**第一次网安综合课程设计报告**

**（Environment Variable and SET-UID Program Lab）**

57117228 陈佑

# 一．Manipulating Environment Variables操纵环境变量

实验目的——了解用于设置和取消环境变量的命令。

## **Step1.使用printenv和env指令来输出环境变量**

### （1）实验过程截图

**root@VM:/home/seed# printenv**  
ANDROID\_HOME=/home/seed/android/android-sdk-linux  
TERM=xterm-256color  
SHELL=/bin/bash  
LD\_PRELOAD=/home/seed/lib/boost/libboost\_program\_options.so.1.64.0:/home/seed/lib/boost/libboost\_filesystem.so.1.64.0:/home/seed/lib/boost/libboost\_system.so.1.64.0  
USER=root  
LS\_COLORS=rs=0:di=01;34:ln=01;36:mh=00:pi=40;33:so=01;35:do=01;35:bd=40;33;01:cd=40;33;01:or=40;31;01:mi=00:su=37;41:sg=30;43:ca=30;41:tw=30;42:ow=34;42:st=37;44:ex=01;32:\*.tar=01;31:\*.tgz=01;31:\*.arc=01;31:\*.arj=01;31:\*.taz=01;31:\*.lha=01;31:\*.lz4=01;31:\*.lzh=01;31:\*.lzma=01;31:\*.tlz=01;31:\*.txz=01;31:\*.tzo=01;31:\*.t7z=01;31:\*.zip=01;31:\*.z=01;31:\*.Z=01;31:\*.dz=01;31:\*.gz=01;31:\*.lrz=01;31:\*.lz=01;31:\*.lzo=01;31:\*.xz=01;31:\*.bz2=01;31:\*.bz=01;31:\*.tbz=01;31:\*.tbz2=01;31:\*.tz=01;31:\*.deb=01;31:\*.rpm=01;31:\*.jar=01;31:\*.war=01;31:\*.ear=01;31:\*.sar=01;31:\*.rar=01;31:\*.alz=01;31:\*.ace=01;31:\*.zoo=01;31:\*.cpio=01;31:\*.7z=01;31:\*.rz=01;31:\*.cab=01;31:\*.jpg=01;35:\*.jpeg=01;35:\*.gif=01;35:\*.bmp=01;35:\*.pbm=01;35:\*.pgm=01;35:\*.ppm=01;35:\*.tga=01;35:\*.xbm=01;35:\*.xpm=01;35:\*.tif=01;35:\*.tiff=01;35:\*.png=01;35:\*.svg=01;35:\*.svgz=01;35:\*.mng=01;35:\*.pcx=01;35:\*.mov=01;35:\*.mpg=01;35:\*.mpeg=01;35:\*.m2v=01;35:\*.mkv=01;35:\*.webm=01;35:\*.ogm=01;35:\*.mp4=01;35:\*.m4v=01;35:\*.mp4v=01;35:\*.vob=01;35:\*.qt=01;35:\*.nuv=01;35:\*.wmv=01;35:\*.asf=01;35:\*.rm=01;35:\*.rmvb=01;35:\*.flc=01;35:\*.avi=01;35:\*.fli=01;35:\*.flv=01;35:\*.gl=01;35:\*.dl=01;35:\*.xcf=01;35:\*.xwd=01;35:\*.yuv=01;35:\*.cgm=01;35:\*.emf=01;35:\*.ogv=01;35:\*.ogx=01;35:\*.aac=00;36:\*.au=00;36:\*.flac=00;36:\*.m4a=00;36:\*.mid=00;36:\*.midi=00;36:\*.mka=00;36:\*.mp3=00;36:\*.mpc=00;36:\*.ogg=00;36:\*.ra=00;36:\*.wav=00;36:\*.oga=00;36:\*.opus=00;36:\*.spx=00;36:\*.xspf=00;36:  
LD\_LIBRARY\_PATH=/home/seed/source/boost\_1\_64\_0/stage/lib:/home/seed/source/boost\_1\_64\_0/stage/lib:  
SUDO\_USER=seed  
SUDO\_UID=1000  
USERNAME=root  
PATH=/home/seed/bin:/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin:/usr/games:/usr/local/games:.:/home/seed/android/android-sdk-linux/tools:/home/seed/android/android-sdk-linux/platform-tools:/home/seed/android/android-ndk/android-ndk-r8d  
MAIL=/var/mail/root  
PWD=/home/seed  
JAVA\_HOME=/usr/lib/jvm/java-8-oracle  
LANG=en\_US.UTF-8  
HOME=/root  
SUDO\_COMMAND=/bin/su  
SHLVL=2  
LANGUAGE=en\_US  
LOGNAME=root  
LESSOPEN=| /usr/bin/lesspipe %s  
DISPLAY=:0  
SUDO\_GID=1000  
LESSCLOSE=/usr/bin/lesspipe %s %s  
XAUTHORITY=/home/seed/.Xauthority  
\_=/usr/bin/printenv

**root@VM:/home/seed# env**

ANDROID\_HOME=/home/seed/android/android-sdk-linux

TERM=xterm-256color

SHELL=/bin/bash

LD\_PRELOAD=/home/seed/lib/boost/libboost\_program\_options.so.1.64.0:/home/seed/lib/boost/libboost\_filesystem.so.1.64.0:/home/seed/lib/boost/libboost\_system.so.1.64.0

USER=root

LS\_COLORS=rs=0:di=01;34:ln=01;36:mh=00:pi=40;33:so=01;35:do=01;35:bd=40;33;01:cd=40;33;01:or=40;31;01:mi=00:su=37;41:sg=30;43:ca=30;41:tw=30;42:ow=34;42:st=37;44:ex=01;32:\*.tar=01;31:\*.tgz=01;31:\*.arc=01;31:\*.arj=01;31:\*.taz=01;31:\*.lha=01;31:\*.lz4=01;31:\*.lzh=01;31:\*.lzma=01;31:\*.tlz=01;31:\*.txz=01;31:\*.tzo=01;31:\*.t7z=01;31:\*.zip=01;31:\*.z=01;31:\*.Z=01;31:\*.dz=01;31:\*.gz=01;31:\*.lrz=01;31:\*.lz=01;31:\*.lzo=01;31:\*.xz=01;31:\*.bz2=01;31:\*.bz=01;31:\*.tbz=01;31:\*.tbz2=01;31:\*.tz=01;31:\*.deb=01;31:\*.rpm=01;31:\*.jar=01;31:\*.war=01;31:\*.ear=01;31:\*.sar=01;31:\*.rar=01;31:\*.alz=01;31:\*.ace=01;31:\*.zoo=01;31:\*.cpio=01;31:\*.7z=01;31:\*.rz=01;31:\*.cab=01;31:\*.jpg=01;35:\*.jpeg=01;35:\*.gif=01;35:\*.bmp=01;35:\*.pbm=01;35:\*.pgm=01;35:\*.ppm=01;35:\*.tga=01;35:\*.xbm=01;35:\*.xpm=01;35:\*.tif=01;35:\*.tiff=01;35:\*.png=01;35:\*.svg=01;35:\*.svgz=01;35:\*.mng=01;35:\*.pcx=01;35:\*.mov=01;35:\*.mpg=01;35:\*.mpeg=01;35:\*.m2v=01;35:\*.mkv=01;35:\*.webm=01;35:\*.ogm=01;35:\*.mp4=01;35:\*.m4v=01;35:\*.mp4v=01;35:\*.vob=01;35:\*.qt=01;35:\*.nuv=01;35:\*.wmv=01;35:\*.asf=01;35:\*.rm=01;35:\*.rmvb=01;35:\*.flc=01;35:\*.avi=01;35:\*.fli=01;35:\*.flv=01;35:\*.gl=01;35:\*.dl=01;35:\*.xcf=01;35:\*.xwd=01;35:\*.yuv=01;35:\*.cgm=01;35:\*.emf=01;35:\*.ogv=01;35:\*.ogx=01;35:\*.aac=00;36:\*.au=00;36:\*.flac=00;36:\*.m4a=00;36:\*.mid=00;36:\*.midi=00;36:\*.mka=00;36:\*.mp3=00;36:\*.mpc=00;36:\*.ogg=00;36:\*.ra=00;36:\*.wav=00;36:\*.oga=00;36:\*.opus=00;36:\*.spx=00;36:\*.xspf=00;36:

LD\_LIBRARY\_PATH=/home/seed/source/boost\_1\_64\_0/stage/lib:/home/seed/source/boost\_1\_64\_0/stage/lib:

