UNIX／XENIX 系统下的某些安全控制措施

罗　升　陈洪森　（中国工商银行江苏省洪泽县支行）

一、控制用户使用终端及程序运行

随着 UNIX／XENIX 系统的广泛使用,其使用单位为加强系统的安全及统一管理,尽可能减少人为不安全因素,对系统提出更高的要求,如对每个终端设备定岗定位,只能由某些注册用户使用,对系统中的某些应用程序的执行,必须符合在某些终端注册的用户使用等等,提出设计控制方法。笔者通过分析,通过用户环境的再设计,较好地解决了这些问题。

1.确定用户终端与串口卡对应关系

UNIX／XINIX 操作系统支持多用户是通过串口卡建立主机与终端之间相互联系的,串口卡的种类繁多,常用有四、十六、三十二、四十、六十四等等串口卡,还有带智能的串口卡。每一串口与系统中／DEV 目录下的终端设备文件都成一一对应关系。以智能八串口卡为例,串口依次与／DEV 目录下终端设备文件对应为 TTY5A-TTY5H,同理对其它多串口卡也可在系统／DEV 目录下找到对应终端设备文件。

2.控制用户只能使用某终端

使用 UNIX／XENIX 的用户都知道,当特权用户 ROOT 在创建一个用户时系统会在该用户目录下产生一名为。PROFILE 的用户环境文件。我们可以通过重新设置该用户环境文件。PROFILE,达到控制该用户只能使用某终端。具体处理方法为:假定该用户为 LUO 只能在八智能串口卡 1 口上注册;由超级用户 ROOT 进入系统后,转到该用户目录下(／USR／WO)利用 VI 编辑程序重新编辑。PROFILE 文件。处理步骤为:

```
#cd ／usr／luo
#vi .profile
#.....
#.....
path＝／bin:／bin:／usr／luo／bin:／etc
MATL＝／usr／speol／mail／'logname'
umask 022
eval 'txet －m ansi:ansi－m:＼?ansi－r－s－q'
export PATH MAIL
```

在该文件最后增加如下几行:

```
trap "1 2 3 15 #屏幕中断
condition＝'tty'
if[ $ condition!＝"／dev／tty5a"]
then echo 您只能在 tty5a 终端上注册!
     echo 在其它终端上无权注册。
exit o
fi
```

从而起到了控制某用户只能在某终端上注册进入操作系统。

3.控制用户只能在某终端上运行某程序

其控制原理同控制某用户只能使用某终端一样,也是通过该用户在系统中的环境文件 PROFILE 的重新设置的达到控制目的。假设该用户为 LUO,在注册进入系统后只能运行程序名为 EXAMPLE,具体实现步骤为:

由 ROOT 进入系统,转入 LUO 用户目录下,调用 VI 编辑程序修改该用户环境配置文件.PROFILE:

```
Bcd ／usr／luo
#vi .profile
#.....
#.....
path＝／bin:／usr／bin:／luo／bin:／etc
MATL＝／usr／spool／mail／'logname'
umask 022
eval 'txet －m ansi:ansi－m:＼?ansi－r－s－q'
exprot PATH MAIL
```

在.profile 文件中增加如下几行:

```
trap "1 2 3 15
if[－x ／usr／luo／bin／example
then echo 有 example 程序
fi exit 1
if["'tty'"＝"／der／tty5a"]&&example
exit o
```

else echo 在本终端无权运行 example 程序必须在 tty5a 终端上运行
exit1
fi

通过以上修改,存盘后重新启动系统,则可达到控制用户 LUO 只能在八智能卡 1 口上注册运行 EXAMPLE 程序。

4.控制方法的进一步说明

以上控制方法只介绍了如何通过重新设置用户环境文件。PROFILE 控制用户使用终端及只能在指定的终端上运行指定程序的方法。如果直接引用对系统的安全性方面还不够完善,因为当用户能够进入系统后,可以合法地修改自己的环境配置文件.PROFILE,只要改变或删除以上控制语句,则使控制功能丧失。在实际使用及设计中,从安全完整的角度考虑,可在用户环境文件中通过设计菜单或专门设计菜单程序将其挂在 PROFILE 文件中,将用户的所有系统操作,包括执行系统的一些常用命令,程序等等,以菜单形式列出,使用户只能通过菜单与系统建立联系。当命令结束后返回到 LOGIN:注册状态,而不能直接进入系统命令指示符 $ 状态下,从而使系统的安全性达到较高水准。

