如何实现文件与子目录的加密

刘宪权　（中国矿业大学）

使用微机的用户有时想采取一些加密方法把自己的某些文件或子目录加密，以防止别人看到、调用、执行或拷贝删除等操作，本文就笔者的一些使用经验对文件及子目录加密方法作一概括总结，以供大家参考。

一、文件加密

1.口令法

口令法是防止无关人员擅自招待磁盘中某一可执行文件的一种加密方法。它是在编程时，设置口令及相应的输入指令，当编译连接产生执行文件后，无关人员无法查到口令，执行文件时，先提示输入口令，若用户输入的口令与预先设置的相同就执行；若不同，则重复询问几次(次数可随意设定)，若连续几次键入的口令都不下确，则拒绝用户执行该文件。

2.磁盘目录项加密法

在 DOS 操作系统格式化的磁盘中，每一个文件由文件分配表(FAT)分配一个 32 个字节的目录项，该目录项定义了该文件的文件名、扩展名、文件属性、文件生成或最新修改的日斯、时间文件开始簇及文件大小，文件目录表中目录项的格式如图 1 所示。

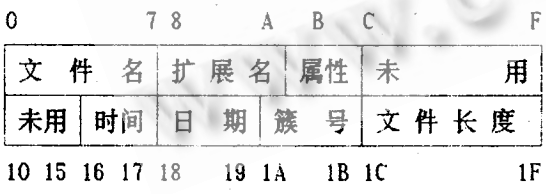

图 1　目录项格式表

操作系统把所有目录项集中在一起形成的个目录表，并在磁盘上自动开壁一个存放目录表的区域，称为目录区，常见的磁盘格式见表 1。

表 1　常见磁盘格式表

磁盘介质	磁盘容量	BOOT 逻辑扇区	FAT1 FAT2 逻辑扇区	DIR 逻辑扇区	DATA 逻辑扇区
软盘	360K	0	01～04H	05 ～0BH	0CH开始
软盘	1.2M	0	01～0EH	0FH～1CH	1DH开始
硬盘	10M	0	01～14H	15H～34H	35H开始
硬盘	20M	0	01～52H	53H～72H	73H开始
硬盘	33M	0	01～80H	81H～A0H	A1H开始

逻辑扇区可由物理扇区换算得到，以双面双密盘为例：物理扇区是按 0 面 0 道 1 区，0 面 0 道 2 区，…0 面 0 道 9 区，0 面 1 道 1 区，…0 面 1 道 9 区，…0 面 39 道 9 区，1 面 0 道 1 区，…1 面 39 道 9 区排列，而逻辑扇区与物理扇区的关系为 0 面 0 道 1 扇区至 9 扇区，逻辑扇区号为 9-11H，0 面 1 道 1 扇区至 9 扇区，逻辑扇区号为 12-1AH，…，这样每道先 0 面后一面一直排下去。

操作系统通过文件目录项中的各种信息了解、使用和处理文件，因此，可以巧妙地修饰文件目录项中的有关信息，使 DOS 或 PCTOOLS 无法了解、使用和处理该文件，从而达到加密的目的。具体方法有修改目录项第一字节的方法、修改文件名的方法、修改目录项文件属性的方法、修改文件开始簇的方法及修改文件长度的方法。

(1)修改目录项第一字节。在文件管理系统中，文件目录项有三种状态，即未使用状态、使用状态各删除状态。所谓未使用状态是该目录项未存储任何文件信息因此，可以用于记录新建立的文件名及其有关信息；使用状态是该目录项存储某一文件名及其有关信息；删除状态是该目录项原来记录了某一文件名及其有关信息，而现在用户已经宣布该文件已被删除，但实际上，原文件的有关信息仍然记录在该目录项中。

