UNIX／XENIX下文件／目录的简单加密与解密

唐兆海 石学荣 （江苏省洪泽县工商银行）

笔者采用扩展键和组合键等不能直接显示的效果，将扩展键引入目录名或文件名的加密方法，从而得以实现。并就此类加密给出一种通用的解密方法。现以SCO XENIX 2,32为操作系统，说明如何用扩展键及组合键等对文件和目录名进行加密与解密。

一、文件和目录的加密

1.空格式加密

扩展键虽然不能直接显示于屏幕，但是各个扩展键却有不同的表现形式。空格式加密是在利用扩展键时，屏幕上只得到一个以空格显示的"表象"，非法者在侵入系统后，若不知其真正的涵义，以空格键键入，则无法进入，出错揭示"bad directory"。例如：

```
$ mkdir t(ctrl+F2)t
$ l-i
$ 2004 drwxr-xr-x 2 icbss group 192 Nov 16 15:00t t
```

2.内藏式加密

运用此类扩展键时，屏幕上无任何显示，但其内容已包括在目录名内，该键就象藏于其背后的一样，使非法用户在不能进入时，感到莫名其妙。例如：

```
$ mkdir t(shift+F3)t
$ l-i
$ 2004 drwxr-xr-x 2 icbss group 192 Nov 16 15:00t t
```

3.隐含式加密

利用此扩展键能将屏幕上键入的字符消隐，屏幕上只有漆黑一片，什么也没有；并且显示命令对它也无效。

这种加密方法效果较好。例如:

$ mkdir tt(F1)

$ l–i

$ (屏幕显示为空)

4.混合式加密

运用以上介绍的三种方法,进行混合应用,以达到良好的加密效果,加大解密的难度。例如:

$ mkdir (shift+F3)t(ctrl+F2)t(F1)

$ l–i

$ (屏幕显示为空)

5.加密文件的相互调用

对目录名的加密方法也适用于文件名的加密,在编辑一个文件时,可以将扩展键插入文件名中,象加密目录名一样可得到加密的文件名,如:vi t(ctrl+F2)t.c.不仅可以在编辑文件时对文件名进行加密,而且可以在对文件进行编译时加密,所得的效果象对目录名加密一样,既可以达到加密的目的,又不影响文件的执行。例如:

$ cc–o tt(F1) t(ctrl+F2)t.c

$ l–i

$ (屏幕显示为空)

编辑文件主要是为了能够运用程序,在程序之间能相互调用,而经过加密后的文件名如何才能在自己的程序中得到调用呢? 我们知道象 vi 等编辑软件常把 Fn、ctrl+Fn、insert、pageup、pagedown、ctrl+字母、shift+Fn 等扩展键和组合键作为功能键来处理,因此,在用 vi 编辑工具编辑程序时,是无法直接得到以扩展键命令的程序名作为本程序的正文内容。但系统给键盘上的每个按键都规定一个特殊的值,只要将此值替换到调用的加密文件名相应的位置,即可获得对加密文件的调用。例如,有两个执行文件 tt(ctrl+F2)t 和 tt(F1),tt(ctrl+F2)t 要调用 tt(F1),那么可在 tt(ctrl+F2)t 的程序行中的必要处加入 system("tt\033[M"),即能获得对 tt(F1) 程序的调用。

二、文件和目录的解密

对目录名加密的目的,在于利用扩展键的特殊性质,使不知其义的非法者无法用一般的方法获得完整的目录名称,也就无法对子目录进行操作,从而达到保护子目录中的信息的数据资料,即达到对子目录加密的目的。

由于目录名的加密是采用特殊的扩展键加密的,因此,在解密时,只要知道加密目录名中的扩展键名,或者能晓得键值,并由此来求得扩展键名,从而得到完整的目录名称,就达到解密的目的了。

在 UNIX、XENIX 系统里,所有的文件都由各自文件系统管理,一般每个系统中至少有一个名为根文件系统,该文件系统对应的管理设备文件是 / dev / root。现以根文件系统下的加密目录 / usr / icbss / ttt / ttt(F1) 为例,介绍如何对此进行解密。

加密目录名 ttt(F1)是一不可视的隐藏式加密目录,命令 l–i 无法得到它的 i 节点号,因此,从它上一层目录 ttt 开始解密,若目录 ttt 也是加密的,那么就从目录 icbss 开始解密,依次类推。首先查出目录 ttt 的 i 节点号为 2448,将 2448– 1 后化为十六进制数 98f,再将 98f 化成二进制数 1001 1000 1111,并于二进制数 100000 进行或运算后,再左移六位,即于其数 10011010111 后添加六个零,得到二进制数 26bc0h,此为目录 ttt 在文件系统内的地址。

当知道了目录地址后,便可查出目录的节点信息,用命令 hd–wx–s–0x26bc0 / dev / root / more,可获得 i 节点编号为 2448 的目录 ttt 的节点信息(见图 1)。

```
26bc0    41ed 000b 00c9 0032 00c0 0000 6f04 0000
26bd0    0000 0000 0000 0000 0000 0000 0000 0000
*
26bf0    0000 0000 25cb 2cef 9693 2ced 9693 2ced
26b00    41ed 0002 00c9 0032 05a0 0000 6f05 bf00
26c10    006f 0000 0000 0000 0000 0000 0000 0000
26c20    0000 0000 0000 0000 0000 0000 0000 0000
26c30    0000 0000 2562 2cef 398e 2ce3 398e 2ce3
26c40    81a4 0001 00c9 0032 0392 0000 6f06 0000
26c50    0000 0000 0000 0000 0000 0000 0000 0000
```

