# 如何提高 XENIX 系统的安全性

林荣庆 (浙江省台州地区人民银行)

XENIX 系统已普遍应用,它的安全已成为广大用户非常关心的问题,随着版本的不断更新,XENIX 系统已形成一系列比较完整的安全保护机制,如口令保护、文件权限和加密命令等。用户应该熟悉这些保护机制,并在实际应用中不断加强和完善安全措施,笔者就如何提高 XENIX 系统的安全性提出具体产实施方法。

## 一、设置口令保护

口令保护是 XENIX 系统最基本的保护机制,在建立用户目录时把予先设置的口令以加密形式保存在 /etc/passwd 口令文件中,除该用户自已外,其他人无法知道其口令明文。用户注册时先打入有效的用户名,再输入口令,若输入正确,则进入系统,否则拒绝用户登录,从而达到保护目的。因此用户设置的口令既要便于记忆,以不能过于简单,避免以用户自已的姓名编写或工程代号件为口令,防止被非法用户猜中,普通用户要经常更换自已的口令,防止无关人员偶然知道。对于失去保护作用的口令,系统管理员有责任帮助用户重新设置新的口令,系统管理员要设置口令使用的期限和长度,促使用户定期更换口令。

## 二、文件权限的设置

文件保护也是 XENIX 系统最期本的保护机制,口令保护可以确保别的用户不能直接进入自已目录,但这并不保险,因为其他用户可以通过 CD 命令进入你的目录,也可以通过文件全路径名访问你的目录和文件,只有恰当地设置文件和目录的权限,才能有效地保护用户的文件和目录的安全。

XENIX 系统把使用文件的人分成三个等级,即文件的创建者—文件的主人,同组的人和其他人。三种人的权利是逐级降低的,文件的主人权力最大,由它决定下面二级的应用权力。每一个等级的人对文件都有三种不同的存取权,即阅读权 R,写入权 W 和执行权 X。

| R | W | X | | R | W | X | | R | W | X |
|---|---|---|---|---|---|---|---|---|---|---|
| 主人 | | | | 同组人 | | | | 其他人 | | |

文件的存取权都由文件的主人决定,用户可以通过 chmod 命令正确设置自已的文件和目录的存取权,可以达到对文件和目录的有效保护。例如要取消同组人和其他人的读、写和执行权,则除文件目录的主人外,其他用户既不能读目录,也不能删除、修改和建立文件,也不能执行其中的文件。

在 XENIX 系统中,设备都当作文件看待,称为特别文件,它们存于 /DEV 目录下,主要用于系统中设备之间的数据传输,这些特别文件是系统安全的一个重要方面,另外系统配置文件,例如 /ETC/RC/ / ETC/TTYS 等,都要特别加以保护,不能允许普通用户修改。

## 三、用户的设置

XENIX 系统是多用户操作系统,合理地设置用户可以保护系统的安全,每个要用 XINIX 系统机器的人,都要建立自已的用户目录,避免几处用户使用一个用户目录,就是系统管理员进行非系统维护的一般性操作,如学习研究和开发应用程序等,也不能以超级用户身份进行,应该有普通用户的目录,以普通用户身份进行操作。超级用户也称特权用户,其权力是无限大的,它们可以任意修改和删除任何人的文件,对系统的管理和维护负有特殊的责任,因此知道超级用户口令的人越少,系统就越安全,特别对系统刚入门的人不应该成为超级用户,而知道根目录口令的人,不是在必须维护系统时也不应该在根目录下工作。

为防止普通用户随意进入其他用户目录或对系统文件造成伤害,可指定普通用户使用受限制的 SHELL,强制用户在有限范围内使用系统。也可以在普通用户的。

PROFILE 文件中设置安全的命令目录和运行环境,如路径 PATH 等设置。

一个更安全有效的方法是使业务操作人员只能利用应用程序系统处理业务,可由系统管理员编制专用的 SHELL 程序,代替标准的 SHELL,用户进入系统后立即执行专用的 SHELL 程序,程序运行结束后自动退出系统,回到登录状态。同时把用户一些常用的命令,例如软盘格式化、拷贝、列目录等命令,也做在用户的专用 SHELL 程序里,减少业务操作人员同操作系统的接触,并且去掉用户某些不需要的操作权限,使其在程序的严格控制下操作。

例如用户 lrq 专用 SHELL 程序为 gh.sh 如下:

```
foxplus gz
exit
```

在 / etc / pallwd 口令文件中,用户 lrg 一行原是:

lrq::201:50:: / usr / lrq: / bin / sh 改成

lrq::201:50:: / usr / lrq: / usr / lrq / gz.sh

则用户 lrq 登录后直接进入 FoxBASE 运行 gz.prg 程序,执行完毕后自动退到 login: 状态。也可以在用户的.profile 文件中增加 foxplus gz 和 exit 二行,达到同样的效果。

## 四、用户终端的设置

利用 XENIX 系统适用于多用户终端设备的特点,可以给各应用系统的用户分配固定的终端,这样非法用户即使知道其他用户的口令和密码,也无法在自己的终端上运行其他用户的应用程序。具体做法是在用户的.profile 文件中增加以下几行程序。

```
if test 'tty'!= / dev / tty1a
  then echo "你不能使用本终端"
exit
fi
foxplus gz
exit
```

同时可在用户使用终端前由系统管理员用 enable 命令激活各终端,关机前再由系统管理员用 disable 命令锁住各终端。

## 五、给 *XENIX* 系统加锁

XENIX 系统的机器只限于系统管理员开启主机,防止普通用户,特别是非法用户随意开启机器,可进一步提高系统的安全性。在进入多用户前设置口令检测,即加锁,此口令只由系统管理员掌握,原理和做法如下。

