FoxBASE+ 程序设计中的加密技术

张克友 郑云 (河南信阳师范学院 464000)

当 FoxBASE+ 系统被正确地建立在硬盘目录中之后就可以开始工作了。同样地这一工作方式的软件系统由于脱离了软盘,许多非法使用者就企图从硬盘中直接拷贝工作方式的系统。因此,作为软件系统的第二种方式也应考虑加密,使非法人员即使从硬盘拷贝也无法使拷贝的系统有效工作,从而两方面都杜绝被侵害权益的可能。传统的方法是使系统每次工作时都读一下系统盘,没有系统盘就拒绝工作。但是这样对合法用户的工作效率有降低影响,并且软盘反复读写也易损坏。因此,更好的加密方法是将工作方式的系统加密与发售方式的加密分开,这样合法用户一旦建立系统就可以仅使用硬盘启动系统工作,而非法用户即使从硬盘拷贝也不能启动系统。

对于 FoxBASE+ 应用系统来说,其程序开发者犹如发行商,有时兼作第一手用户的职能。这就是说,如果你设计的系统准备提供给其他用户,则必须在考虑各种加密措施的前提下提供一手用户设置系统各入口的合法用户手段,包括姓名及口令等。而如果所设计的系统仅为某一用户服务,则可提供较简单的设置手段或在系统交付时设置好。

下面介绍 FoxBASE+ 应用系统中所涉及的各种文件数据及软件系统的加密技术。这些方法并不是针对某一个应用系统而言,可以适用于任何 FoxBASE+ 应用系统的情况。

一、FoxBASE+ 源程序(命令)文件加密

FoxBASE+ 的源程序文件是一种 ASCII 码文本文件,程序的每一语句由回车控制符和换行控制符结束,程序最后一个语句的回车换行符之后即为文件结束控制符。这些控制符在一般的显示及编辑处理中并不显示出来,而仅起控制作用。由于 FoxBASE+ 源程序文件的这些特性,使得 DOS 操作系统的任何文处理命令或软件,例如 TYPE, EDLIN, CCED 及 WPS 等均能对源程序文件进行观察、编辑和修改。而对于某些需要加密的源程序来说,这样的情况就意味着程序内容很容易被了解,所以必须进行加密处理。

FoxBASE+ 源程序文件的一种加密方法是利用库文件与文本文件的相互转换命令来进行的加密方法。这一方法使得源程序文件的内容通过相应的 ASCII 码值变换映射而改变,用 DOS 的显示、编辑命令或 FoxBASE+ 本身的命令就都无法正确进行显示和编辑。这种方法简单实用,并且仅利用 FoxBASE+ 本身的命令就可以实现。但这样加密后的程序无法正常运行,必须在运行前恢复原来的程序内容,即解密后才能运行。如果程序较长,则加密与解密的时间也较长,并且实施加密与解密的程序本身也必须实施加密处理,否则很容易泄密。

源程序文件加密的另一种方法是利用 FoxBASE+ 系统本身所带的编译软件来实现,特别是带 E 尾缀的伪编译方式不仅可以提高程序的运行速度,还可以提高程序内容的保密程度,一般情况下很难破解其真实内容。然而这一方式的加密要求程序中设置运行命令历史档案记录空间为 0,且关闭运行记录开关,即必须设置如下两条命令:

```
SET HISTORY TO 0
SET DOHISTORY OFF
```

否则,通过同以上两条命令相反的设置并运行程序便可以从档案记录中了解程序的内容。

为了防止对 FoxBASE+ 伪编译程序的反编译,在设计源程序时可采用以下方法来保护源程序:

1. 在源程序文件中加入以下 SET 命令:

```
SET ESCA OFF
SET DOHI OFF
SET ECHO OFF
SET ALTE OFF
```

2. 尽量在调用子程序时带参数,即"DO 子程序名 WITH 参数表。"这样可避免在每个子程序中都进行重复设置 SET 。并可使在使用"DO<文件名>"时,因不知入口参数而使调用无效。

此外,最好在进行伪编译时做以下反窃取工作:

(1)将 .PRG 文件用"FOXPCOMP －E 源文件名.PRG"来进行伪编译加密;

(2)删除工作盘上的 .PRG 和 .BAK 文件。为防止用工具软件 PCTOOLS 恢复被删文件,可用 PCTOOLS 磁盘服务功能中的 E 功能,按 F2 进入 BOOT 区,将全部以 E5(已作删除标记)开头的文件名及后缀改为 00,将文件存放起始族号和文件长度(第 1A － 1F 字节)也改为 00。

另外,运用这一方式对源程序进行编译之后形成的 FOX 文件无法再恢复原态,即无法将其恢复成原来的源程序内容。因此,系统或在软盘中还需要保存相应的源程序内容备用,这样仍然还存在着源程序的加密问题。

