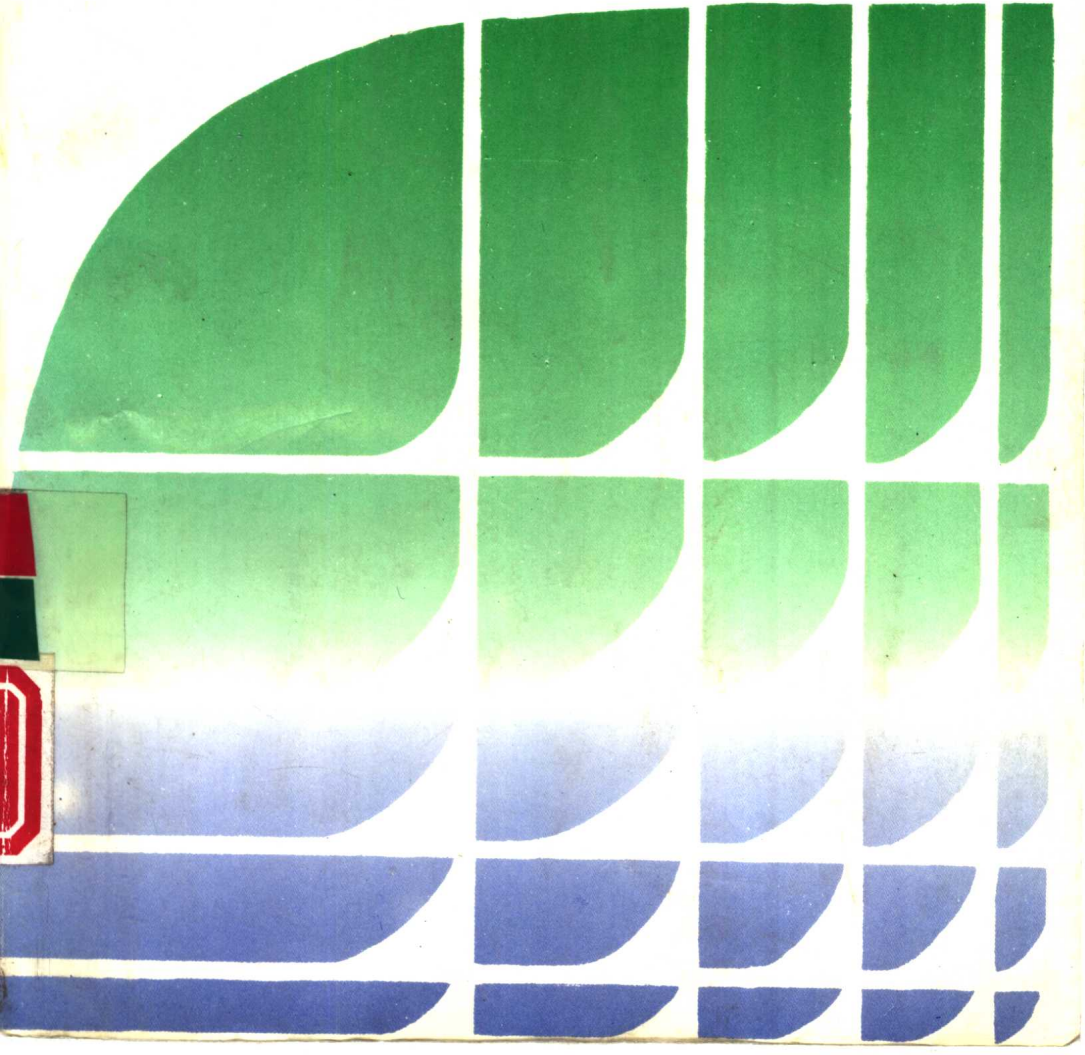
计算机磁盘加密技术

刘 鸣 编著

天津大学出版社



计算机磁盘加密技术

刘　鸣　编著

天津大学出版社

内容提要

本书从实用角度出发详细介绍了计算机磁盘加密的方法。主要内容有DOS的内部结构、磁盘系统的组织管理、反拷贝技术、密文技术、反跟踪技术等。书中结合当前计算机的发展，以高密磁盘为主给出了大量的加密程序。掌握加密技术后，读者可对自己的应用程序做加密保护。