以上控制方法均在 OLIVETTI M300/16、ZJ386/33、HP386/20、浪潮 LC386/33 等微型机上实现。

二、一种安全的关机方法

UNIX/XENIX 操作系统是多用户、多任务分时处理系统。系统的关闭必须由特权用户执行,普通用户无法关闭系统。由于进入操作系统(以特权用户注册)则对系统而言存在一定的危险性,对不太熟悉系统的用户,这种危险更大,所以特权用户为方便普通用户,一般都采用提供关机用户或增加关机命令等方法。如:

1.在/ETC/PASSWD 注册文件中增加一行:

halt::0:0::/etc/haltsys:/bin/sh

将/etc/passwd 存盘后,只需在 login 注册画面下输入 halt 回车即可关机。

2.利用 mkuser 命令生成一个关机用户 halt 无口令,再将/etc/passwd 文件中包含 halt 的一行修改为 :halt::0.....:0::/usr/haltsys:/bin/sh:即将画横线的 uid(用户标识)/gid(组标识)改为特权用户 0.0,然后在 halt 用户的.profile 文件中增加一条 shell 语句/etc/haltsys 存盘,即可在 login:注册状态下输入 halt 回车,关闭系统。

以上介绍的各种方法虽然可行,但存在一些问题,如盲目性,即输入关机命令时无论机器上有无其它用户,也不论在于什么都强行关机,可能给其它用户带来损失;另外还存在不安全性,因为利用以上方法有可能使普通用户进入特权用户环境,对系统的安全构成威协。本人通过增加一关机用户,在用户的 profile 文件中编制 shell 程序,较好地解决了这个问题。具体方法如下:

1.生成关机用户 halt:用 mkuser 建立无口令用户 halt。

2.用 VI 编辑程序对/etc/passwd 修改 halt 用户行,将 uid 及 gid 都改为 o,使 halt 成为特权用户。改为 :halt::0:0::/usr/haltsys:/bin/sh/usr/halt/halt。

3.在用户 halt 的环境文件 profile 中增加二行,即 trap,,1 2 3 15。

和 halt″<′关机 shell 程序>

4.编制 halt 关机 shell 程序:

```
#关机 shell 程序,本程序能查询未退出系统
#用户终端号,并可决定是否关机。
#用户工作自动关闭系统
#Author:罗升 陈洪森
#hate:b-05-1989
today=′date′
echo″ $ today″
echo′\n————————————′
echo′\nHALTSYS MAIN′
echo′\n————————————′
echo′\n O.exit.
echo′1.force strong haltsys.′
echo′2.halt system.′
echo′\n————————————′
echo″\n\oot please option:\c″
read option rest
case $ optoion rest
case $ option in
0)  break
    ;;
1)  sync
    sync
    haltsys
```

(下转第 20 页)

(上接第 55 页)

```
    ;;
    2)  number='who   wc-l'
    if [ $ number.-eq1]
    then syne
    syne
    haltsys
    else
    clear
    who
    echo"\ h\ 007 Terminal not all logout,can not haltsys!"
    echo'n please press. <Enter> return"
    read option rest
    if
    ;;
    * );;
    esac
    clear
    exit o
```

存盘后,用 chmod777 halt 改为可执行,再将 uid 改为 bin 即 chown bin halt; 将 gid 改为 goup 即 chgrp goup halt。至此,就构成了一个关机用户。当输入 1 时则强行关闭系统,而不考虑机器中是否有其它用户;输入 2 时,首先检查机器系统中用户是否都退出,若是则关机,否则,列出所有的用户及注册终端,不关闭系统。这种办法有效地解决了特权用户的负担,又达到安全、不盲目的目的,经过近几年来的使用,较果显著。

以上程序及办法在 OLIVETTI / M380、ZJ386 / 33、HP386 / 33 及浪潮 LC386 / 33 等机器上运行通过,操作系统为 XENIX SYSTEM V2.3.2 版本。