SUDO\_USER=seed

SUDO\_UID=1000

USERNAME=root

PATH=/home/seed/bin:/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin:/usr/games:/usr/local/games:.:/home/seed/android/android-sdk-linux/tools:/home/seed/android/android-sdk-linux/platform-tools:/home/seed/android/android-ndk/android-ndk-r8d

MAIL=/var/mail/root

PWD=/home/seed

JAVA\_HOME=/usr/lib/jvm/java-8-oracle

LANG=en\_US.UTF-8

HOME=/root

SUDO\_COMMAND=/bin/su

SHLVL=2

LANGUAGE=en\_US

LOGNAME=root

LESSOPEN=| /usr/bin/lesspipe %s

DISPLAY=:0

SUDO\_GID=1000

LESSCLOSE=/usr/bin/lesspipe %s %s

XAUTHORITY=/home/seed/.Xauthority

\_=/usr/bin/env

**root@VM:/home/seed# printenv PWD**

/home/seed

**root@VM:/home/seed# env | grep PWD**

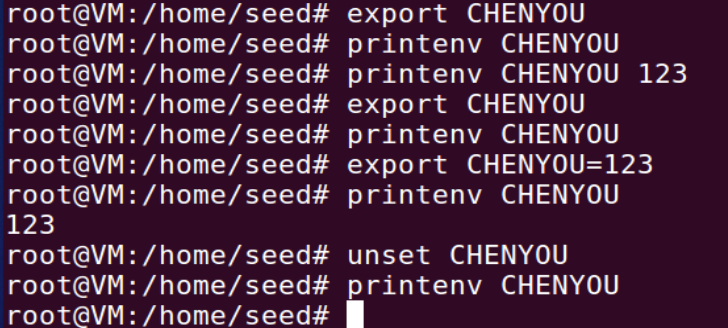
PWD=/home/seed

### 实验结果说明

Printenv和env可以输出环境变量的值，printenv和env后面加具体的环境变量可以查看该具体环境变量的值。

## **Step2.使用export和unset指令来设置或者取消环境变量**

### （1）实验过程截图



### （2）实验结果说明

export+新建环境变量名=值，可以设置新环境变量。

在环境变量设置前，printenv输出为空，设置完后，printenv输出为更新后的值。

Unset+环境变量名，可以取消环境变量。

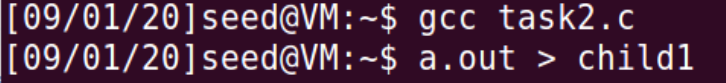
在环境变量取消后，printenv输出为空。

# Passing Environment Variables from Parent Process to Child Process 环境变量在父子进程间的传递

实验目的——知道父环境变量是否由子进程继承

## **Step1.将①保留，将②注释，输出为child1**

**实验结果截图**



**输出结果**

XDG\_VTNR=7

XDG\_SESSION\_ID=c1

XDG\_GREETER\_DATA\_DIR=/var/lib/lightdm-data/seed

CLUTTER\_IM\_MODULE=xim

SESSION=ubuntu

ANDROID\_HOME=/home/seed/android/android-sdk-linux

GPG\_AGENT\_INFO=/home/seed/.gnupg/S.gpg-agent:0:1

TERM=xterm-256color

VTE\_VERSION=4205

XDG\_MENU\_PREFIX=gnome-

SHELL=/bin/bash

DERBY\_HOME=/usr/lib/jvm/java-8-oracle/db

QT\_LINUX\_ACCESSIBILITY\_ALWAYS\_ON=1

LD\_PRELOAD=/home/seed/lib/boost/libboost\_program\_options.so.1.64.0:/home/seed/lib/boost/libboost\_filesystem.so.1.64.0:/home/seed/lib/boost/libboost\_system.so.1.64.0

WINDOWID=23071584

UPSTART\_SESSION=unix:abstract=/com/ubuntu/upstart-session/1000/1245

GNOME\_KEYRING\_CONTROL=

GTK\_MODULES=gail:atk-bridge:unity-gtk-module

USER=seed

LS\_COLORS=rs=0:di=01;34:ln=01;36:mh=00:pi=40;33:so=01;35:do=01;35:bd=40;33;01:cd=40;33;01:or=40;31;01:mi=00:su=37;41:sg=30;43:ca=30;41:tw=30;42:ow=34;42:st=37;44:ex=01;32:\*.tar=01;31:\*.tgz=01;31:\*.arc=01;31:\*.arj=01;31:\*.taz=01;31:\*.lha=01;31:\*.lz4=01;31:\*.lzh=01;31:\*.lzma=01;31:\*.tlz=01;31:\*.txz=01;31:\*.tzo=01;31:\*.t7z=01;31:\*.zip=01;31:\*.z=01;31:\*.Z=01;31:\*.dz=01;31:\*.gz=01;31:\*.lrz=01;31:\*.lz=01;31:\*.lzo=01;31:\*.xz=01;31:\*.bz2=01;31:\*.bz=01;31:\*.tbz=01;31:\*.tbz2=01;31:\*.tz=01;31:\*.deb=01;31:\*.rpm=01;31:\*.jar=01;31:\*.war=01;31:\*.ear=01;31:\*.sar=01;31:\*.rar=01;31:\*.alz=01;31:\*.ace=01;31:\*.zoo=01;31:\*.cpio=01;31:\*.7z=01;31:\*.rz=01;31:\*.cab=01;31:\*.jpg=01;35:\*.jpeg=01;35:\*.gif=01;35:\*.bmp=01;35:\*.pbm=01;35:\*.pgm=01;35:\*.ppm=01;35:\*.tga=01;35:\*.xbm=01;35:\*.xpm=01;35:\*.tif=01;35:\*.tiff=01;35:\*.png=01;35:\*.svg=01;35:\*.svgz=01;35:\*.mng=01;35:\*.pcx=01;35:\*.mov=01;35:\*.mpg=01;35:\*.mpeg=01;35:\*.m2v=01;35:\*.mkv=01;35:\*.webm=01;35:\*.ogm=01;35:\*.mp4=01;35:\*.m4v=01;35:\*.mp4v=01;35:\*.vob=01;35:\*.qt=01;35:\*.nuv=01;35:\*.wmv=01;35:\*.asf=01;35:\*.rm=01;35:\*.rmvb=01;35:\*.flc=01;35:\*.avi=01;35:\*.fli=01;35:\*.flv=01;35:\*.gl=01;35:\*.dl=01;35:\*.xcf=01;35:\*.xwd=01;35:\*.yuv=01;35:\*.cgm=01;35:\*.emf=01;35:\*.ogv=01;35:\*.ogx=01;35:\*.aac=00;36:\*.au=00;36:\*.flac=00;36:\*.m4a=00;36:\*.mid=00;36:\*.midi=00;36:\*.mka=00;36:\*.mp3=00;36:\*.mpc=00;36:\*.ogg=00;36:\*.ra=00;36:\*.wav=00;36:\*.oga=00;36:\*.opus=00;36:\*.spx=00;36:\*.xspf=00;36:

QT\_ACCESSIBILITY=1

LD\_LIBRARY\_PATH=/home/seed/source/boost\_1\_64\_0/stage/lib:/home/seed/source/boost\_1\_64\_0/stage/lib:

XDG\_SESSION\_PATH=/org/freedesktop/DisplayManager/Session0

XDG\_SEAT\_PATH=/org/freedesktop/DisplayManager/Seat0

SSH\_AUTH\_SOCK=/run/user/1000/keyring/ssh

DEFAULTS\_PATH=/usr/share/gconf/ubuntu.default.path

SESSION\_MANAGER=local/VM:@/tmp/.ICE-unix/1720,unix/VM:/tmp/.ICE-unix/1720

XDG\_CONFIG\_DIRS=/etc/xdg/xdg-ubuntu:/usr/share/upstart/xdg:/etc/xdg

DESKTOP\_SESSION=ubuntu

PATH=/home/seed/bin:/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin:/usr/games:/usr/local/games:.:/snap/bin:/usr/lib/jvm/java-8-oracle/bin:/usr/lib/jvm/java-8-oracle/db/bin:/usr/lib/jvm/java-8-oracle/jre/bin:/home/seed/android/android-sdk-linux/tools:/home/seed/android/android-sdk-linux/platform-tools:/home/seed/android/android-ndk/android-ndk-r8d:/home/seed/.local/bin