文件目录项的这三种状态是由目录项第一字节来标

记的,第一字节为 00H, 表示未使用状态;第一字节为 E5H,表示删除状态;其它是使用状态。文件管理系统总是从文件目录表的上部依次寻找一个未使用或删除状态的目录项,给新建立的文件使用,以便存效地利用磁盘空间。未使用状态的目录项都集中在目录表后部的连续区域里,所以当某一目录项的第一字节为 00H 时,表示该目录项及其后所有目录项均处于未使用状态。当用 DIR 命令查看时,凡是未使用和删除状态的目录都不会显示出来。根据这一原理,为保护某一文件,可用 DEBUG 或 PCTOOLS 改变目录项第一字节为 00H 或 E5H, 这样加密后用 DIR 看不到,PCTOOLS 的文件服务功能也不显示。具体做法如下:

①用 DEBUG 软件(以 5.25″双面双密软盘为例)

a.进入 DEBUG

A＞debug↓

b.装入目录表

-L100 0 5 7 (100 为装入目录表的当前段的偏移置;0 表示 A 盘;5 表示目录表从盘上逻辑扇区 5 开始装入;7 表示共装入了 7 个扇区)。

c.显示目录内容,找到要修改的目录项地址(可从右边 ASCII 码来判别要处理的目录项)。

-D 100(可多次使用 D 命令直到找到要处理的目录项为止)。

d.修改目录项内容

-E＜地址＞＜新内容＞

＜地址＞为欲修改的目录项字节的编移地址;

＜新内容＞为欲改成的新内容。

e.将修改后的目录表写入磁盘目录区

-W 100 0 5 7

②用 PCTOOLS 软件

a.进入 PCTOOLS,按 F3 进入磁盘服务功能。

b.用编辑命令 E 选盘,显示出 BOOT 扇区的十六进制及 ASCII 码。4c.按 F2,在菜单中选 R(第一个根目录区),按 F3 进入编辑状态,此时即可用光标改动内容,然后按 F5,U 存盘。如果用户要加密的文件在子目录中,则在菜单中选 C 输入子目录起始簇号(找到该簇号的方法本文后边将介绍)。

这种第一字节改变为 OOH 或 E5H 的加密方法实施之后,当事者自已也不能看到该文件,要想使用、查阅文件文件,必须先用 DEBUG 或 PCTOOLS 用前述方法改回原值,因此一定不能忘掉原值。加密后不能再进行磁盘写入操作,否则可能把加密的目录项和与它相关的存储区重新分配给其它文件。

(2)修改文件名。用上述方法修改文件名的一部分或全部,使之变为无法用键盘直接输入的字符,主要使用一些不常见的 ASCII 码,这样尽管 DIS 显示, 但一般用户难以输入文件名。

(3)修改目录项文件属性的方法。

文件目录项的第十一个字节(OBH)是文件的属性字节,一个文件根据它的用途可以有不同的属性,如只读文件、隐藏文件、系统文件、卷标文件、子目录文件。目录项中文件属性字节各位的含义如图 2 所示。

b_7	b_6	b_5	b_4	b_3	b_2	b_1	b_0
×	×	更改位	子目录	卷标位	系 统	隐 藏	只 读

图 2 文件属性字节各位含义

其具体含义如下:

b0＝1,其值为 01H,表示文件是只读的

b1＝1,其值为 02H,表示隐藏文件

b2＝1,其值为 04H,表示系统文件

b3＝1,其值为 08H,表示卷标

b4＝1,其值为 10H,表示子目标

b5＝1,其值为 20H,表示归档位,当文件已写入和关闭时,引位置为 1(b5＝1)

b6,b7 为保留位,取 0。

文件属性共有六种,其中有些属性可组合使用,要注意的是卷标位与其它属性相加是无意义的,子目录与更改位相加则引起混乱。除此之外,属性可任意组合,例如,01H+01H＝03H(对应 b0,b1 为 1)。由于当文件写入和关闭时 b5＝1,因此当查看到的属性字节多为 20(普通文

件)、27(DOS 系统文件)、28(卷标)。

根据以上原理,用前述工具及方法修改属性字节内容即可加密,若要加密普通文件将 0BH 字节内容改为 03 或 02 即可,要隐藏系统文件把 0B 字节内容改为 07 即可,要隐藏子目录将 0BH 字节内容改为 17 即可。