本书是计算机应用人员做加密保护的良师益友，也可供各类学校的教师、学生阅读。

计算机磁盘加密技术

刘 鸣 编著

天津大学出版社出版
（天津大学内）
邮编：300072
河北省昌黎县刷厂印刷
新华书店天津发行所发行

开本：850×1168 毫米 1/32 印张：12 7/8 字数：335 千
1996年10月第一版 1996年10月第一次印刷
印数：1—5000
ISBN 7-5618-0887-9
TP·86 定价：16.80元

前　言

磁盘作为现代计算机的主要外存储设备之一，起到了信息存储和传播的重要作用。目前，计算机的各种软件几乎都是通过磁盘传播得到的。如果不考虑计算机网络的话，计算机信息的共享也是靠磁盘实现的。作为一种特殊商品，计算机软件的销售基本上是通过磁盘实现的。由于磁盘的这种特殊作用，对计算机软件的加密保护在某种程度上说就是对磁盘的加密处理。

磁盘加密问题很早受到人们的重视，随着计算机技术和密码技术的不断发展，磁盘加密技术已达到更新的领域，逐步成为一门特殊的技术。由于磁盘加密所涉及到的学科很多，从 DOS 的内部结构到密码学及抗分析反跟踪程序的设计，都是磁盘加密所要掌握的基本内容。为了使广大计算机用户对软件进行保护，特别是对磁盘加密方法有深入了解，本人编写了这本书。该书的特点是，在掌握了磁盘加密的一些基本要领后，完全可以自己编制出独具特色的加密程序，而且可以应用到所设计的应用软件中去，达到实际使用的效果。

全书共分六章，主要介绍 DOS 的内部结构、磁盘系统、磁盘反拷贝技术、密文技术和反跟踪技术。结合目前广泛使用的 PC 微机，书中给出了大量的实用程序，可供读者深入了解加密过程时参考。

本书在写作期间得到了有关人员的大力支持，并为本书提供了一些参考资料，在此表示衷心感谢。由于本人水平有限，书中难免有不足之处，敬请广大读者给予指正。

作者

1995 年底于天津大学

目　　录

第一章　软件保护概述…… 1
第一节　软件权益的保护…… 1
第二节　软件保护方法…… 2
第二章　深入 DOS 操作系统 …… 7
第一节　DOS 如何加载程序 …… 7
第二节　DOS 的中断系统 …… 15
第三节　DOS 的文件管理系统 …… 37
第四节　DOS 的内存分配 …… 77
第三章　计算机磁盘系统 …… 86
第一节　磁盘及其结构 …… 86
第二节　磁盘的数据记录格式 …… 92
第三节　磁盘的数据组织格式 …… 93
第四节　磁盘参数表…… 100
第五节　簇和逻辑扇区的定位…… 107
第六节　软磁盘驱动器工作原理…… 109
第四章　磁盘反拷贝技术…… 128
第一节　磁盘软指纹技术…… 128
第二节　磁盘硬指纹技术…… 219
第五章　密文技术…… 247
第一节　简单密文方法…… 248
第二节　现代密码技术…… 269
第三节　磁盘文件加密…… 274
第六章　反跟踪技术…… 303
第一节　取消跟踪功能…… 304

第二节　设置跟踪障碍…… 314
第三节　利用特殊中断反跟踪…… 339
第四节　封锁输入/输出设备 …… 351
第五节　利用特殊技术反跟踪…… 365
结束语…… 402

第一章　软件保护概述

现在，电子计算机已成为社会进步、科学技术兴旺的象征。计算机的普及使它成为当今新技术革命中最活跃的因素。它在工业、农业、交通、国防和科学教育等方面发挥着巨大的作用，并使现代化的人类社会进入信息化。作为一种高智能的特殊产品，计算机软件是计算机有效工作必不可少的组成部分。软件产品的开发往往要耗费巨资，并付出大量的人力，而且制作难度大，升级换代快。然而，复制计算机软件却很容易，因而导致非法复制他人软件之风泛滥，严重地损害了软件所有者的合法权益，也影响了计算机的应用和发展。在这种情况下，为了保护软件的合法权益，软件所有者应依靠国家法律和技术手段保护自己的利益。