QT\_IM\_MODULE=ibus

QT\_QPA\_PLATFORMTHEME=appmenu-qt5

XDG\_SESSION\_TYPE=x11

PWD=/home/seed

JOB=dbus

XMODIFIERS=@im=ibus

JAVA\_HOME=/usr/lib/jvm/java-8-oracle

GNOME\_KEYRING\_PID=

LANG=en\_US.UTF-8

GDM\_LANG=en\_US

MANDATORY\_PATH=/usr/share/gconf/ubuntu.mandatory.path

COMPIZ\_CONFIG\_PROFILE=ubuntu

IM\_CONFIG\_PHASE=1

GDMSESSION=ubuntu

SESSIONTYPE=gnome-session

GTK2\_MODULES=overlay-scrollbar

SHLVL=1

HOME=/home/seed

XDG\_SEAT=seat0

LANGUAGE=en\_US

LIBGL\_ALWAYS\_SOFTWARE=1

GNOME\_DESKTOP\_SESSION\_ID=this-is-deprecated

XDG\_SESSION\_DESKTOP=ubuntu

LOGNAME=seed

DBUS\_SESSION\_BUS\_ADDRESS=unix:abstract=/tmp/dbus-NReMOz7fZj

J2SDKDIR=/usr/lib/jvm/java-8-oracle

XDG\_DATA\_DIRS=/usr/share/ubuntu:/usr/share/gnome:/usr/local/share/:/usr/share/:/var/lib/snapd/desktop

QT4\_IM\_MODULE=xim

LESSOPEN=| /usr/bin/lesspipe %s

INSTANCE=

XDG\_RUNTIME\_DIR=/run/user/1000

DISPLAY=:0

XDG\_CURRENT\_DESKTOP=Unity

GTK\_IM\_MODULE=ibus

J2REDIR=/usr/lib/jvm/java-8-oracle/jre

LESSCLOSE=/usr/bin/lesspipe %s %s

XAUTHORITY=/home/seed/.Xauthority

\_=./a.out

## **Step2.将②保留，将①注释，输出为child2**

**输出结果：**

XDG\_VTNR=7

XDG\_SESSION\_ID=c1

XDG\_GREETER\_DATA\_DIR=/var/lib/lightdm-data/seed

CLUTTER\_IM\_MODULE=xim

SESSION=ubuntu

ANDROID\_HOME=/home/seed/android/android-sdk-linux

GPG\_AGENT\_INFO=/home/seed/.gnupg/S.gpg-agent:0:1

TERM=xterm-256color

VTE\_VERSION=4205

XDG\_MENU\_PREFIX=gnome-

SHELL=/bin/bash

DERBY\_HOME=/usr/lib/jvm/java-8-oracle/db

QT\_LINUX\_ACCESSIBILITY\_ALWAYS\_ON=1

LD\_PRELOAD=/home/seed/lib/boost/libboost\_program\_options.so.1.64.0:/home/seed/lib/boost/libboost\_filesystem.so.1.64.0:/home/seed/lib/boost/libboost\_system.so.1.64.0

WINDOWID=23071584

UPSTART\_SESSION=unix:abstract=/com/ubuntu/upstart-session/1000/1245

GNOME\_KEYRING\_CONTROL=

GTK\_MODULES=gail:atk-bridge:unity-gtk-module

USER=seed

LS\_COLORS=rs=0:di=01;34:ln=01;36:mh=00:pi=40;33:so=01;35:do=01;35:bd=40;33;01:cd=40;33;01:or=40;31;01:mi=00:su=37;41:sg=30;43:ca=30;41:tw=30;42:ow=34;42:st=37;44:ex=01;32:\*.tar=01;31:\*.tgz=01;31:\*.arc=01;31:\*.arj=01;31:\*.taz=01;31:\*.lha=01;31:\*.lz4=01;31:\*.lzh=01;31:\*.lzma=01;31:\*.tlz=01;31:\*.txz=01;31:\*.tzo=01;31:\*.t7z=01;31:\*.zip=01;31:\*.z=01;31:\*.Z=01;31:\*.dz=01;31:\*.gz=01;31:\*.lrz=01;31:\*.lz=01;31:\*.lzo=01;31:\*.xz=01;31:\*.bz2=01;31:\*.bz=01;31:\*.tbz=01;31:\*.tbz2=01;31:\*.tz=01;31:\*.deb=01;31:\*.rpm=01;31:\*.jar=01;31:\*.war=01;31:\*.ear=01;31:\*.sar=01;31:\*.rar=01;31:\*.alz=01;31:\*.ace=01;31:\*.zoo=01;31:\*.cpio=01;31:\*.7z=01;31:\*.rz=01;31:\*.cab=01;31:\*.jpg=01;35:\*.jpeg=01;35:\*.gif=01;35:\*.bmp=01;35:\*.pbm=01;35:\*.pgm=01;35:\*.ppm=01;35:\*.tga=01;35:\*.xbm=01;35:\*.xpm=01;35:\*.tif=01;35:\*.tiff=01;35:\*.png=01;35:\*.svg=01;35:\*.svgz=01;35:\*.mng=01;35:\*.pcx=01;35:\*.mov=01;35:\*.mpg=01;35:\*.mpeg=01;35:\*.m2v=01;35:\*.mkv=01;35:\*.webm=01;35:\*.ogm=01;35:\*.mp4=01;35:\*.m4v=01;35:\*.mp4v=01;35:\*.vob=01;35:\*.qt=01;35:\*.nuv=01;35:\*.wmv=01;35:\*.asf=01;35:\*.rm=01;35:\*.rmvb=01;35:\*.flc=01;35:\*.avi=01;35:\*.fli=01;35:\*.flv=01;35:\*.gl=01;35:\*.dl=01;35:\*.xcf=01;35:\*.xwd=01;35:\*.yuv=01;35:\*.cgm=01;35:\*.emf=01;35:\*.ogv=01;35:\*.ogx=01;35:\*.aac=00;36:\*.au=00;36:\*.flac=00;36:\*.m4a=00;36:\*.mid=00;36:\*.midi=00;36:\*.mka=00;36:\*.mp3=00;36:\*.mpc=00;36:\*.ogg=00;36:\*.ra=00;36:\*.wav=00;36:\*.oga=00;36:\*.opus=00;36:\*.spx=00;36:\*.xspf=00;36:

QT\_ACCESSIBILITY=1

LD\_LIBRARY\_PATH=/home/seed/source/boost\_1\_64\_0/stage/lib:/home/seed/source/boost\_1\_64\_0/stage/lib:

XDG\_SESSION\_PATH=/org/freedesktop/DisplayManager/Session0

XDG\_SEAT\_PATH=/org/freedesktop/DisplayManager/Seat0

SSH\_AUTH\_SOCK=/run/user/1000/keyring/ssh

DEFAULTS\_PATH=/usr/share/gconf/ubuntu.default.path

SESSION\_MANAGER=local/VM:@/tmp/.ICE-unix/1720,unix/VM:/tmp/.ICE-unix/1720

XDG\_CONFIG\_DIRS=/etc/xdg/xdg-ubuntu:/usr/share/upstart/xdg:/etc/xdg

DESKTOP\_SESSION=ubuntu

PATH=/home/seed/bin:/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin:/usr/games:/usr/local/games:.:/snap/bin:/usr/lib/jvm/java-8-oracle/bin:/usr/lib/jvm/java-8-oracle/db/bin:/usr/lib/jvm/java-8-oracle/jre/bin:/home/seed/android/android-sdk-linux/tools:/home/seed/android/android-sdk-linux/platform-tools:/home/seed/android/android-ndk/android-ndk-r8d:/home/seed/.local/bin

QT\_IM\_MODULE=ibus

QT\_QPA\_PLATFORMTHEME=appmenu-qt5

XDG\_SESSION\_TYPE=x11

PWD=/home/seed

JOB=dbus

XMODIFIERS=@im=ibus

JAVA\_HOME=/usr/lib/jvm/java-8-oracle

GNOME\_KEYRING\_PID=

LANG=en\_US.UTF-8

GDM\_LANG=en\_US

MANDATORY\_PATH=/usr/share/gconf/ubuntu.mandatory.path

COMPIZ\_CONFIG\_PROFILE=ubuntu

IM\_CONFIG\_PHASE=1

GDMSESSION=ubuntu

SESSIONTYPE=gnome-session

GTK2\_MODULES=overlay-scrollbar

SHLVL=1

HOME=/home/seed

XDG\_SEAT=seat0

LANGUAGE=en\_US

LIBGL\_ALWAYS\_SOFTWARE=1

GNOME\_DESKTOP\_SESSION\_ID=this-is-deprecated

XDG\_SESSION\_DESKTOP=ubuntu

LOGNAME=seed

DBUS\_SESSION\_BUS\_ADDRESS=unix:abstract=/tmp/dbus-NReMOz7fZj

J2SDKDIR=/usr/lib/jvm/java-8-oracle

XDG\_DATA\_DIRS=/usr/share/ubuntu:/usr/share/gnome:/usr/local/share/:/usr/share/:/var/lib/snapd/desktop

