子目录隐含加密方法

瞿 波 (湖北荆州师范专科学校计算机系)

摘要:在找出 *PCTOOLS* 显示子目录时其目录项必须满足的四个条件后,提出了如何使子目录在 *PCTOOLS* 下不被显示的对策,归纳出了两个在子目录隐含加密方面具有重要作用的公式,给出了四个具体的子目录隐含加密法,最后举了一个加密实例。

PC 机用户常将子目录置成隐含,使之在 DOS 下不被显示,以达到保密的目的。传统的子目录隐含方法是将子目录目录项的文件属性字节值置成 12H 或 17H,但经过这样处理的子目录在功能强大的工具软件 PCTOOLS 下却暴露无遗!而且现在 PCTOOLS 的使用又很广泛。因而,传统的加密法其保密性能大为减弱。现在的问题是能否找到对付 PCTOOLS 的方法,使隐含子目录在 PCTOOLS 下也显示不出来。如果能找到这样的方法,子目录隐含加密法将获得新的生命力。

1.PCTOOLS 对子目录目录项的要求

PCTOOLS 在搜寻子目录时,若目录项符合下列四个条件,即认为是有效子目录,并在子目录树结构图上显示出来。

(1)目录项属性字节值具有子目录标志 10H,若属性字节值为多种属性的组合,但只要能分解出 10H 也可,如 12H=10H(子目录)+02H(隐含),17H=10H(子目录)+01H(只读)+02H(隐含),04(系统)。

(2)具有合法的子目录名,即子目录名要符合 DOS 对文件名的要求。

(3)目录项中标记的起始簇号不能大于磁盘数据区的最大簇号(磁盘数据区即磁盘格式化后提供给用户的可用空间)。

(4)目录项中标记文件长度的字节值可以不为 0,但其值不能大于磁盘数据区的最大字节值。

上述四个条件可看成是 PCTOOLS 判别子目录的重要条件,只要其中任一条件不满足,PCTOOLS 就不会在目录树上显示相应的子目录。

2.屏蔽子目录的对策及两个重要公式

知道了 PCTOOLS 在显示子目录时对子目录目录项的要求,不难找到对付 PCTOOLS 的方法。我们可以通过 DEBUG 程序或者 PCTOOLS 程序本身提供的阅鉴编辑功能,对根目录下子目录的目录项进行修改,使之不符合 PCTOOLS 的要求,从而使子目录在 PCTOOLS 下不被显示。若分别从文件属性、子目录名、起始簇号及文件长度四个方面进行修改,就会获得四个对付 PCTOOLS 的方法。

在修改起始簇号或文件长度时,必须先知道磁盘数据区的最大簇号或数据区的最大字节值。由于目前所使用的磁盘其规格形式、容量多种多样,最大簇号、最大字节值各不相同,即使是同一张磁盘,在不同的 DOS 版本下格式化,其最大簇号,最大字节值也有不一样的情况。那么,如何知道所使用的磁盘数据区最大簇号和最大字节值呢?笔者归纳出了两个公式,可方便的计算出每个磁盘数据区的最大簇号和和最大字节值。

(1)计算最大字节值 K

$$K=(S-(1+2\times F+N\times 32/512))\times 512$$

(2)计算最大簇号 C

$$C=(S-(1+2\times F+N\times 32/512))/M+1$$

公式中,S 为磁盘的总扇区数;F 为一 FAT 表所包含的扇区数;N 为根目录所能容纳的最大文件个数;M 为每簇包含的扇区数。

S,F,N,M 的值,可从磁盘的逻辑 0 扇区中查得,S 值在 0 扇区的 13～14H 字节中,F 值在 0 扇区的 16～17H 字节中,N 值在 0 扇区的 11～12 H 字节中,M 值在 0 扇区的 0DH 字节中。若为两字节表示的值,则低位在前高位在后。

在计算 K 和 C 时,须先将查得的 S,F,N,M 的 16 进制值化成 10 进制值,再代入计算。在修改起始簇号、文件长度时,须再将 K 和 C 化成 16 进制值。

3.四个具体的加密方法

(1)将目录项属性字节置成 02H。目录项的 0BH 字节为属性字节。

将子目录目录项的属性字节值置成 02H 后,由于只有隐含标志 02H,而无子目录标志 10H,因此,PCTOOLS 将该目录项表示的子目录忽略,不予显示。

同时,由于无子目录标志,DOS 也不承认该目录项表示的子目录,也不予显示。

当自己要采用这种方法加密的子目录时,须再在属性字节值中加进 10H。

(2)将子目录各中的字符改成怪字符,同时,将属性字节值置成 12H 或 17H

目录项的 00H～0AH 字节为文件名字节。将目录项文件名字节中表示子目录名字符的 16 进制码换成 80H(128D)～FFH(255D)中的某个值(即产生怪字符的码),使子目录名成为非法的。于是,PCTOOLS 无法将该目录项表示的子目录显示出来。但此时在 DOS 下该目录项表示的子目录仍会显示,故在将子目录名改成非法的同时,还须将子目录置成隐含的,以防子目录在 DOS 下被显示。由于有非法子目录名对付 PCTOOLS,所以,此时将属性字节值置成 12H 或 17H 即可。

采用这种方法加密的子目录,在 PCTOOLS 和 DOS 下均不显示,但在 DOS 下可进入使用该加密子目录。方法是在键入子目录名时,通过 ALT 键和小键盘中的数字键按出子目录名中的怪字符。