第一节　软件权益的保护

一套完整的计算机系统是由硬件和软件两部分组成的。与硬件一样，软件现在已成为一种商品，具有一定的市场价值。目前，各国对计算机软件版权问题非常重视，制定了一些法律保护软件研制者的合法权益。在我国，改革开放以来对知识产权问题也十分重视，并不遗余力地推进软件保护法制的建设。在短短的十几年之内，已陆续颁布了《商标法》《专利法》《著作法》和《计算机软件保护条例》，使我国的知识产权法律形成了完整的体系。计算机软件工作者可以依靠这些法律，保护自己的劳动成果。

依据法律，软件所有者享有以下三个方面的权利，即软件表达

形式方面的权利(著作权)、软件设计构思方面的权利(专利权)和软件标志名称方面的权利(商标权)。

在有关法律、法规的作用下,计算机软件产权的保护取得了很大成绩。但是,计算机信息系统保护工作的难度是极大的。要更好地保护软件产权,必须采取法律、科学技术、管理、社会教育和国际合作等多方面的综合措施。但以下两点十分重要。

1. 建立全民法制观念

立法不易,执法更难。建立、建全法律与法规是保护一切知识产权的基础。而提高全民的计算机软件权益保护意识是维护法律法规的保证。应该使人们认识到,侵犯、盗窃他人知识成果是非法的,是犯罪行为。

2. 从科学技术上采取有效措施

要想有效地保护软件产权,除建立全面法制观念外,还必须运用技术手段(如密码技术、反拷贝技术等)对软件进行保护,防止非法用户使用软件。加强这方面的理论研究,制订一系列软、硬件产品安全标准,便能最大程度地保护软件所有者的合法利益。

大多数计算机用户都能够尊重知识产权、尊重他人的劳动成果,仅少数人总是反其道而行之,对加密软件进行解密,与软件保护相对抗。随着软件的更新及各种新技术的不断涌现,这种对抗也愈演愈烈。作为对立的双方,软件加密、解密技术都在不断完善。从某种意义上讲,软件的解密也促进了加密技术的进步。

第二节　软件保护方法

通过加密手段对软件进行保护的方法很多,但指导思想是一致的,即在软件系统中加入一种特殊的信息。这种信息是秘密的,不能被他人察觉,而且在软件的复制过程中也不会被复制过去。由于加密软件在运行中必须用到该秘密信息,所以计算机用户在运

行加密软件时，要完全依靠购买的原版软件。

作为一门特殊的技术，软件加密保护涉及到计算机硬件、软件、密码学等相关领域，为了使加密软件不易破译，在一个加密系统中，往往采用多种保护方法，层层把关。由于各用户的计算机使用情况不同（如单用户使用和联网使用等），所以软件保护方法也不同，主要有磁盘加密、硬件电路加密、数据通信加密、用户身份鉴别、用户访问权限等。

1. **磁盘加密**

磁盘加密实际上是反拷贝加密。它利用一些特殊技术防止对软件的非法复制与仿制。利用加密磁盘存储信息时，除去正常的数据外，磁盘上的特别部位还记录一些秘密信息，即通常所说的“磁盘指纹”。虽然磁盘具有可复制性，但制作精良的磁盘指纹是不能随软件一同复制的。当磁盘具有指纹之后，在磁盘上的软件就有了合法身份，而且有的软件只有在确认为原始磁盘之后才能正常运行。

在国外，磁盘加密技术发展迅速。各计算机公司，特别是计算机软件公司，十分重视磁盘加密工作。他们投入了大量的人力和资金，依靠现代化设备进行研究。对在市场上出售的软件，大都施行加密保护措施，如用于管理的数据库软件 dBASE 和 FoxBASE 都进行了加密处理。在我国，虽然设备不及国外，但依靠计算机技术人员的聪明才智，在磁盘加密技术上也做出了一定成绩。