QT4\_IM\_MODULE=xim

LESSOPEN=| /usr/bin/lesspipe %s

INSTANCE=

XDG\_RUNTIME\_DIR=/run/user/1000

DISPLAY=:0

XDG\_CURRENT\_DESKTOP=Unity

GTK\_IM\_MODULE=ibus

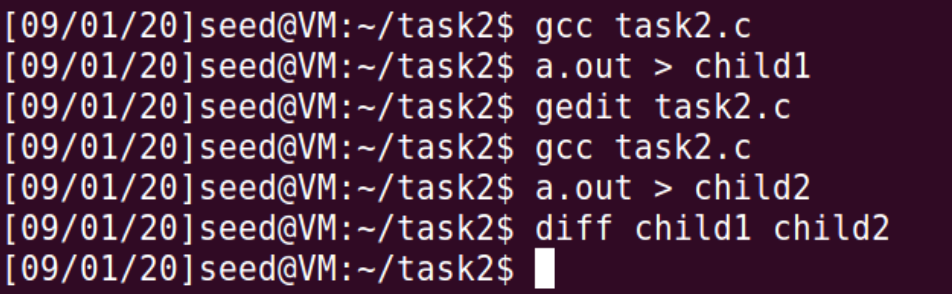
J2REDIR=/usr/lib/jvm/java-8-oracle/jre

LESSCLOSE=/usr/bin/lesspipe %s %s

XAUTHORITY=/home/seed/.Xauthority

\_=./a.out

## **Step3.比较两个输出文件的差异**



原程序中

switch(childPid = fork()) {

case 0: /\* child process \*/

printenv(); ➀

exit(0);

default: /\* parent process \*/

//printenv(); ➁

exit(0);

}

当对②注释时，表示输出输出子进程的环境变量，因为ChildPid==0表示子进程；

当对①注释时，表示输出输出父进程的环境变量，因为ChildPid！=0表示父进程。

**使用diff指令比较两个输出文件的值，发现两个文件一样，可见，子进程会从父进程处继承所有的环境变量。**

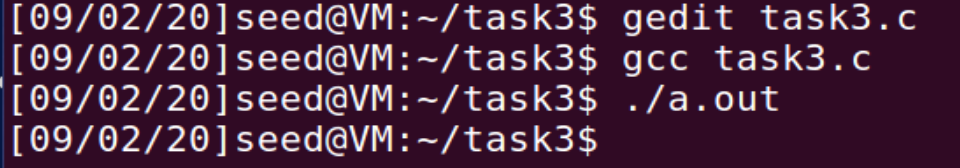
**fork函数通过系统调用创建一个与原来进程几乎完全相同的进程，子进程自父进程继承了进程的环境，堆栈与内存根目录等；但是子进程不会继承父进程的某些特性，比如父进程号，文件描述符。所以两个进程的环境变量是相同的。**

# Environment Variables and execve()

实验目的——研究当通过execve()执行新程序时，环境变量是如何受到影响的。

## **Step1. 执行名为/usr/bin/env的程序，打印出当前进程的环境变量**

（结果截图）



当execve第三个参数为NULL时，无输出。

## **Step2.将execve("/usr/bin/env",argv,NULL)改成execve("/usr/bin/env", argv, environ)后**

**当execve第三个参数为environ时，打印输出环境变量。**

**具体输出如下：**

XDG\_VTNR=7

XDG\_SESSION\_ID=c1

XDG\_GREETER\_DATA\_DIR=/var/lib/lightdm-data/seed

CLUTTER\_IM\_MODULE=xim

SESSION=ubuntu

ANDROID\_HOME=/home/seed/android/android-sdk-linux

GPG\_AGENT\_INFO=/home/seed/.gnupg/S.gpg-agent:0:1

TERM=xterm-256color

VTE\_VERSION=4205

XDG\_MENU\_PREFIX=gnome-

SHELL=/bin/bash

DERBY\_HOME=/usr/lib/jvm/java-8-oracle/db

QT\_LINUX\_ACCESSIBILITY\_ALWAYS\_ON=1

LD\_PRELOAD=/home/seed/lib/boost/libboost\_program\_options.so.1.64.0:/home/seed/lib/boost/libboost\_filesystem.so.1.64.0:/home/seed/lib/boost/libboost\_system.so.1.64.0

WINDOWID=23068682

UPSTART\_SESSION=unix:abstract=/com/ubuntu/upstart-session/1000/1245

GNOME\_KEYRING\_CONTROL=

GTK\_MODULES=gail:atk-bridge:unity-gtk-module

USER=seed

LS\_COLORS=rs=0:di=01;34:ln=01;36:mh=00:pi=40;33:so=01;35:do=01;35:bd=40;33;01:cd=40;33;01:or=40;31;01:mi=00:su=37;41:sg=30;43:ca=30;41:tw=30;42:ow=34;42:st=37;44:ex=01;32:\*.tar=01;31:\*.tgz=01;31:\*.arc=01;31:\*.arj=01;31:\*.taz=01;31:\*.lha=01;31:\*.lz4=01;31:\*.lzh=01;31:\*.lzma=01;31:\*.tlz=01;31:\*.txz=01;31:\*.tzo=01;31:\*.t7z=01;31:\*.zip=01;31:\*.z=01;31:\*.Z=01;31:\*.dz=01;31:\*.gz=01;31:\*.lrz=01;31:\*.lz=01;31:\*.lzo=01;31:\*.xz=01;31:\*.bz2=01;31:\*.bz=01;31:\*.tbz=01;31:\*.tbz2=01;31:\*.tz=01;31:\*.deb=01;31:\*.rpm=01;31:\*.jar=01;31:\*.war=01;31:\*.ear=01;31:\*.sar=01;31:\*.rar=01;31:\*.alz=01;31:\*.ace=01;31:\*.zoo=01;31:\*.cpio=01;31:\*.7z=01;31:\*.rz=01;31:\*.cab=01;31:\*.jpg=01;35:\*.jpeg=01;35:\*.gif=01;35:\*.bmp=01;35:\*.pbm=01;35:\*.pgm=01;35:\*.ppm=01;35:\*.tga=01;35:\*.xbm=01;35:\*.xpm=01;35:\*.tif=01;35:\*.tiff=01;35:\*.png=01;35:\*.svg=01;35:\*.svgz=01;35:\*.mng=01;35:\*.pcx=01;35:\*.mov=01;35:\*.mpg=01;35:\*.mpeg=01;35:\*.m2v=01;35:\*.mkv=01;35:\*.webm=01;35:\*.ogm=01;35:\*.mp4=01;35:\*.m4v=01;35:\*.mp4v=01;35:\*.vob=01;35:\*.qt=01;35:\*.nuv=01;35:\*.wmv=01;35:\*.asf=01;35:\*.rm=01;35:\*.rmvb=01;35:\*.flc=01;35:\*.avi=01;35:\*.fli=01;35:\*.flv=01;35:\*.gl=01;35:\*.dl=01;35:\*.xcf=01;35:\*.xwd=01;35:\*.yuv=01;35:\*.cgm=01;35:\*.emf=01;35:\*.ogv=01;35:\*.ogx=01;35:\*.aac=00;36:\*.au=00;36:\*.flac=00;36:\*.m4a=00;36:\*.mid=00;36:\*.midi=00;36:\*.mka=00;36:\*.mp3=00;36:\*.mpc=00;36:\*.ogg=00;36:\*.ra=00;36:\*.wav=00;36:\*.oga=00;36:\*.opus=00;36:\*.spx=00;36:\*.xspf=00;36:

QT\_ACCESSIBILITY=1

LD\_LIBRARY\_PATH=/home/seed/source/boost\_1\_64\_0/stage/lib:/home/seed/source/boost\_1\_64\_0/stage/lib:

XDG\_SESSION\_PATH=/org/freedesktop/DisplayManager/Session0

XDG\_SEAT\_PATH=/org/freedesktop/DisplayManager/Seat0

SSH\_AUTH\_SOCK=/run/user/1000/keyring/ssh

DEFAULTS\_PATH=/usr/share/gconf/ubuntu.default.path

SESSION\_MANAGER=local/VM:@/tmp/.ICE-unix/1720,unix/VM:/tmp/.ICE-unix/1720

XDG\_CONFIG\_DIRS=/etc/xdg/xdg-ubuntu:/usr/share/upstart/xdg:/etc/xdg

DESKTOP\_SESSION=ubuntu

PATH=/home/seed/bin:/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin:/usr/games:/usr/local/games:.:/snap/bin:/usr/lib/jvm/java-8-oracle/bin:/usr/lib/jvm/java-8-oracle/db/bin:/usr/lib/jvm/java-8-oracle/jre/bin:/home/seed/android/android-sdk-linux/tools:/home/seed/android/android-sdk-linux/platform-tools:/home/seed/android/android-ndk/android-ndk-r8d:/home/seed/.local/bin

