磁盘文件／子目录加密解密新技术

海南师范学院数学系 陈 宏
广东茂名石油工业公司 陈 勇

摘要：本文以实例说明利用设备链对磁盘文件或子目录加解密的实现原理和方法。

文件加密除了将文件内容变成密文外，最常见的是对文件的目录项各域进行修改变换，如修改文件属性、将文件名改为不能正常显示字符、隐藏起始簇等方法。本文从另一个角度出发，巧妙地利用 DOS 2.0 版本后引入的设备与文件一致化处理思想，同样也能实现对磁盘文件或子目录的加密和解密。

为了将 DOS 内核与硬件的具体操作分开，DOS2.0 引入由设备头、策略过程中断过程组成的设备驱动程序，DOS 内核以“I／O 请求头”通过驱动程序完成对系统 I／O 设备的各种请求(文献)。按照设备的特性和工作方式可分为块设备和字符设备两种，块设备是用逻辑名 A、B、C、D 等来命名和访问的，而每一个字符设备都有一个象 CON、AUX、PRN、COM1、LPT1、CLOCK 等的设备名。对字符设备的访问是以其设备名来进行的，字符设备具有象磁盘文件一亲戚的打开、关闭、读、写等操作，在 DOS 给程序员提供的 DOS 功能调用中将字符设备也当作是文件来处理，当然这里是指通过设备驱动程序访问设备而不是调用 ROM BIOS 中断或直接去操纵硬件、设备和文件的一致化处理无疑给用户编程带来很大的方便，也充分体现出设备驱动程序对 DOS 内核透明其中的具体硬件细节思想。即然 DOS 为字符设备保留的设备名都当作是访问设备的标识，在 DOS 对文件进行建立、打开、删除、改名和对子目录进行建立、删除、查找等操作时都首先要进行文件名的检查，在系统初始化时 DOS 将所有的常驻设备和 CONFIG.SYS 的 DEVICE 命令定义的可安装设备设备头链接在一起形成设备链，该链的链头指向 NUL 设备头，当 DOS 要进行文件名检查时从链首 UNL 开始逐一取出所有字符设备名与所请求的文件名或子目录名进行比较，如果两者相等则打开相应的设备，只有与所有设备名比较都不成功后才当作是磁盘文件或子目录，因此设备名的优先级要比文件名高，在文件名与设备名相同情况下，DOS 访问的是设备而不是文件。事实上，设备链的唯一作用在于检查字符设备名与文件名是否相同而已，对于块设备只要通过 DPB 连就可得到设备头所含的有关信息，正因如此 DIR II 病素只修改 DPB 链的设备驱动程序中断、策略过程入口，对设备链中的这两个入口没有必要事实上也没有作任何改动，根据上述处理过程可以构造这样的一个对文件或子目录进行加密方法：在设备链中增加与要加密的文件或目录名相同的设备头，相当于增加与文件或子目录同名的字符设备，这样几乎所有的 DOS 命令均无法对原来的文件或子目录进行操作了。笔者用汇编语言编写了实现这种加密方法的 LOCK 程序，其主要思想是在内存中常驻一块能存放 10 个设备头的空间，这 10 个设备头将完全复制 NUL 的设备头内容，同时修改设备头链接域，使得增加的 10 个设备头插入原来的设备链中，设备头结构如下：

00～01H 设备链的下一个驱动程序的入口偏移地址
02～03H 设备链的下一个驱动程序的入口段址
04～05H 设备的属性字(最高位为 1 表明是字符设备，否则为块设备)
16～07H 驱动程序的策略过程入口偏移地址
08～09H 驱动程序的中断过程入口偏移地址
0A～011H 字符设备的设备名(8 字节)
或者是块设备的部件数(1 字节)其后 7 个字节保留

把文件或子目录名填入那 10 个设备头其中空闭(设

备名为 NUL)的一个就完成了加密过程,解密则相反将相应的设备名恢复为 NUL 即可。设备链链头 NUL 设备头可由 DOS 功能 52H 返回的 ES: BX+22H (DOS3.X、4.X、5.0)。驻留内存部分除 10 个设备头外还给中断 2FH 的增加 C801 功能用于测试 LOCK 是否已经驻留过(CX 返回 5A5AH),功能 C802 返回驻留于内存增加的设备头首地址 ES: DI 经 MASM、LINK、EXE2BIN 变成 COM 文件后,具体使用方法如下:

