硬盘文件的保护*

韩立毛
(盐城工专基础科学部,盐城,224003)

摘 要 硬盘文件的保护在当今微机维护中是一项十分重要的工作,关系到微机能否正常工作以及能否充分发挥性能。给出了一些保护硬盘文件的具体方法和措施,这些方法和措施对于指导工作实践将起到积极的作用。

关键词 主引导扇区 文件首簇号 文件簇号链 子目录首簇号
分类号 TP33

1 问题的提出

随着微型计算机技术的迅速发展,性能不断提高,功能不断增加,硬件配置在不断更新,大多数微机都有容量可观的硬盘。由于硬盘存贮容量大,读写速度快,所以一般用户将常用的软件都存放于硬盘上,以方便使用。又由于一台微机常常可能有多人使用,故应采取一些措施和方法保护硬盘上的文件,以防止文件被非法拷贝、病毒感染硬盘上的文件、文件的非法删除等。这里就硬盘文件的防拷贝、硬盘文件病毒的预防、硬盘文件的非法删除作一讨论。

2 硬盘文件的保护方法

2.1 采用文件防拷贝技术保护硬盘文件

对于硬盘上一些重要文件应采用防拷贝方法以防他人非法拷贝,硬盘文件防拷贝方法主要可采取两种方法,即主引导扇区设置密码防拷贝和利用文件首簇号防拷贝。

2.1.1 主引导扇区设置密码防拷贝

在IBM PC及其兼容机上,硬盘主引导扇区是一个特殊的扇区,它是独立于DOS分区的一个扇区,仅利用DOS的系统功能调用是读取不到这一扇区的内容的。在该扇区中存放有硬盘主引导程序和硬盘分区的信息。一般引导扇区占用的扇区在偏移地址0000—00D9H,而硬盘分区表则从偏移地址01BEH开始存放直至01FDH,结束标志为AA55H。在硬盘主引导程序与硬盘分区表间大约有222个字节是空白区,如果硬盘安装程序在此空白区域设置一个密码,并在被存放到硬盘的加密软件中编写一段程序,读取主引导扇区的这一密码,如果发现密码,则程序正常运行,否则进入死机状态。如果有人试图将加密软件拷贝到另一台微机上使用,由于没有将硬盘主引导扇区中的密码设置到另一台微机的主引导扇区中,因此被拷贝的文件在另一台微机上是无法运行的。这样,被加密的文件就具有了防拷贝的功能。

2.1.2 利用文件首簇号防拷贝

文件首簇号是表示文件在磁盘上所占用的开始扇区的逻辑位置,由于不同类型的硬盘其

* 收稿日期:1996—01—03

柱面数、磁头数、每个柱面上的扇区数都是不尽相同的，所以，对于一个文件来说，如果同时被拷贝到两个硬盘上，其首簇号一般是不相同的。即使是同一类型的硬盘，由于各自在存贮介质上文件的建立、修改与删除操作情形是不同的，文件的数目、子目录数也不尽相同，所以磁盘空间的使用情况也就不尽相同，这样即使同一文件装入到两个类型相同的硬盘上，它们所占用的首簇号一般也不会相同。

文件首簇号的获取与安装操作由安装程序完成，安装程序的主要工作：将被加密的文件拷贝到硬盘目录或某一子目录下，读取该文件的首簇号，将首簇号以明文或密码的形式写入到被加密文件的规定的地方。

文件首簇号的识别操作由被加密程序完成，在被加密程序中编写一段程序读取自身文件的首簇号，将读取的结果与程序中由安装程序事先安装的首簇号进行比较，如果发现两者相同，则使程序正常运行；如两者不同，则使程序转入死循环状态。

2.1.3　利用文件簇号链保护硬盘文件

在实际应用中还可以使用硬盘文件自身的簇号链对被加密文件的主程序进行加密变换，即以硬盘文件的簇号链为加密密钥对文件本身的主程序进行加密变换，再加上动态跟踪技术，就可以使磁盘上的文件得到有效保护。这是由于即使同一个文件安装在相同类型的硬盘上，由于两个硬盘上文件的个数以及用户对这些文件的建立、修改和删除操作的情况是不相同的，所以同一个文件被拷贝到两台微机的硬盘上，不仅两个文件各自占用的簇号不同，而且簇号链上的所有簇号一般也不相同。因此，使用硬盘文件簇号链上的所有簇号作为加密密钥能有效地保护硬盘文件。

2.2　预防病毒感染硬盘文件

几年来，已发现数千种计算机病毒及其变形在世界各地传播，其危害已引起了世界范围的恐慌和警觉。目前，我国出现的计算机病毒主要攻击IBM PC及其兼容机，大约有上千种。