/ etc / rc 含有 XINIX 系统一系列初始化命令,系统开机时就先执行这些命令,它们显示启动信息,启动各种系统进程,装载文件系统,然后进入多用户登录选择,相当于 DOS 操作系统中的自动批处理文件,对所有用户都是有效的。今在 / etc / rc 文件中设置口令检测,如输入口令正确则允许进入系统,即允许普通用记登录,否则自动关机,有效地防止其他普通用户随意开机进入 XENIX 系统。在 / etc / rc 文件的末尾加入下面一段 sheel 程序。

```
echo "请输入进入 XENIX 系统的口令"
if test 'inpasswd.exe'!= "XENIX"
then exec / etc / haltsys
fi
```

这里"XENIX"就是系统管理员予先设置的口令,其中 inpasswd.exe 是 c 语言编制的执行程序,源程序如下:

inpasswd.c

```
#include <curses.h>
main()
{
char c[10];
initscr(0);
noecho();
getstr(c);
echo();
puts(c);
endwin();
}
```

## 六、执行正常的关机步骤

普通用户完成业务操作后,不能一走了事,必须从终端退出,即在普通用户提示符 $ 下按 ctrl+d 键,回到多用户登录状态,显示 login:, 否则非法用户照样可以进入系统操作。

使用 XENIX 系统必须正确关闭主机,否则会造成文件系统混乱, 下次开机时就会出现如下信息:

```
The system was not shut down properey,
and the root file system should be cleaned。
proceed with cleaning (y / n)?
```

含义是系统没有正确关闭,根文件系统需要清理,问是否继续清理?

这时就要清理,系统检查和恢复文件系统,但有时也会造成不能恢复,不得不进行系统维护,不但费时费力,而且可能危及数据文件,因此正确关机显得尤其重要。

XINIX 系统提供了二条关机命令,一条是 haltsys,一条是 Shutdown,但都是在超级用户下执行,普通用户为了关机而经常进入超级用户,对系统的安全级为不利。为使普通用户既不进入超级用户又能执行正常关机,可以设置一个用户,专门作为关机用户,方法如下。

1.在超级用户下建立关机用户,假设名为 gjyh,它也有口令,应让其他普通用户都知道。

2.修改 / etc / passwd 文件,把关机用户的用户标识号和用户组标识号都改成同 root 超级用户一样。

3.在关机用户的.profile 文件的末尾增加下面一条命令 exec / etc / haltsys。

4.普通用户按 ctrl+d,在多用户方式下以关机用户注册,当回答口令正确后,则立即执行.profile,屏幕显示正常关机后的信息,此时可关闭主机电源。

## 七、建立超级用户的后备口令

超级用户也是特权用户,是在 XENIX 系统中享有最高权利的人,文件保护机制对它不起任何作用,因此知道超级用户口令的人不宜多,且超级用户也要经常更换自己的口令,这对系统的安全是非常必要的。超级用户权利越大意味着责任越大,但是一旦超级用户忘记了自己的口令而无法进行系统维护时,问题就严重了,因此有必要建立超级用户的后备口令,下面介绍一种方法。

先制作启动软盘,把超级用户口令置成无口令状态,也就是后备口令,把此时的口令文件 / etc / passwd 复制到启动软盘上,再在硬盘系统中设置超级用户所需要的口令。当超级用户忘记口令而无法进入系统维护时,就用启动软盘启动系统,当单用户方式以 root 登录要求输入口令时,就打回车键(即无口令设置),从而进入系统,显示#,再用 passwd 命令重新设置超级用户口令。

## 八、软盘启动和维护

多用户 XENIX 操作系统已广泛应用,日常维护问题比较突出。未正常关机往往引起系统混乱,造成硬盘文件系统不能正常运行,重新安装系统不但费时费力,而且会丢失用户文件,给工作带来严重损失,对系统的安全十分不利。因此要解决利用软盘启动和维护问题,下面介绍维护软盘的制作和使用。

**1.制作维护软盘**

维护软盘要有硬盘文件系统正常的机器上制作,准备一张 1.2M 新软盘,进入硬盘系统的超级用户。

(1)格式化软盘,把软盘插在 0 号驱动器

#format / dev / rfd096ds

(2)构造带有引导和根文件系统软盘

# mkdev fd

根据屏幕显示选择文件系统的软盘类型为双面、每磁道 9 个扇区,选择软盘文件系统内容为根文件及有引导。此时软盘已产生部分系统文件且可引导。

(3)把启动过程中用的文件和常用命令复制到软盘

# mount / dev / fd0 / mnt

# cp / dev / console / mnt / dev

# cd / bin

# cp l cat fsck / mnt / bin

# cd / etc

# cp passwd ttys getty rc group init inir login mount umount haltsys cp / mnt / etc

(4)产生.profile 文件。

# vi / mnt / .profile

PATH = / : / bin / etc

HZ = 50

export PATHhz

# umount / dev / fd0

**2.使用方法**

在硬盘系统启动中主要用到下列文件:

boot,xenix,init,inir,ttys,getty,passwd,rc,group,login,console。

如上述文件有损坏,硬盘系统不能引导,或不能进入多用户或系统设置不符合要求等,在这种情况下,可用维护软盘启动,进入软盘文件系统,再把硬盘安装到软盘文件系统中,然后根据故障现象,把维护软盘上的有关文件复制到硬盘上,卸下硬盘,就能恢复硬盘文件系统了。