图 1

在偏移为 26bcch 处,6f04h 是目录文件 ttt 的数据存储块号,目录文件 ttt 所有信息都记在此块内。将块号 6f04h,由十六进制化为二进制 0110 1111 0000 0100,然后将其左移十位,得到二进制数 01101111 0000010000 00000000,再转化成十六进制数 1bc1000h,即是目录 ttt 数据存储地址。用命令 hd –s 0x1bc1000、dev、root more,可取得目录的数据信息(见图 2),

```
1bc1000   90 09 2e 00 00 00 00 00 00 00 00 00 00 00 00 00  ..........
1bc1010   8e 06 2e 2e 00 00 00 00 00 00 00 00 00 00 00 00  ..........
1bc1020   91 09 74 31 00 00 00 00 00 00 00 00 00 00 00 00  ..t1......
1bc1030   ae 09 74 32 00 00 00 00 00 00 00 00 00 00 00 00  ..t2......
1bc1040   74 0a 74 33 00 00 00 00 00 00 00 00 00 00 00 00  t.t3......
1bc1050   99 0a 74 34 00 00 00 00 00 00 00 00 00 00 00 00  ..t4......
1bc1060   e7 0a 74 35 00 00 00 00 00 00 00 00 00 00 00 00  ..t5......
1bc1070   ac 0b 74 36 00 00 00 00 00 00 00 00 00 00 00 00  ..t6......
1bc1080   3e 0c 74 37 00 00 00 00 00 00 00 00 00 00 00 00  >.t7......
1bc1090   99 0c 74 38 00 00 00 00 00 00 00 00 00 00 00 00  ..t8......
1bc10a0   0c 00 74 00 00 00 00 00 00 00 00 00 00 00 00 00  ..t.......
1bc10b0   d6 07 74 74 1b 5b 4d 00 00 00 00 00 00 00 00 00  ..ttt.[M..
1bc10c0   00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ..........
```

图 2

其中编移地址 1bc10b0h 处的信息 ttt.[m,即为我们要解密的目录信息。而".[M" 就是用于加密的扩展键显示形式,其对应的十六进制数是"1b 5b 4d"。

那么,如何由键值求得扩展键名呢?在 UNIX、XENIX 下,系统将每个设备都作为一个文件处理,对于键盘来说也不例外,因此只要找到键盘的影射文件,便可查出每个键的键值,及它所对应的扩展键名称。经过分析得到,系统的键盘文件在、usr、1ib、keyboard 下,其中有两个文件 keys 和 strings,它们规定了键盘上所有键的键值及其对应的键名,包括单个键、组合键、扩展键等。因而就很容易由"1b 5b 4d"求得其八进制数为"033 133 116",也就是"＼033[M";从文件 strings 中,可查得它为扩展键"F1"。此目录名即被解密。

对于文件名的解密,以上方法是同样适用的。其过程也是如此,因为每个文件必定存在于某个目录中,只要将目录的加密解除,得到目录的数据存储信息,即可对文件名进行解密。由于加密目录是隐藏式的,用一般方法无法得到它的节点号。怎样才能获得加密目录的节点号呢?以前文加密目录来说,假设目录下有两个加密的可执行文件 g(F1)和 t(F1)。在编移 1bc10b0h 处,头两个字节"d6 07"即为目录的 i 节点号,将其按高低位排列得"07d6",用前面所说的方法,可求得该目录的数据存储块号"d5c9",再求出数据地址为"3572400h",即可得加密目录的数据信息(见图 3),

```
3572400   d6 07 74 00 00 00 00 00 00 00 00 00 00 00 00 00  ..........
3572410   90 07 74 2e 00 00 00 00 00 00 00 00 00 00 00 00  ..........
3572420   00 07 1b 00 00 00 00 00 00 00 00 00 00 00 00 00  ..........
3572430   91 07 67 2e 63 00 00 00 00 00 00 00 00 00 00 00  ..g.c.....
3572440   93 07 74 2e 63 00 00 00 00 00 00 00 00 00 00 00  ..t.c.....
3572450   86 07 67 1b 5b 4d 00 00 00 00 00 00 00 00 00 00  ..g.[M....
3572460   98 07 67 1b 1b 2e 63 00 00 00 00 00 00 00 00 00  ..g...c...
3572470   da 07 74 1b 5b 4d 00 00 00 00 00 00 00 00 00 00  ..t.[M....
3572480   00 00 61 2e 6f 75 74 00 00 00 00 00 00 00 00 00  ..a.out...
3572490   00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ..........
```

图 3

在编移地址 3572450h 处,显示信息为".g.[M",和偏移地址 3572470h 处的显示信息".t.[M",就是我们要找的两个加密文件名;再将以上信息与两个键盘影射文件的内容相比较,就能得到两加密文件的解密结果,它们分别是".g(F1)"和".t(F1)",所用的加密扩展键就是"F1"

若文件".t(F1)"是被文件".g(F1)"调用的,想得到完整的 g(F1)文件,那应如何解密?在本例中,可以用同样的方法求出主调文件的 i 节点号,从它的 i 节点信息中,按所列的块号求得数据存储区的数据信息,便可发现由命令 system()调用的文件及调用路径,若是用扩展键加密的文件名,也可对此进行解密,从而获得完整的主调文件。

以上介绍了文件和目录名的简单加密与解密的一些方法,当然对目录名和文件名的加密方法还有很多,比如自定义键加密、半分键加密或四分键加密及三分键加密等,都可说是简单类加密,而对此解密仍然可用上述方法进行,在此不再赘述。