计算机病毒对微机的危害程度是相当严重的，主要危害有：破坏硬盘的分区表、文件分配表和目录表；删除、修改和破坏磁盘文件；反复感染、拷贝，造成磁盘空间减少，并影响系统的运行效率；对整个磁盘进行非法格式化，破坏全盘文件；在DOS内存参数区写入非法数据，使系统陷于瘫痪。由于硬盘容量之大，文件之多，一旦感染上病毒，传播快，影响大，严重者致使整台机器无法正常工作，从而陷于瘫痪状态。

预防计算机病毒破坏或感染硬盘文件的主要途径是阻止病毒入侵硬盘。要阻止病毒入侵硬盘，则必须加强管理，并辅之以一定的技术措施，这些管理手段和技术措施主要有：1、尽量不采用软盘启动机器，尤其不能用来历不明的系统盘启动机器；2、计算机启动前后均应进行病毒检查，以便及时发现和清除病毒。如：采用BOOTSAFE.EXE程序监视主引导扇区和文件分配表，一旦主引导扇区被破坏，就可以用备份文件恢复原来的主引导扇区。再者用VSAFE.COM程序驻留内存动态监视病毒的活动情况；3、对硬盘上的重要文件要定期备份；4、对一切外来磁盘在使用之前必须进行病毒检查，确保无病毒感染；5、可采用硬盘分区保护的办法防止病毒进入硬盘分区，从而保护分区里的文件。

2.3 防止硬盘文件的非法删除

2.3.1 防止硬盘误被格式化

PORMAT.COM是DOS中一个较常用的命令，因为启动新盘需要用它进行格式化，但是

FORMAT.COM 又是个危险的命令，稍不留心就会把磁盘上所有文件删除掉。为了防止硬盘被意外格式化，可将 FORMAT.COM 文件用 DEBUG 程序修改一下，使之在执行 FORMAT C:时，显示一信息"是否真的要对硬盘进行格式化？"若是，则敲"Y"，否则敲"N"，这样就可防止硬盘误被格式化。此外，也可以将硬盘的卷标修改为大写字母表示，使 FORMAT C:不能对硬盘进行格式化。当然，防止硬盘误被格式化还有其它方法，这里不再介绍。

2.3.2 用 DM 或 ADM 软件对硬盘分区加密

DM 和 ADM 都是磁盘管理软件，一般用于对硬盘进行分区管理、低级格式化与高级格式化、读写检验与磁盘诊断等。用 ADM 软件可以把一个物理硬盘划分为几个逻辑盘，每个逻辑盘对应一个分区，给每一个分区设置一个口令及读写权限，同样，用 DM 软件也可以给每一个分区设置读写权限。这样一来，用户就可以把一些重要文件或常用软件集中放于一个分区中，同时用 DM 或 ADM 把此分区设置为写保护。因此，对于这个分区用户只能读出文件而不能写入文件，也不能删除文件，从而达到保护硬盘文件的目的。另外，DM 软件还可以通过修改 CONFIG.SYS 文件来隐藏逻辑盘，若删除 CONFIG.SYS 中 DEVICE=C:\DMDRVR.BIN 一项，则逻辑盘 D·E 等都不会被启动，从而起到了对逻辑盘 D·E 上文件的保护作用。

2.3.3 改变子目录首簇号使其下的文件隐含

前已述及采用改变文件首簇号的方法防非法拷贝，这里讨论通过改变子目录首簇号使其下的文件隐含的方法。假设在硬盘目录下建立一个两级子目录系统：根目录——USE——HLM，首先将这两个子目录项的第 11 个字节的内容由 10H 改为 12H，使这两个子目录为隐含，然后再修改 USE 子目录下的两个目录项.和..的首簇号，即把 2E 目录项的首簇号修改为 HLM 子目录的首簇号，再把 2E2E 目录项的首簇号修改为 USE 子目录的首簇号，这样用 PCTOOLS 或 CHKDSK 等虽然可以查出隐含的子目录名，但是用 DIR 命令却看不到隐含的子目录，由于改变了子目录的首簇号，使 PCTOOLS 中的大部分功能失效，因为它们一动作就会陷入所设置的死循环中，从而造成死机，这样也就保护了子目录下的文件。

3 结束语

综上所述，硬盘文件的保护在当今微机维护中是一项十分重要的工作，前面给出了一些保护硬盘文件的具体措施和方法，可用于具体实践工作中。可以这样认为，硬盘文件保护的方法还有很多，而且随着微型计算机技术和软件的发展，必将推出更多更新的硬盘文件保护方法。