QT\_IM\_MODULE=ibus

QT\_QPA\_PLATFORMTHEME=appmenu-qt5

XDG\_SESSION\_TYPE=x11

PWD=/home/seed/task3

JOB=dbus

XMODIFIERS=@im=ibus

JAVA\_HOME=/usr/lib/jvm/java-8-oracle

GNOME\_KEYRING\_PID=

LANG=en\_US.UTF-8

GDM\_LANG=en\_US

MANDATORY\_PATH=/usr/share/gconf/ubuntu.mandatory.path

COMPIZ\_CONFIG\_PROFILE=ubuntu

IM\_CONFIG\_PHASE=1

GDMSESSION=ubuntu

SESSIONTYPE=gnome-session

GTK2\_MODULES=overlay-scrollbar

SHLVL=1

HOME=/home/seed

XDG\_SEAT=seat0

LANGUAGE=en\_US

LIBGL\_ALWAYS\_SOFTWARE=1

GNOME\_DESKTOP\_SESSION\_ID=this-is-deprecated

XDG\_SESSION\_DESKTOP=ubuntu

LOGNAME=seed

DBUS\_SESSION\_BUS\_ADDRESS=unix:abstract=/tmp/dbus-NReMOz7fZj

J2SDKDIR=/usr/lib/jvm/java-8-oracle

XDG\_DATA\_DIRS=/usr/share/ubuntu:/usr/share/gnome:/usr/local/share/:/usr/share/:/var/lib/snapd/desktop

QT4\_IM\_MODULE=xim

LESSOPEN=| /usr/bin/lesspipe %s

INSTANCE=

XDG\_RUNTIME\_DIR=/run/user/1000

DISPLAY=:0

XDG\_CURRENT\_DESKTOP=Unity

GTK\_IM\_MODULE=ibus

J2REDIR=/usr/lib/jvm/java-8-oracle/jre

LESSCLOSE=/usr/bin/lesspipe %s %s

XAUTHORITY=/home/seed/.Xauthority

OLDPWD=/home/seed

\_=./a.out

## **Step3.** 就新程序如何获得其环境变量得出结论

**从以上实验可以看出，execve()函数的第三个参数代表了——传递给执行文件的新环境变量数组。当它设置为NULL的时候，打印信息为空，无法获得环境变量；当它设置为environ时，新程序能够从第三个参数中获取环境变量。**

# Environment Variables and system()

研究目的——研究当通过调用system()函数来执行新程序时，环境变量是如何受到影响的。

## **Step1.** 程序运行结果

LESSOPEN=| /usr/bin/lesspipe %s

GNOME\_KEYRING\_PID=

USER=seed

LANGUAGE=en\_US

J2SDKDIR=/usr/lib/jvm/java-8-oracle

XDG\_SEAT=seat0

SESSION=ubuntu

XDG\_SESSION\_TYPE=x11

COMPIZ\_CONFIG\_PROFILE=ubuntu

LD\_LIBRARY\_PATH=/home/seed/source/boost\_1\_64\_0/stage/lib:/home/seed/source/boost\_1\_64\_0/stage/lib:

SHLVL=1

LIBGL\_ALWAYS\_SOFTWARE=1

J2REDIR=/usr/lib/jvm/java-8-oracle/jre

HOME=/home/seed

QT4\_IM\_MODULE=xim

OLDPWD=/home/seed

DESKTOP\_SESSION=ubuntu

QT\_LINUX\_ACCESSIBILITY\_ALWAYS\_ON=1

GTK\_MODULES=gail:atk-bridge:unity-gtk-module

XDG\_SEAT\_PATH=/org/freedesktop/DisplayManager/Seat0

INSTANCE=

DBUS\_SESSION\_BUS\_ADDRESS=unix:abstract=/tmp/dbus-NReMOz7fZj

GNOME\_KEYRING\_CONTROL=

QT\_QPA\_PLATFORMTHEME=appmenu-qt5

MANDATORY\_PATH=/usr/share/gconf/ubuntu.mandatory.path

IM\_CONFIG\_PHASE=1

SESSIONTYPE=gnome-session

LOGNAME=seed

GTK\_IM\_MODULE=ibus

WINDOWID=23068682

\_=./a.out

DEFAULTS\_PATH=/usr/share/gconf/ubuntu.default.path

XDG\_SESSION\_ID=c1

TERM=xterm-256color

GNOME\_DESKTOP\_SESSION\_ID=this-is-deprecated

GTK2\_MODULES=overlay-scrollbar

PATH=/home/seed/bin:/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin:/usr/games:/usr/local/games:.:/snap/bin:/usr/lib/jvm/java-8-oracle/bin:/usr/lib/jvm/java-8-oracle/db/bin:/usr/lib/jvm/java-8-oracle/jre/bin:/home/seed/android/android-sdk-linux/tools:/home/seed/android/android-sdk-linux/platform-tools:/home/seed/android/android-ndk/android-ndk-r8d:/home/seed/.local/bin

DERBY\_HOME=/usr/lib/jvm/java-8-oracle/db

SESSION\_MANAGER=local/VM:@/tmp/.ICE-unix/1720,unix/VM:/tmp/.ICE-unix/1720

GDM\_LANG=en\_US

XDG\_MENU\_PREFIX=gnome-

XDG\_SESSION\_PATH=/org/freedesktop/DisplayManager/Session0

XDG\_RUNTIME\_DIR=/run/user/1000

DISPLAY=:0

LD\_PRELOAD=/home/seed/lib/boost/libboost\_program\_options.so.1.64.0:/home/seed/lib/boost/libboost\_filesystem.so.1.64.0:/home/seed/lib/boost/libboost\_system.so.1.64.0

LANG=en\_US.UTF-8

XDG\_CURRENT\_DESKTOP=Unity

LS\_COLORS=rs=0:di=01;34:ln=01;36:mh=00:pi=40;33:so=01;35:do=01;35:bd=40;33;01:cd=40;33;01:or=40;31;01:mi=00:su=37;41:sg=30;43:ca=30;41:tw=30;42:ow=34;42:st=37;44:ex=01;32:\*.tar=01;31:\*.tgz=01;31:\*.arc=01;31:\*.arj=01;31:\*.taz=01;31:\*.lha=01;31:\*.lz4=01;31:\*.lzh=01;31:\*.lzma=01;31:\*.tlz=01;31:\*.txz=01;31:\*.tzo=01;31:\*.t7z=01;31:\*.zip=01;31:\*.z=01;31:\*.Z=01;31:\*.dz=01;31:\*.gz=01;31:\*.lrz=01;31:\*.lz=01;31:\*.lzo=01;31:\*.xz=01;31:\*.bz2=01;31:\*.bz=01;31:\*.tbz=01;31:\*.tbz2=01;31:\*.tz=01;31:\*.deb=01;31:\*.rpm=01;31:\*.jar=01;31:\*.war=01;31:\*.ear=01;31:\*.sar=01;31:\*.rar=01;31:\*.alz=01;31:\*.ace=01;31:\*.zoo=01;31:\*.cpio=01;31:\*.7z=01;31:\*.rz=01;31:\*.cab=01;31:\*.jpg=01;35:\*.jpeg=01;35:\*.gif=01;35:\*.bmp=01;35:\*.pbm=01;35:\*.pgm=01;35:\*.ppm=01;35:\*.tga=01;35:\*.xbm=01;35:\*.xpm=01;35:\*.tif=01;35:\*.tiff=01;35:\*.png=01;35:\*.svg=01;35:\*.svgz=01;35:\*.mng=01;35:\*.pcx=01;35:\*.mov=01;35:\*.mpg=01;35:\*.mpeg=01;35:\*.m2v=01;35:\*.mkv=01;35:\*.webm=01;35:\*.ogm=01;35:\*.mp4=01;35:\*.m4v=01;35:\*.mp4v=01;35:\*.vob=01;35:\*.qt=01;35:\*.nuv=01;35:\*.wmv=01;35:\*.asf=01;35:\*.rm=01;35:\*.rmvb=01;35:\*.flc=01;35:\*.avi=01;35:\*.fli=01;35:\*.flv=01;35:\*.gl=01;35:\*.dl=01;35:\*.xcf=01;35:\*.xwd=01;35:\*.yuv=01;35:\*.cgm=01;35:\*.emf=01;35:\*.ogv=01;35:\*.ogx=01;35:\*.aac=00;36:\*.au=00;36:\*.flac=00;36:\*.m4a=00;36:\*.mid=00;36:\*.midi=00;36:\*.mka=00;36:\*.mp3=00;36:\*.mpc=00;36:\*.ogg=00;36:\*.ra=00;36:\*.wav=00;36:\*.oga=00;36:\*.opus=00;36:\*.spx=00;36:\*.xspf=00;36:

