**Environment Variable and Set-UID Program Lab**

57117214 吴国铨

**Task 1: Manipulating Environment Variables**

使用printenv打印变量

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=60817418

UPSTART\_SESSION=unix:abstract=/com/ubuntu/upstart-session/1000/1472

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/1753,unix/VM:/tmp/.ICE-unix/1753

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-lowgfx

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-bLAgB2vv4e

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

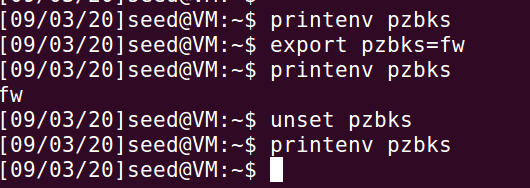
J2REDIR=/usr/lib/jvm/java-8-oracle/jre

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

XAUTHORITY=/home/seed/.Xauthority

\_=/usr/bin/printenv

使用export和unset设置和取消环境变量



**Task2: Passing Environment Variables from Parent Process to Child Process**

注释掉default分支的printenv，保留case 0分支的printenv，即为打印子进程环境变量，结果与task1的结果完全一致，并保存在child1中：



注释掉case0分支的printenv，保留default分支的printenv，即为打印父进程环境变量，结果与task1的结果完全一致，并保存在child2中：



使用diff child1 child2，输出为空，证明结果相同。

**Task 3: Environment Variables and execve()**

将NULL作为第二个参数传给execve：

execve(“/usr/bin/env”,argv,NULL)

编译运行后输出为空。

将外部变量environ作为第三个参数床给execve：

execve(“/usr/bin/env”,argv, environ)

输出结果与task1完全一致，证明使用execve()创建的子程序，环境变量取决于第三个参数。

**Task 4: Environment Variables and system()**

使用system(“/usr/bin/env”)，输出结果与task1完全一致，说明system()创建的子进程会继承父进程所有环境变量。

**Task 5: Environment Variable and Set-UID Programs**

使用sudo进行提权，将程序升级为root用户的set-uid程序。

在普通用户的Shell下，使用export命令设置：

path

LD\_LTBBRARY\_PATH

pzbks=fw

运行编译的程序：

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=gnomeSHELL=/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.s

o.1.64.0

WINDOWID=62914570

OLDPWD=/home/seed/Downloads

UPSTART\_SESSION=unix:abstract=/com/ubuntu/upstart-session/1000/1396 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:\*.l ha=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:\*.tbz 2=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=0 1;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:\*.fl ac=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/boo st\_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

GENIUS=pzbks

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

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

PATH=pzbks

QT\_IM\_MODULE=ibus

QT\_QPA\_PLATFORMTHEME=appmenu-qt5

XDG\_SESSION\_TYPE=x11

PWD=/home/seed

JOB=unity-settings-daemon 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-lowgfx 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

UPSTART\_INSTANCE=

UPSTART\_EVENTS=xsession started

XDG\_SESSION\_DESKTOP=ubuntu

LOGNAME=seed

COMPIZ\_BIN\_PATH=/usr/bin/

DBUS\_SESSION\_BUS\_ADDRESS=unix:abstract=/tmp/dbus-fJdXl82raq 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= UPSTART\_JOB=unity7

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

\_=./task5

其中，PATH和GENIUS都变成了pzbks，但是LD\_LTBRARY\_PATH没有变，是因为set-uid程序会自动忽略LD\_LTBRARY\_PATH环境变量

**Task 6: The PATH Environment Variable and SetUID Programs**

首先使用



将/bin/sh链接到/bin/zsh

然后将当前的home路径添加到path中



在/home/seed下面编写ls.c

#include <stdio.h>

#include <sys/types.h>

#include <unistd.h>

int main() {

printf("Hi, I'm ls written by pzbks.\nRUID is %d, and EUID is %d.\n",getuid(), geteuid());

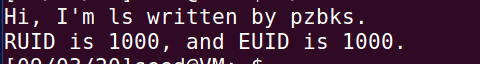
return 0;

}

并编译为ls程序



将给出代码作为task6，root成为set-uid程序，运行：



**Task 7: The LD\_PRELOAD Environment Variable and Set-UID Programs**

在当前目录下编译动态链接库libmylib.so.1.0.1

将LD\_PRELOAD设置为新编译的动态链接库

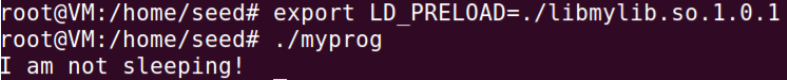
普通用户运行普通程序myprog：



说明sleep是libmylib.so.1.0.1的

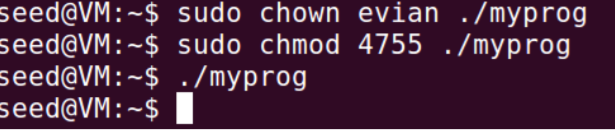
普通用户运行set-uid的root程序myprog，无输出，说明sleep是系统库的。

root⽤户设置好 LD\_PRELOAD 后运⾏setuid的root程序 myprog



说明sleep是libmylib.so.1.0.1的

当前用户运行set-uid的别的用户的普通程序myprog



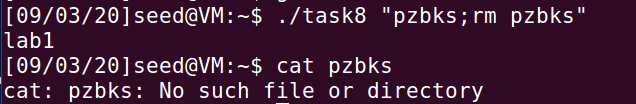
说明sleep是系统库的。

**Task 8: Invoking External Programs Using system() versus execve()**

首先创建一个pzbks文件，内容为“lab1”



调用时输入加上；来增加一行调用



第二次cat的时候文件已经被删除，因为执行内容是/bin/cat pzbks; rm pzbks

将system()改成execve()，重新操作，



在execve()中，“pzbks；rm pzbks”被当作参数传递给子程序，所以找不到这个文件

**Task 9: Capability Leaking**

创建/etc/zzz文件，输入题目程序，并查看文件



能够写入。

因为在调用fork()之前，fd并没有被关闭，因此子进程会复制父进程所有文件描述，包括fd，尽管在父进程中使用close（fd）关闭了fd，但是在子进程中的fd不收父进程影响，依然存在，此时尽管子进程权限已经被降级，但是拥有文件描述符，可以对/etc/zzz文件进行写操作