用这种方法加密的文件大部分不影响调用及执行,因此此法被用户广泛使用,某些加密后不能执行的文件如.EXE 文件.COM 文件,可先把它们拷入一个子目录中,再将子目录加密。

(4)修改目录项文件开始簇。磁盘存储文件是以簇为单位的,一个簇由几个扇区组成;一般扇区数为 1,2,4,8 等几种规格,在磁盘中存储一个文件可能需要几个簇,第一个簇,称为文件开始簇。

修改文件开始簇的方法,是不管目录文件中开始簇的值为多少,把其值改为 00H,这样加密后,虽然可用 DIR 列出,但无关用户因找不到文件入口地址而无法查阅该文件,用户一定要记住原值,使用时改回。

(5)修改文件长度。将目录项长度字节最高位置为 1,此时,DIS 可显示,PCTOOLS 不显示,也不影响文件使用,可和前面几种配合使用。

3.直接命令法

这种方法是利用一些输入技巧或直接命令来实现对文件的加密,以可分为几种:

(1)软件本身自带设置密码命令,如 CCED、WPS、BASIC 的 P 命令存盘等。

(2)DOS 的 Attrib 命令,如:

A>Attrib file1,可显示文件属性;

A>Attrib +R file1,文件属性改为只读;

A>Attrib −R file1,文件属性去掉只读;

(3)特殊文件名法,主要采用怪字符或不可见字符,无字符区位码、半个汉字等办法来达到对文件名的加密。

二、子目录加密

如果用户需要加密的文件较多或不想让别人看到自己的子目录,可以采取加密子目录的办法。子目录加密一般不影响文件的执行,如果为了更加安全,也可以把文件也加密起来,达到双重效果。

子目录加密主要是在目录项上作文章,前面已经提到,目录项 0BH 字节为 10H 的是子目录,如果把 10H 改为 17H,则达到了加密的目的,用 DEBUG 和 PCTOOLS 均可,PCTOOLS 更快且方便。这样 DIR 命令就不显示该子目录了,如果再把该目录项的节 1FH 字节内容改为 FF,PCTOOLS 也不再显示,这个子目录不再列于目录树,但不影响子目录的下常使用,如果想用 PCTOOLS 对该子目录操作,则把 1FH 字节的值改回 00 即可。

如果用户还想加密一级子目录下的二级子目录,则只要记住一级子目录的起始簇号,换算为十进制,然后在 PCTOOSL 磁盘服务功能编辑状态下,按 F2,选 C,把上面得到的十进制簇号值输入,即可得到一级子目录下的文件目录及二级子目录,然后用同样办法加密。

找到下级子目录目录项的办法还可用 PCTOOLS 磁盘服务功能的 MAP 功能,选 M 后,选盘,按 F 显示单个文件映像,按 F10,选择所需子目录,按 G,按←键即可得所需子目录的起始簇号,该值为十进制,然后再进入 E 编辑,输入簇号即可加密二级子目录,三级或更深层次子目录加密方法相同。

子目录加密还有一种方法,是子目录簇号循环法,就是使后一级(或后几级)子目录的起始簇号改为前级子目录的起始簇号,这样 PCTOOLS 进入选盘,画目录树的过程中就会进入死循环,导致不能工作,这种方法付出的代价是 PCTOOLS 对该子目录所在盘的操作失效并导致假死机,因为大多数用户加密子目录是在硬盘上,PCTOOLS 不能对硬盘操作,带来的损失是很大的,所以笔者建议一般用户不要轻易用此法。

当然子目录加密也可用特殊字符名法及用 PCSHELL 的子目录属性命令,这里不再详述。

下面是需要注意的几点:

(1)运行 DEBUG 和 PCTOOLS 的各步要十分仔细,不能因误操作修改了不应修改的内容,必要时,可在纸上记下操作过程中的各个数值,以防止误操作导致严重后果。

(2)因加解密常用到一些 ASCII 码及其十六进制值,最好记住一些常用字符的十六进制值。如记不住要备有 ASCII 码字符表。

(3)文件和子目录加密方法较多,可结合起来使用,以满足不同等级的加密要求。