C:>LOCK ;LOCK 如还没有驻留则驻留内存,已驻留就显示增加的 10 个设备设备名,方便查看已加密的文件或子目录名。

C:>LOCK 文件名(或子目录名);如果该文件先前没有加密则加密,否则解密。在输入文件名或子目录名长度为 8 个字符且不能带有":"或"\"的符号。

我们可以把此程序用于暂时关闭某些危险的外部命令如 FORMAT 等或者不允许其它用户进入某个子目录,再次键入相同的命令即可恢复正常使用,可运行于 DOS 3.X5.0。在 5.0 下效果更佳,DIR 命令也不能显示出被加密的文件名或子目录名,经测试与 NOVELL 网、金山、2.13 和 Borland C++集成环境等很好地兼容。参考文献张载鸿局部网络操作系统 DOS 高级技术分析(第十章)国防工业出版社 1988

```
;LOCK。ASM
CODE  SEGMENT
    ORG  100H
    ASSUME  CS:CODE, DS: CODE, ES: CODE
START: JMP  BEGIN
DEV header DB 10 * 12H DUP(0);10 个设备头空间
OLD INT2F  DW  00
    DW  00
NEW__INT2F:
    CMP  AX,0C801H
    JNZ  J1
    MOV  CX,015A5H
    IRET
J1: CMP   AX,0C802H
    JNZ   LINK
    PUSH  CS
    POP   ES
    MOV   DI,OFFSET DEV__header
    IRET
LINK:CLI
    JMP  DWORD PTR CS:[OLD__INT2F]
INST__END  DB" $ ";驻留部分结束
BEGIN:
    XOR  CX,CX
    MOV  AX,0C801H
    JNT  2FH
    CMP  CX,0A5A5H
    JNZ  INSTALL;没驻留过,转
    JMP  LOCKFUNC
INSTALL:
    MOV   AH,52H
    INT   21H
    ADD   BX,22H;ES:BX 指向设备链头 NUL
    PUSH  ES
    POP   DS
    MOV   SI,BX
    PUSH  DS[SI];保存第二个设备头的地址
    PUSH  DS:[SI+2]
    PUSH  CS
    POP   ES
    MOV   DX,10
    MOV   DI,OFFSET DEV__header
NEXT:MOV  BX,DI
    PUSH  DI
    PUSH  CS
    POP   DS:[SI+2];修改链接域
    POP   DS:[SI]
    MOV   CX,12H
    REP   MOVSB;复制 NUL 设备头内容
    DEC   DX
    JZ    J3
    MOV   SI,BX
    PUSH  CS
    POP   DS
    JMP   NEXT
J3:SUB    DI,12H
    POP   ES:[DI+2];链接回原来的第二个设备头
    POP   ES:[DI]
    MOV   AX,352FH
```

```
    INT   21H
    MOV   CS:[OLD__INT2F],BX
    MOV   CS:[OLD__INT2F+2],ES
    MOV   DX,OFFSET NEW  INT2F
    MOV   AX,252FH
    INT   21H
    LEA   DX,INIT
    MOV   AH,09
    INT   21H
    MOV   AH,31H
    LEA   DX,INST__END
    ADD   DX,110H
    MOV   CL,04
    SHR   DX,CL
    INT   21H ;驻留内存
init  DB 07,"LOCK installtion', Od Oah,24h
LOCKFUNC:
    MOV  DI,81H
    XOR  CX,CX
    MOV  CL,DS:[80H]
    OR   CX,CX
    JNZLLOCK;命令带请求文件/子目录的名字,转
    CALL DISPLAY
    JMP EXIT
LLOCK:
    PUSH  CX
    MOV   AL,":"
    REPNZ SCASB
    JZ    ERR
    POP   CX
    PUSH  CX
    MOV   AL,"\"
    MOV   DI,81H
    REPNZ SCASB
    JNZ   FILENAME
ERR: ;文件名/子目录名若有":"或"\",出错
    MOV  DX,OFFSET  MSG
    MOV  AH,09
    INT  21H
    JMP  EXIT
S__ NEXT:
    MOV   CX,08
    ADD   DI,OAH
SO: PUSH  DI
    PUSH  SI
    PEPZ  CMPSB;比较文件/子目录名是否相同
    POP   SI
    POP   DI
    JCXZ  SI  ;相同
    ADD   DI,8
    DEC   BX
    JNZ   SNEXT
    STC; 没有与请求名相同的设备名
    RET
S1:CLC
    RET
searchfile  ENDP
DISPLAY  PROC  NEAR
;显示驻留 10 个设备头的名字
    MOV   AX,0C802H
    INT   2FH
    MOV   DX,0AH
    MOV   SI,DI
    PUS   H ES
    POP   DS
D0: ADD   SI,OAH
    MOV   CX,08
D1: LODSB
    MOV   AH,0EH
    MOV   BX,0007
    INT   10H
    LOOP  D1
    DEC   DX
    JNZ   DO
    RET
DISPLAY   ENDP
FILE  DB  8 DUP(20H)
MSG DB 07,"Paramter Error!!,Exp: C:>LOCK
    filename C:>LOCK",ODH,OAH,24H
    NULL DB "NUL"
    MSG2 DB ODH, OAH,"There are not free item
    to lock file $" CODE ENDS
```