磁盘加密技术是利用“磁盘指纹”区别正常磁盘与复制磁盘。磁盘指纹又有软指纹和硬指纹之分。软指纹是在不破坏磁盘物理结构的基础上，使用软件方法在磁盘特殊部位上形成指纹；硬指纹是通过专用的设备在磁盘上留下不能被取消的痕迹。比如，美国的 VAULT 公司推出的激光磁盘加密技术就是用激光刻画出人眼难以分辨的磁盘硬指纹。我国计算机工作者采用的针孔加密法也是磁盘硬加密方法。不论是软指纹，还是硬指纹，均要求不能被复制。硬指纹是很容易做到这一点的，而软指纹则有些困难。由于各种拷

贝工具的出现，除少数几种反拷贝方法有效之外，大部分软指纹都难以抵抗专用工具的复制。但在实际应用中，毕竟拥有专用磁盘复制工具的领域并不广泛。因此，磁盘软加密方法仍不失为一种物美价廉的好方法，是目前软件加密的主流。

磁盘加密不单是磁盘反拷贝方法。程序的密文技术和反跟踪技术也是磁盘加密的具体措施。磁盘加密与以往的通信加密不同。因为加密的磁盘要在使用者面前解密。如果没有较好的自封闭系统，是很难对付解密者的攻击的。当加密磁盘具有很强的反拷贝功能后，它所注意的是程序的抗分析上。这包括程序的抗静态分析和抗动态跟踪。防止静分析很容易实现。从早期的密码技术到现代的 DES、RSA 密码体制都能解决这个问题。如果没有解密的钥匙，要想破译密文几乎是不可能的。防止程序跟踪是比较困难的，因为程序运行时要在完全正确的指令格式下工作。这时，就要运用计算机系统提供的一切条件进行特殊编程，如采用逆指令流法、动态解码法等，以破坏或阻碍跟踪，保证加密磁盘有效。

2. 硬件电路加密

硬件电路加密是最近几年广为流行的计算机软件加密方法。它是用一块硬件电路板插在计算机的扩展槽中或并行接口上。也有些加密电路与软件所需的附加卡（如图像卡、汉字卡等）做在一起，使两者合二为一，既减少了占用空间，也起到了软件的保护作用。

硬件电路加密原理是在电路中存有加密程序所需要的数据。电路接口从计算机总线上获取信号并加以处理，再通过总线将结果返回。加密程序的运行正常与否，要依靠加密电路送出数据的正确性。

加密电路最大的优点是工作可靠。但是，为了增加硬件破译的难度，往往在电路的设计上十分复杂（采用大规模集成化的芯片），这又使得硬件电路的成本较高，使用上也不方便。因此，对不需要增加外部设备的软件来说，一般不愿意使用它。

3. **数据通信加密**

普通数据用一定的密码算法加工之后就形成了密文。如果不掌握密钥是无法了解加密的信息的。这在计算机网络广泛应用的今天尤为重要。为了保证数据的安全，通信的双方在传送前将数据加密，接收数据的一方可以由约定的解密方法将数据解密。数据加密会使企图截获信息的攻击者难以了解到实际内容。

4. **用户身份鉴别**

用户身份鉴别的基本方法是由计算机识别使用计算机的人是否为合法用户。如果是合法用户，计算机系统将允许其进行操作，否则将其拒之于门外。使用这种方法，可以对计算机系统中的程序和信息提供一定的保护措施。

口令字(Pass word)识别是常见的一种简易可行的方法。不论是单用户，还是网络中的多用户，口令字只有计算机和用户本人知道。用户上机时，打入相应的口令字后，才能合法使用计算机。有些软件也要视运行它的用户身份合法才能正常执行。

5. **用户访问权限**

用户访问权限是对不同用户访问一些程序和数据的权力限定。一般在多用户系统或网络中使用较多。常使用的权限有以下8种：

①读权限，可读取指定范围内的信息；

②写权限，允许用户在指定范围写入或修改信息；

③读、写权限，具有读、写两种权限；

④读、写、建立权限，除具有读的权限之外，还可以在指定区域建立或删除文件；

⑤自用权限，只允许自己访问；

⑥执行权限，可以执行指定范围内的程序；

⑦移动权限，可以在指定范围内移动信息的存放位置；

⑧证实权限，限定用户在指定范围内证实某种信息是否存在。

不同的软件保护方法从不同侧面起到了软件安全运行的作

用。但不论采取什么样的保护措施，都很难保证软件运行的绝对安全。就磁盘加密而言，解密算法和密钥共存是磁盘加密的特殊所在。它们满足了解密的充要条件，因而理论上可以证明，磁盘加密是可解的。软件加密唯一能够生存发展的原因是依靠解密的难易和解密时间的长短。因为，任何软件都是有一定的生命周期的。理论上的可解性并不等于实际中的可解性。只要在软件的使用周期内不被解密，软件的加密保护就是成功的。这也正是软件保护技术不断发展的原因。

