系统定义为：

是一组控制和管理系统资源，合理地对各类作业进行调度、以及方便用户使用计算机的程序集合。

从 1955 年开始出现操作系统到现在的 40 年中，在各种机器上实际运行的操作系统有过几百个，它们中最小的有上万行代码，最大的达几十万行（30 万行 PL/1）甚至几百万行代码（汇编，几千名程序员），甚至更多。在实际运行时它们占用了大量的机器时空资源：占用了 20%～45%的 CPU 时间，最大的操作系统本身占内存空间多达 4～6 兆字节，还占用了大量的外存空间等等。这些数字都说明了操作系统的规模巨大。另外，不同机器上的操作系统