二、文件名加密

所谓文件名加密的原理是通过某种方法使文件名中输入一些不可显示或键盘上无法直接进行输入的字符,这样就可以使任何文件处理命令因无法表示确切的文件名而不能对其进行处理,当然更谈不上显示与编辑修改了。这种加密方法无论是对 FoxBASE＋系统的命令文件还是数据库文件均可运用。

1.设计原理:由于 DOS 操作系统要求文件名中不出现空格,如果在文件名中出现空格,该文件视为无效。而利用 FoxBASE＋ 的宏替换函数能够很巧妙地将空格加入文件名中,这样就处理后的文件不能用 DOS 命令对其进行复制、修改,也不能在点状态对数据进行其他操作。

2.实现方法:进入 FoxBASE＋ 的文件编辑状态,按如下过程建立文件和使用文件:

. MODI COMM JMWJ.PRG PARA JA, JB, JC JA 为字符串, JB, JC 为数字 NAME = TRIM(JA) + STR(JC, JB) CREATE "&NAME" RTURN	. MODI COMM JMUSE.PRG PARA JA, JB, JC JA 为字符串, JB, JC 为数字 NAME = TRIM(JA) + STR(JC, JB) USE "&NAME" RETURN
如果建立 ZKY1.DBF 文件,则执行 . DO JMWJ WITH "ZKY", 3, 1	. DO JMUSE WITH "ZKY", 3, 1 如果打开 ZKY1.DBF 则执行命令

三、软件系统加密

软件系统的加密是一个综合设计问题,前面所述的加密方法也可以同样用来为软件系统的加密服务。一般总是将一个软件或应用系统中所包含的所有文件、数据进行综合加密考虑的问题称之为软件系统加密,其目的有二:一是保证软件不被非法用户顺利使用,二是保证软件设计方法及内容不被非法侵权者破解、剽窃甚至非法销售。

要保证应用系统不被非法用户使用的处理较简单,可以通过在系统程序中设置口令的方式来实现。如果非法用户回答不出正确的口令则系统不能工作。另外,对系统中的各种功能处理可以按照不同的保密级别设置专人口令,以使不同权限的合法用户能使用其权限内的系统功能。下面介绍软件系统中常用的口令设置及识别的设计方法。

为了防止非法用户使用系统或合法用户越权使用,应用系统中应在各功能处理入口进行特定人员口令识别,并通过判别输入口令的正确与否来决定系统是否拒绝来者的使用。例如,在会计帐务处理系统中的帐务查询、修改及输入功能绝对不能对任何使用者开放,还有人事管理系统中有关职工简历、工资及档案查询也应由专人负责。

要使软件系统加密的数据不被非法用户所使用,一个保险的办法是再将保存数据的目录进行加密,这样的双重加密可使数据更安全。笔者在程序设计中发现,利用区位码中的空位置实施子目录的加密效果很好,下面是其实现过程:

1.设计原理

在"区位码图形代码表"中,汉字、符号都被当作字符进行处理。除汉字、符号之外,表中还有许多空白位置,如区位码 0660、0661 等,由于这些空白位置的字符所对应的机器内码无法显示。因此,用这些符作为子目录名,就能使子目录的文件得以保护。

2.实现过程

(1)键入命令 C:》MD (0660),创建一个子目录,然后将需要保密的全部文件装入子目录。如果用直接键入区位码的方法进入子目录,必须先调用 CCDOS,然后键入区位码。这样操作过程过于繁锁,加上区位码不易记忆,往往会给自己带来不便。

(2)利用批处理文件,通过对口令的判断决定是否进入了目录,从而避免了直接键入区位码的麻烦。建立批处理文件如下:

```
C:》TYPE AUTOEXEC.BAT
  @echo off
  cls
  \(0660)\ mfoxplus kl.fox
  cls
```

```
Prompt $P$g
cd\(0660)
@echo on
```

批处理文件所调用的 KL.FOX 文件用来判断保密口令，原程序是 KL.PRG，程序清单如下：

```
@ 0,0 clear
mm=" "
do while mm<>"1997"
  @ 0,0 clear
  set cons off
  accept "Secret Code:" to mm
  set cons on
enddo
quit
```

在该程序中将保密口令设置为“1997”。KL.PRG 经加密编译成 KL.FOX，这样把原程序的语句转化为人们不易识别的机器代码形式，从而保护了口令，使其不会外泄。在微机中建立上述文件后，用硬盘启动机器，屏幕显示“Secret Code:”，要求用户输入口令，如果口令不对，机器重复显示“Secret Code:”，直到输入正确口令后便会直接进入子目录。若用软盘启动，只能进入目录，对加密的子目录仍然无法进入，实现了限制对指定文件随意操作的目的。

（来稿时间：1997 年 7 月）