第二章　深入DOS操作系统

自从IBM公司推出微型计算机以来，伴随它的DOS操作系统给用户使用计算机带来了极大的方便。DOS操作系统是用户与计算机系统进行通信的一个接口程序。为了方便用户，DOS操作系统在接口程序中安排了许多功能调用模块，通过中断调用就可以使用DOS操作系统提供的各种服务程序。除去中断调用功能外，DOS操作系统还具有文件管理、程序加载运行、内存分配管理等项功能。掌握DOS操作系统的这些功能对搞好磁盘加密技术有很大帮助。

第一节　DOS如何加载程序

计算机的外部命令和外存储器上的可执行程序，运行时需要在DOS操作系统控制下装到内存，并按照一定的格式完成一些程序的定位等项操作。这中间包括许多DOS的功能调用。下面详细介绍DOS加载程序过程。

1. COMMAND处理命令过程

计算机系统启动后，屏幕上出现“C>”号的提示符，此时系统已在COMMAND控制之下，用户可以输入各种命令（包括内部命令、外部命令或批处理命令），使DOS执行相应的程序。

DOS执行命令是有顺序的，即优先处理内部命令。内部命令包含在COMMAND的暂驻内存部分，位于内存的高端。若输入命令不是内部命令，DOS系统执行命令的顺序为：.COM文件第

一，.EXE 文件第二，.BAT 文件第三。当命令是一个.COM 文件或.EXE 文件时，COMMAND 就调用系统的 EXEC 子功能加载该文件并执行之。执行时，首先在 DOS 常驻内存部分之上的可用内存空间最低端建立一个名为程序前缀的控制块 PSP。该控制块中包含命令行参数、文件块、环境块地址以及系统内部使用的若干附加信息。若是.EXE 文件，还需对程序的各段进行重定位。最后，被加载的程序位于 PSP 的上方，"CS：IP"指向程序的第一条指令，程序正常运行。

当命令为批处理文件的文件名时，转入 COMMAND 暂驻内存部分的批处理程序，以解释和执行该文件中的每一条命令。这些命令可以是内部命令、外部命令或批命令。批命令的最后一条命令还可以是另一个批文件名。当所有命令执行完毕，返回到 DOS 提示符下，准备接收新的命令。

2. 程序段前缀 PSP

当 DOS 用 EXEC 子功能加载一个程序时，首先要在内存可用空间的最低端建立一个程序前缀 PSP。这个前缀控制块中包含程序重定位(对.EXE 文件)和运行时需要的若干信息。这些信息包括下面几项。

(1)供 DOS 本身使用的入口

该入口信息存放在 PSP＋0AH、PSP＋0EH、PSP＋12H 和 PSP＋2CH 四个字段中。其中，前三个字段存放了中断 21H、23H 和 24H 的原始中断向量。这三个中断分别用于程序的结束处理、CTRL—C 处理和严重错误处理。之所以要保留这三个中断向量，是为了允许用户在程序中修改和接管其中一个向量，以便自己处理这三类问题。当被加载的程序运行结束返回 DOS 时，DOS 系统就自动恢复上述三个中断向量。

PSP＋2CH 字段包含了环境块的段地址。环境是由一系列字符串组成的。例如，"COMSPEC＝"指示命令处理程序在盘中的位置；"PATH"指示待搜索的路径等。环境块中的信息是程序被加载

时从 DOS 中获得的。

(2)供被加载程序使用的入口

该类信息位于 PSP+00H、PSP+02H、PSP+05H 和 PSP+2CH 字段处。PSP+00H 字段中有一条 INT 20H 指令。该指令是 DOS 提供的终止程序运行并自动恢复 INT 22H、INT 23H 和 INT 24H 中断向量的中断例程。它同时通知 DOS 释放被应用程序占用的内存,将控制权交给 COMMAND.COM。PSP+02H 字段含有 DOS 分配给被加载程序使用的内存高端地址,它表明了内存的总量。PSP+05H 字段含有 DOS 系统功能调用 INT12H 远调用入口。PSP+2CH 含有环境块的地址。