XMODIFIERS=@im=ibus

XDG\_SESSION\_DESKTOP=ubuntu

XAUTHORITY=/home/seed/.Xauthority

XDG\_GREETER\_DATA\_DIR=/var/lib/lightdm-data/seed

SSH\_AUTH\_SOCK=/run/user/1000/keyring/ssh

SHELL=/bin/bash

QT\_ACCESSIBILITY=1

GDMSESSION=ubuntu

LESSCLOSE=/usr/bin/lesspipe %s %s

GPG\_AGENT\_INFO=/home/seed/.gnupg/S.gpg-agent:0:1

UPSTART\_SESSION=unix:abstract=/com/ubuntu/upstart-session/1000/1245

XDG\_VTNR=7

QT\_IM\_MODULE=ibus

PWD=/home/seed/task4

JAVA\_HOME=/usr/lib/jvm/java-8-oracle

CLUTTER\_IM\_MODULE=xim

ANDROID\_HOME=/home/seed/android/android-sdk-linux

XDG\_CONFIG\_DIRS=/etc/xdg/xdg-ubuntu:/usr/share/upstart/xdg:/etc/xdg

XDG\_DATA\_DIRS=/usr/share/ubuntu:/usr/share/gnome:/usr/local/share/:/usr/share/:/var/lib/snapd/desktop

VTE\_VERSION=4205

JOB=dbus

## **Step2.** 结果证明

system函数定义为 int system（const char \* string），该函数会执行了三步操作：

（1）fork一个子进程；

（2）在子进程中调用exec函数去执行指令；

（3）在父进程中调用wait去等待子进程结束。

**在本例中，system()函数使用execl()执行/bin/sh；execl()调用execve()，会将环境变量数组传递给它。所以，使用system()函数，可以将调用进程的环境变量传递给新程序，程序的输出结果就是父进程的环境变量。证明结束。**

# Environment Variable and SET-UID Programs

研究目标—— 找出环境变量是否由SET-UID程序的进程从用户的进程继承。

## **Step1.** 编写以下程序，可以打印出当前进程中的所有环境变量

……………………

LD\_LIBRARY\_PATH=/home/seed/source/boost\_1\_64\_0/stage/lib:/home/seed/source/boost\_1\_64\_0/stage/**lib:**

……………………

PATH=/home/seed/bin:/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin:/usr/games:/usr/local/games:.:/snap/bin:/usr/lib/jvm/java-8-oracle/bin:/usr/lib/jvm/java-8-oracle/db/bin:/usr/lib/jvm/java-8-oracle/jre/bin:/home/seed/android/android-sdk-linux/tools:/home/seed/android/android-sdk-linux/platform-tools:/home/seed/android/android-ndk/android-ndk-r8d:/home/seed/.local/**bin**

## **Step2.** 编译上述程序，将其所有权更改为root，并使其成为SET-UID程序

## **Step3.** 在shell中（您需要在普通用户账户中，而不是根账户中)，使用导出命令设置以下环境变量(它们可能已经存在）

设置PATH环境变量(可执行程序的查找路径)：

export PATH=$PATH:/task5

设置LD\_LIBRARY\_PATH环境变量(动态库的查找路径)：

export LD\_LIBRARY\_PATH=$LD\_LIBRARY\_PATH:/task5

设置XLWANG环境变量：

export CHENYOU=$CHENYOU:/555

## **实验结果说明：**

在设置了以上三个环境变量后，环境变量的取值变为

LD\_LIBRARY\_PATH=/home/seed/source/boost\_1\_64\_0/stage/lib:/home/seed/source/boost\_1\_64\_0/stage/lib::/**task5**

……………………

PATH=/home/seed/bin:/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin:/usr/games:/usr/local/games:.:/snap/bin:/usr/lib/jvm/java-8-oracle/bin:/usr/lib/jvm/java-8-oracle/db/bin:/usr/lib/jvm/java-8-oracle/jre/bin:/home/seed/android/android-sdk-linux/tools:/home/seed/android/android-sdk-linux/platform-tools:/home/seed/android/android-ndk/android-ndk-r8d:/home/seed/.local/bin:/**task5**

……………………

**CHENYOU=:/555**

……………………

**对比step1结果和最终结果中绿色字体及高光处可得，以上三个重新定义（或者新创建）的环境变量都更新成功，这说明在shell进程（父进程）中设置的所有环境变量都进入SET-UID子进程。所以，环境变量可以由SET-UID程序的进程从用户的进程继承。**

# The PATH Environment Variable and SET-UID Programs

**研究问题——**

由于调用shell程序，在SET-UID程序中调用system()函数是相当危险的。 这是因为shell程序的实际行为可能受到环境变量（例如PATH）的影响。

这些环境变量由用户提供，用户可能是恶意的。通过改变这些变量，恶意用户可以控制SET-UID程序的行为。

在Bash中，您可以以下方式更改PATH环境变量(本例将目录/home/seed添加到PATH环境变量的开头)。

$ export PATH=/home/seed:$PATH

但是，程序员只能使用ls命令的相对路径，而不是绝对路径：

int main()

{

system("ls");

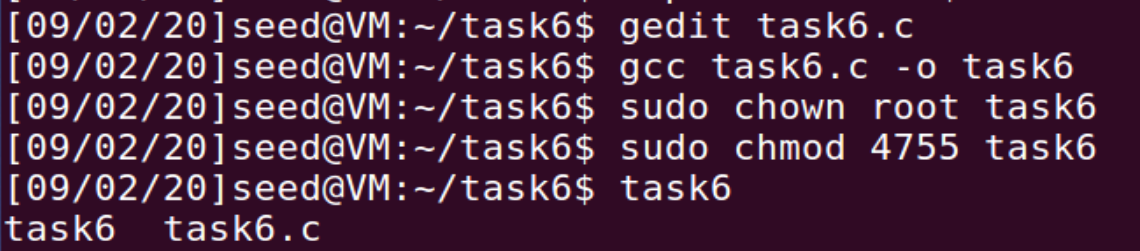
return 0;

}

编译上述程序，并将其所有者改为root，将其设置为SET-UID程序。你可以让这个SET-UID程序运行你的代码而不是/bin/ls吗？描述和解释你的观察。

## **Step1. 编译程序**程序运行结果

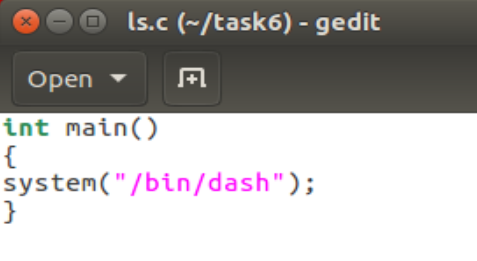
## **Step2. 将程序文件权限改为root权限，使其成为SET-UID程序**



如上图所示，函数执行的是/bin/ls指令

## **Step3. 修改环境变量PATH，让其运行自定义的代码，而非/bin/ls指令**

（1）新建一个自定义的.c文件，为ls.c文件，该文件的作用是获取一个shell。



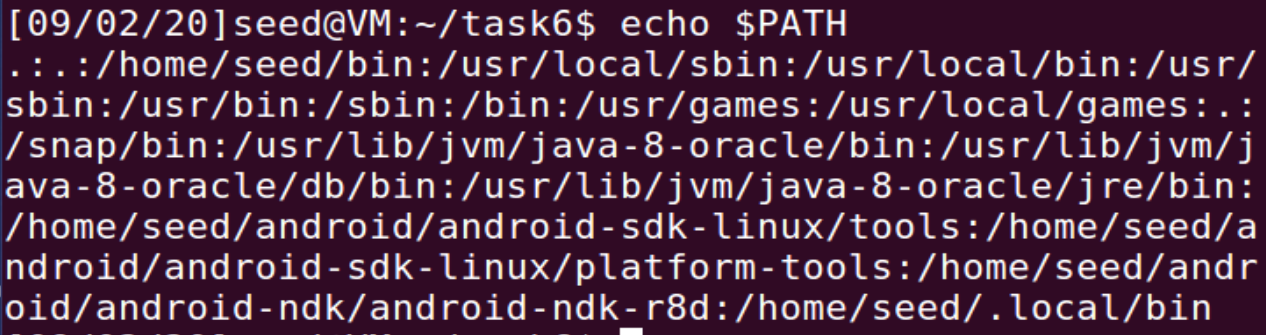
对ls.c编译成可执行程序ls，用于后续覆盖/bin/ls指令。

![](CT9IHU}]491]GQ90]3%N4](data:image/png;base64,)