(3)使起始簇号大于磁盘数据区最大簇号加 1。目录项的 1AH～1BH 字节的值为起始簇号。低位在前,高位在后。

将起始簇号改成磁盘数据区最大簇号加 1(若最大簇号为 355,则改成 356),PCTOOLS 在搜索目录时,会给出"Sector not found"(找不到扇区)的信息,而不显示任何目录。这样,虽然在 PCTOOLS 下隐藏了欲加密的子目录,但磁盘上其它的文件也都被隐藏起来,这似乎不太合适(当然,在某种场合,这也可看成是一个重要的加密方法,笔者在文献[3]中讨论了其应用),不过,只要我们将起始簇号改成大于最大簇号加 1,使之成为最大簇号加 2～65535(FFFFH)中的某个值,就可以只隐藏欲加密的子目录而不影响其它的文件。

(至于如何获得最大簇号,前面已给出了计算公式。)

将起始簇号作了上述修改后,其子目录在 PCTOOLS 下不被显示,在 DOS 下却仍会显示,但此时子目录已不可随便使用了,一旦对它进行操作,将会得到"File allocationtable bad"(文件分配表坏)的信息。为了使加密子目录在 DOS 下也不被显示出来,还须将属性字节值置成 12H 或 17H。

当自己要采用这种方法加密的子目录时,须再将起始簇号改为先前正确的值。因此,必须将正确的起始簇号记录在备忘录上,以防日久遗忘。

(4)使文件长度值大于磁盘数据区最大字节值。目录项的 1CH～1FH 字节为文件长度字节,低位在前,高位在后。

对于子目录,文件长度字节值应为 0,但人为的在文件长度字节上填上某个非 0 值,对子目录也没有任何不良影响,而且在这个字节填上大于磁盘数据区最大字节值的值,还可起到在 PCTOOLS 下屏蔽子目录的加密作用。注意!若填上小于或等于磁盘数据区最大字节值的值,将不起加密作用。

将子目录文件长度值修改成大于磁盘数据区最大字节值的值后,PCTOOLS 不能将该子目录予以显示,但在 DOS 下仍会显示出来。因此,也必须将其属性字节值置成 12H 或者 17H,使之在 DOS 下也不被显示。

经这种方法加密的子目录,虽然在 PCTOOLS 和 DOS 下均不显示,但只要知道子目录名则仍可使用。由于他人无法知道子目录名,而只有自己知道,所以,这种加密方法既较好的隐藏了子目录,又不会给自己使用子目录带来不便,不失为一种上乘的子目录隐含加密法。磁盘数据区最大字节值可使用前面介绍的公式进行计算。

4.一个加密实例

在 20MB 硬盘上有一子目录,名为 ABC,现对其采用上述的第 4 种方法加密,即修改文件长度字节和属性字节来隐含子目录。为简便起见,修改工具使用最广、最易得到的 PCTOOLS R1.00 版。

先计算出硬盘数据区最大字节值。运行 PCTOOLS 程序,选择 VIEW、EDIT(阅览、编辑)功能,当屏幕询问是编辑阅览 File 还是 Disk 时,将箭头下移指

向 Disk, 用回车键认可屏幕显示的准备操作的 C 驱动器。之后,硬盘的逻辑 0 扇区的前 256 个字节的 16 进制码首先在屏幕上显示出来。于是,从 0 扇区的 13～14H 字节查得 S 的值为 A307H(即 41735D), 从 16～17H 字节查得 F 的值为 0029H(即 41D),从 11～12H 字节查得 N 的值为 0200H(即 512D)。将 S,F,N 的 10 进制值代入下面的公式计算:

$$K=(S-(1+2\times F+N\times 32/512))\times 512$$
$$=(41735-(1+2\times 41+512\times 32/512))\times 512$$
$$=21309440(\text{字节})$$

即所使用的硬盘数据区最大字节值为 21309440,化成 16 进制值为 02452800H, 修改子目录文件长度字节时,应取大于 01452800H 的值才能起加密作用,如取 01452801H。

接着按 PgDn 键,屏幕将继续依次次显示硬盘其它扇区的内容。当通过 PgDn 键翻页, 在目录扇区中搜索到子目录 ABC 的目录项后,按 F3 键,进入编辑状态,通过光标移动键将光标移到子目录 ABC 的目录项的 0BH 字节,将 10H 改成 12H。之后, 将光标移到文件长度字节(即目录项的 1C～1FH 字节),将全 0 值改成 01452801H。注意,低位在前, 高位在后,1CH 字节为 01H,1DH 字节为 28H,1EH 字节为 45H,1FH 字节为 01H。随后,按 F5 键对硬盘进行实际的修改。接着按任一键回到阅览状态,再按 ESC 键回到主菜单, 将箭头上移到 DIRECTORY(目录)项,显示硬盘子目录树结构图, 此时,你会惊奇的发现,子目录 ABC 不见了。

当退出 PCTOOLS,在 DOS 下列磁盘目录时,子目录 ABC 也无影无踪了。对于非法用户, 子目录 ABC 犹如不存在一样,但对于合法用户,由于知道加密子目录名为 ABC, 故仍可方便的使用,键入:

C>CD ABC 回车

则会立即进入加密子目录 ABC。

本文所述加密方法在 AEI 486、EC386、浪潮 0530、IBM PC/XT 等微机上通过。所试验的 PCTOOLS 版本为 R1.00～R7.00。