(3)供被加载程序使用的参数

该类参数位于 PSP+5CH、PSP+6CH 和 PSP+80H 字段处。

PSP+5CH 和 PSP+6CH 两个字段包含两个格式化后的文件参数。COMMAND 在处理一个外部命令时,将命令字后的两个文件名参数解释为两个未打开的文件控制块 FCB。在执行中,被加载程序可以用串传送指令将这两个字段的内容移到指定区域使用。当第一个文件控制块处于打开状态时,则按打开的 FCB 格式覆盖 PSP+6CH 字段中的第二个文件控制块。

PSP+80H 到 PSP+FFH(共 128 个字节)是非格式化参数区,其中前 28 个字节用作缺省的磁盘传送区 DTA。

由以上分析可以看出,总长度为 256 个字节的程序前缀 PSP 包括了许多运行参数。通过对 PSP 编程,可以实现系统功能调用、设置环境块和终止程序运行等功能。

3. .COM **文件的加载原理**

.COM 文件又称为"映象文件",因为它在磁盘上的存储结构与在内存中的分布是一致的,即.COM 文件在加载时不需要对各段进行重定位..COM 文件的这种性质决定了它的长度不能超过一个段(64kB),并且结构紧凑、加载速度快。这种文件适用于小型程序。

.COM 文件的结构有如下规定：

①程序只能有一个统一的段，且不能另外设置堆栈段。在汇编、链接.COM 文件时，会出现“没有堆栈段”的警告，对此可以不理会。

②程序必须小于 64kB。

③程序要预留 100H 长的空间，且第一条执行指令必须在位移 100H 处。

④程序的起始标号要用 END 语句说明其为开始地址。

⑤程序全部采用近调用(NEAR)。

以下是.COM 文件结构的例子：

```
name        comfile
code        segment public 'code'
            org 100h
            assume ds:code,es:code,ss:code
start       proc near
            ..........
start       endp
code        ends
            end start
```

DOS 加载.COM 文件时，首先在内存可用端的最低处建立一个相应的程序段前缀 PSP，紧接着 PSP 的上方将.COM 文件装入，并置 IP 值为 PSP+100H。这就说明为什么.COM 文件要预留 100H 字节空间并将第 1 条指令放在 ORG 100H 处的原因。留下的 100H 字节空间被 PSP 占用。表 2—1 是.COM 文件加载之后的内存映象。

表 2—1 .COM 文件加载后的内存映象

内存地址	内　容
0000H—	中断向量表
40：00H—	DOS 常驻区

续表

CS=ES=DS	程序前缀 PSP
CS：IP	.COM 文件代码段
SS：SP	堆栈区
	00H
	00H
	剩余空间
RAM 高端	DOS 暂驻区

由.COM 文件加载之后的映象可以看出,.COM 文件的堆栈由 64kB－2 字节处向上生长。当内存不足 64kB 时,SP 的初始值等于可用内存数减 2。

4. .EXE 文件的加载

.EXE 文件又称为“重定位文件”,这是因为它在磁盘上的存储结构与加载到内存后的分布是完全不一样的,即.EXE 文件在加载时需要对各段重新定位。.EXE 文件的这种性质决定了它的长度可以突破 64kB 的限制,但同时也使它具有占用磁盘空间多、加载速度慢的特性。.EXE 程序可以控制系统几乎所有的资源。因此,它适用大、中型程序。

.EXE 文件的结构有以下规定：

①该程序允许有若干个不同名的代码段、数据段、附加段或堆栈段。

②程序的长度可以大大超过 64kB,它仅受可用内存空间的限制。

③程序的入口不一定在 100H 处,只需要起始标号与 END 语句说明的起始地址一致即可。

④程序中既可以有 NEAR 调用,也可以有 FAR 调用。

由于.EXE 文件需要重定位,所以链接程序 LINK 在链接程序时生成一个控制块,即重定位信息块,又称.EXE 头文件。应将