由于system()函数是调用了shell的环境变量，所以首先修改PATH环境变量如下

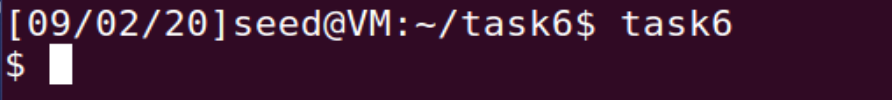
XD{PWWTLAC}J2CV5ZJ8OZF8

“.”表示当前目录。修改后的PATH环境变量如下：



**再次运行task6程序，可以发现执行结果变为打开一个shell（执行当前文件夹中自定义的ls程序，而非执行/bin/ls指令），攻击成功。**

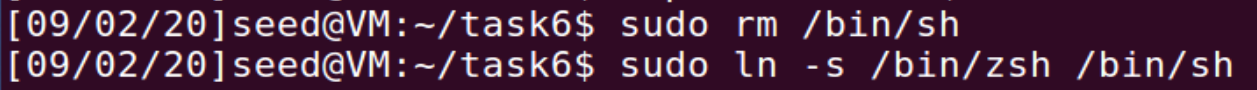
**这是因为PATH改成当前路径，会用当前路径下的ls可执行程序覆盖/bin/ls，因而可以执行用户自定义的程序。**



（2）

虽然结果显示程序是以非root权限执行shell的，这是因为ubuntu16.04的保护机制。Ubuntu16.04中的dash shell有一个防止自己在Set-UID进程中执行的对策。如果dash检测到它是在Set-UID进程中执行的，则立即将有效用户ID更改为进程的实际用户ID，实现删除特权的功能。

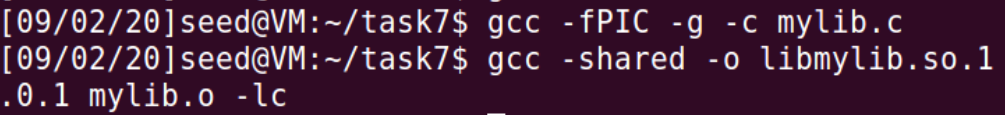
所以，为了观察到攻击行为，需要在Ubuntu16.04中安装一个名为zsh的shell程序， 并使用以下命令将/bin/sh链接到zsh，就可以观察到，程序转为root权限执行。

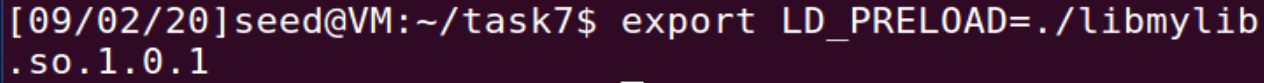


因而可以证明，此SET-UID程序是以root权限执行的。

# The LD PRELOAD Environment Variable and SET-UID Programs

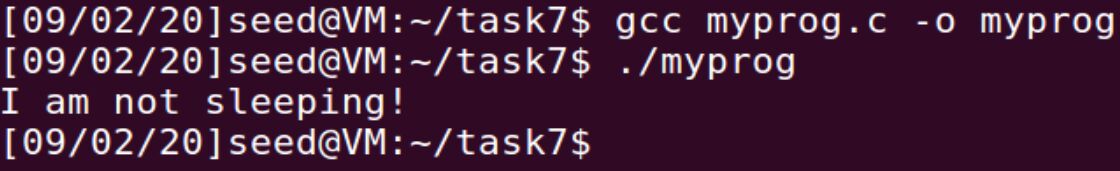
## **Step1.** 新建一个动态链接库。命名下面的代码为mylib.c，该程序基本上覆盖了libc中的sleep函数，并且用下列命令编译mylib.c，设置LD\_PRELOAD环境变量。



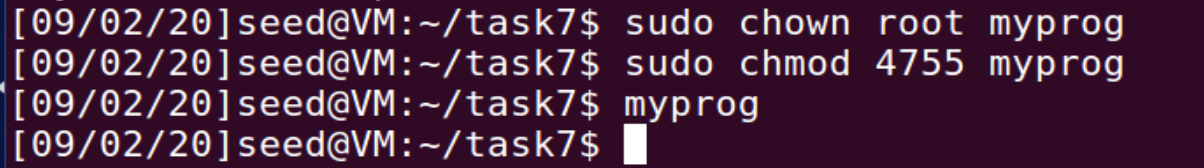


## **Step2. 以多种身份运行myprog程序**

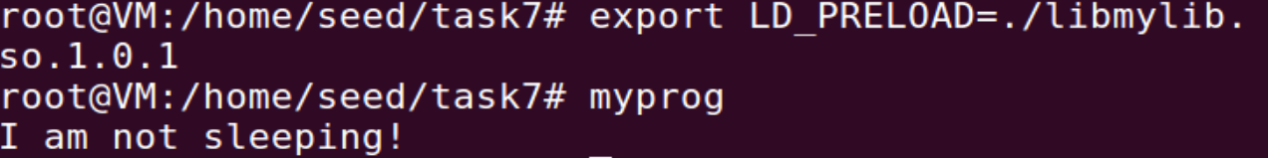
### （1）以普通用户的身份运行myprog程序



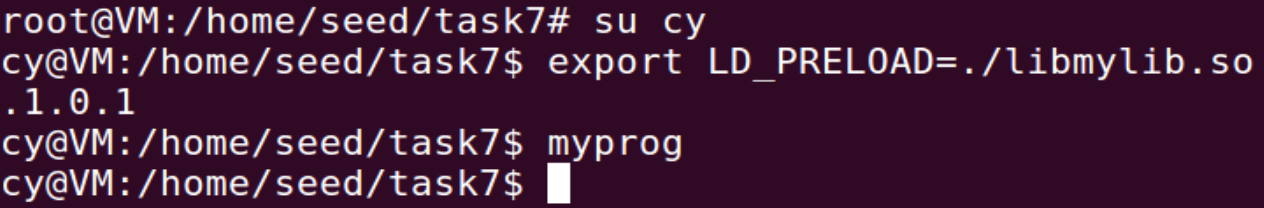
### （2）以普通用户运行拥有root权限的myprog程序



### （3）使myprog成为SET-UID root程序，在root账户中再次导出LDPRELOAD环境变量并运行它。



### （4）使myprog成为一个SET-UID user1程序，在user2用户（非root用户）中再次设置LD\_PRELOAD环境变量，运行myprog程序



## **实验结果说明：**

导致这三种输出不同的原因就在于LD\_PRELOAD环境变量。LD\_PRELOAD环境变量是Unix动态链接库的世界中的一个环境变量，它可以影响程序的运行时的链接，它允许你定义在程序运行前优先加载的动态链接库。这个功能主要是用来有选择性的载入不同动态链接库中的相同函数。

在该实验中，mylib.c通过sleep函数，生成了一个libmylib.so.1.0.1链接库。然后将该链接库添加到LD\_PRELOAD环境变量上。

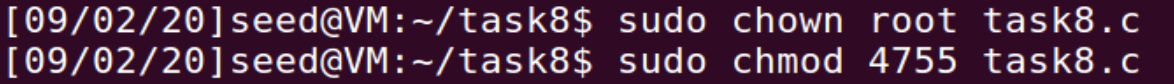
**第一种和第三种情况下，myprog程序均具有seed用户权限，而在seed用户的LD\_PRELOAD环境变量中也添加了该链接库。因此，这两个输出结果为用户新定义的sleep()函数的返回值。**

**在第二种情况下，普通用户运行有root权限的程序，输出结果就为原本的sleep()函数的返回值。**

**在第四种情况下，在非root非seed的用户cy中运行myprog程序，此时LD\_PRELOAD环境变量中并未添加该链接库，所以输出结果为原本的sleep()函数的返回值。**

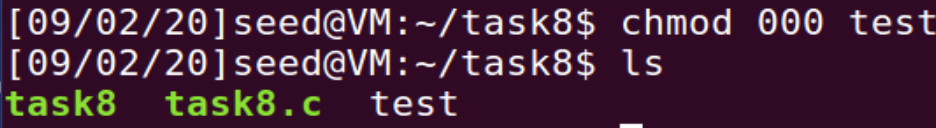
# Invoking External Programs Using system() versus execve()

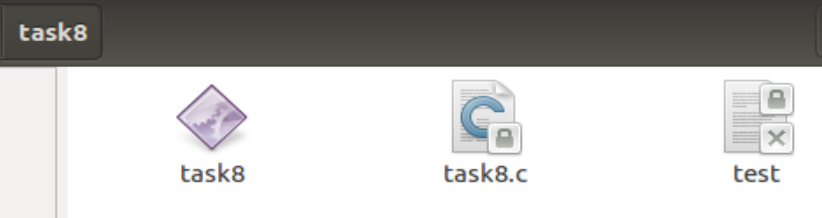
## **Step1.** 编译上述程序，使其成为root拥有的SET-UID程序。



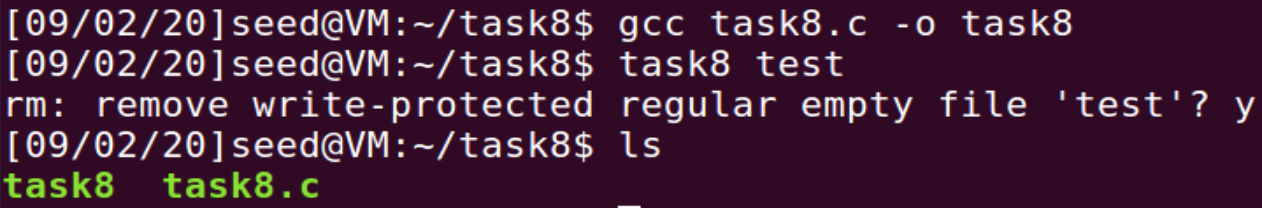
该程序task8.c会使用system()来调用命令。如果将代码中的参数v[0] = "/bin/cat"改为v[0] = "rm"，即删除命令，就可以实现删除文件的功能。

创建一个用户不可写的文件test，将其权限改为000，下图为执行程序之前task8文件夹中文件列表。





执行以下命令，./task8 test，可发现test文件被删除。

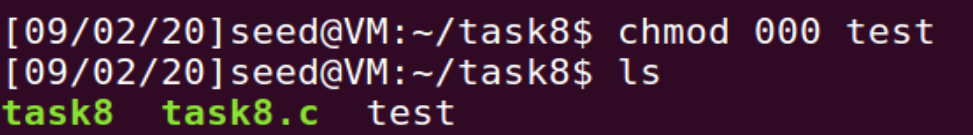


本来test对seed用户是不可写的，但因为task8是SET-UID程序，且为root权限，因此可以删除test文件。

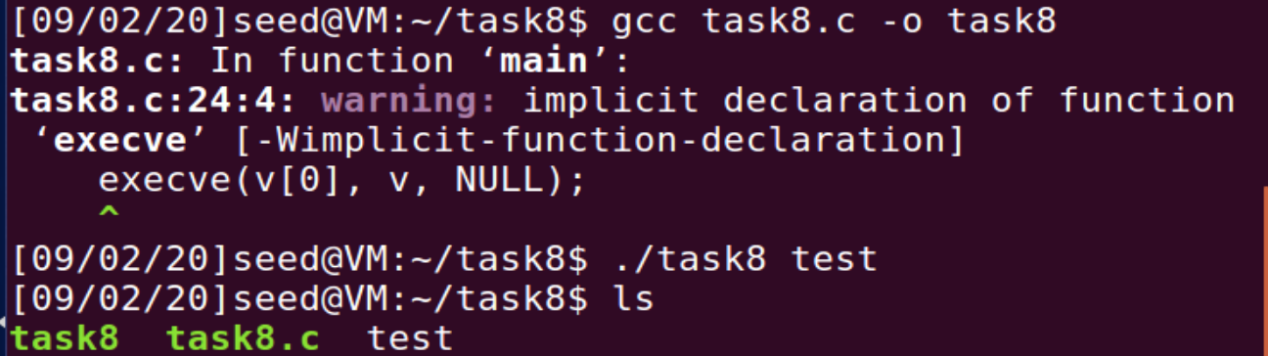
**由此可得出结论：SET-UID程序中的system()函数可能会带来危险。**

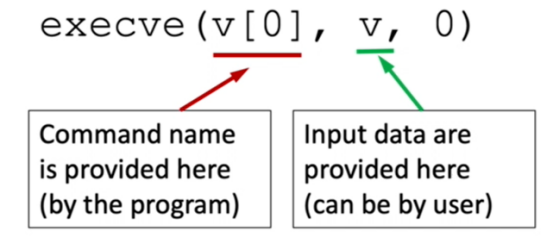
## **Step2.** 注释掉system(command)语句，并取消注释execve()语句。程序将使用execve()来调用命令。编译程序，并使其成为Set-UID程序。那么在步骤一中的攻击是否仍然有效？

创建一个用户不可写的文件test，将其权限改为000，下图为执行程序之前task8文件夹中文件列表。



修改task8.c，注释掉system()语句，取消注释execve()语句，执行以下命令——./task8 test，可发现test文件未被删除，Step1中的攻击没有成功。



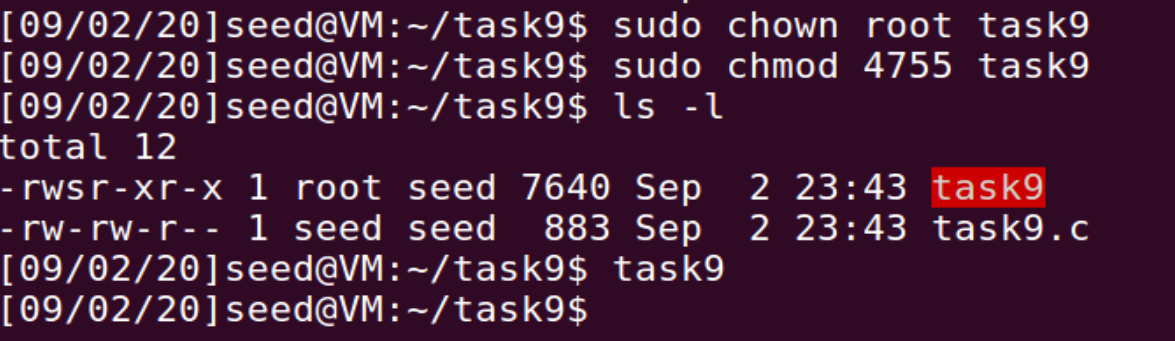


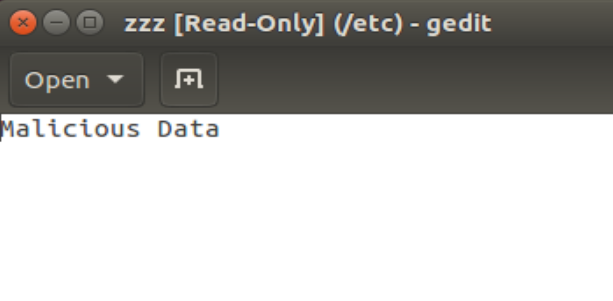
**execve()函数只会执行v[0]中的命令，从而将代码（即指令）与用户输入的数据区分开来，所以用户输入的数据（例如test文件名）不会变成整个shell程序的一部分。所以Step1中的攻击无法实现。**

# Capability Leaking

编译以下程序，将其所有者更改为root，并将其设置为SET-UID程序。以普通用户身份运行程序，并描述所观察到的内容，观察文件/etc/zzz是否被修改。

## **实验结果截图：**





可以看到，原本不能写的文件zzz被修改了，写入了“Maliciou Data”。

## **实验结果说明：**

（部分源代码如下）

/\* Simulate the tasks conducted by the program \*/

sleep(1);

/\* After the task, the root privileges are no longer needed,

it's time to relinquish the root privileges permanently. \*/

setuid(getuid()); /\* getuid() returns the real uid \*/

if (fork()) { /\* In the parent process \*/

close (fd);

exit(0);

} else { /\* in the child process \*/

/\* Now, assume that the child process is compromised, malicious

attackers have injected the following statements

into this process \*/

write (fd, "Malicious Data\n", 15);

close (fd);

}

在setuid(getuid())处，root特权已经被降级，但是write (fd, "Malicious Data\n", 15)语句仍然能够执行，这就说明普通用户通过使用SET-UID程序，获得了只有root才能写的文件zzz的修改权，Capability Leaking攻击实现。