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

**57118133 钟杰**

**Task 1：Manipulating Environment Variables**

1. **Use printenv or env command to print out the environment variables.**

**实验结果：**

[09/02/20]seed@VM:~$ printenv

XDG\_VTNR=7

ORBIT\_SOCKETDIR=/tmp/orbit-seed

XDG\_SESSION\_ID=c1

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

TERMINATOR\_UUID=urn:uuid:68d16744-29dc-4fc2-9193-c128e6511cf4

IBUS\_DISABLE\_SNOOPER=1

CLUTTER\_IM\_MODULE=xim

SESSION=ubuntu

GIO\_LAUNCHED\_DESKTOP\_FILE\_PID=5345

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

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

TERM=xterm

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=52428804

UPSTART\_SESSION=unix:abstract=/com/ubuntu/upstart-session/1000/1913

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

GIO\_LAUNCHED\_DESKTOP\_FILE=/usr/share/applications/terminator.desktop

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=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

IM\_CONFIG\_PHASE=1

GDMSESSION=ubuntu

SESSIONTYPE=gnome-session

GTK2\_MODULES=overlay-scrollbar

SHLVL=1

HOME=/home/seed

XDG\_SEAT=seat0

LANGUAGE=en\_US

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

UPSTART\_INSTANCE=

XDG\_SESSION\_DESKTOP=ubuntu

UPSTART\_EVENTS=xsession started

LOGNAME=seed

COMPIZ\_BIN\_PATH=/usr/bin/

DBUS\_SESSION\_BUS\_ADDRESS=unix:abstract=/tmp/dbus-PVnZz5loPY

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

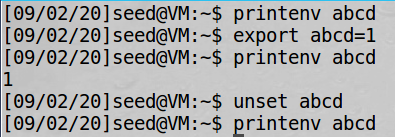
XAUTHORITY=/home/seed/.Xauthority

COLORTERM=gnome-terminal

\_=/usr/bin/printenv

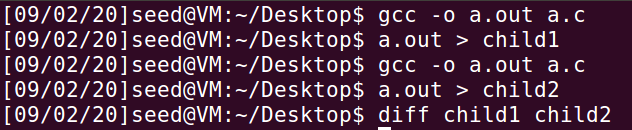
1. **Use export and unset to set or unset environment variables.**

**代码段：**

****

**Task 2：Passing Environment Variables from Parent Process to Child Process**

**代码段：**

****

**分析：**

通过比较这两个文件，可以发现，这两个文件输出的环境变量完全相同。说明原环境变量被子进程完全继承。通过man fork，对fork函数做了进一步了解。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资格，环境，堆栈与内存根目录等；但是子进程没有继承父进程的某些特性，比如父进程号，文件描述符，在tms结构中的系统时间，资源使用等。

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

**运行结果：**

[09/02/20]seed@VM:~/.../task 3$ gcc -o b.out b.c

b.c: In function ‘main’:

b.c:9:2: warning: implicit declaration of function ‘execve’ [-Wimplicit-function-declaration]

execve("/usr/bin/env", argv, NULL);

^

[09/02/20]seed@VM:~/.../task 3$ ./b.out

[09/02/20]seed@VM:~/.../task 3$ gcc -o b.out b.c

b.c: In function ‘main’:

b.c:9:2: warning: implicit declaration of function ‘execve’ [-Wimplicit-function-declaration]

execve("/usr/bin/env", argv, environ);

^

[09/02/20]seed@VM:~/.../task 3$ ./b.out

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=50331658

UPSTART\_SESSION=unix:abstract=/com/ubuntu/upstart-session/1000/1913

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/2367,unix/VM:/tmp/.ICE-unix/2367

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/Desktop/task 3

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

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

XDG\_SESSION\_DESKTOP=ubuntu

LOGNAME=seed

DBUS\_SESSION\_BUS\_ADDRESS=unix:abstract=/tmp/dbus-PVnZz5loPY

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

\_=./b.out

**结论：**

int execve(const char \* filename，char \* const argv[]，char \* const envp[])

execve()用来执行参数filename字符串所代表的文件路径，filename必须是一个二进制的可执行文件，或者是一个脚本以#!格式开头的解释器参数。如果是后者，这个解释器必须是一个可执行的有效的路径名。第二个参数系利用数组指针来传递给执行文件，argv是要调用的程序执行的参数序列，也就是我们要调用的程序需要传入的参数。envp则为传递给执行文件的新环境变量数组,同样也为参数序列。

从以上实验可以看出，execve()产生的新进程的环境变量又调用时重新赋予，而fork()则是直接继承父进程环境变量。

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

**运行结果：**

[09/02/20]seed@VM:~/.../task 4$ gcc -o a.out a.c

[09/02/20]seed@VM:~/.../task 4$ ./a.out

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

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

HOME=/home/seed

QT4\_IM\_MODULE=xim

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-PVnZz5loPY

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=50331658

\_=./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/2367,unix/VM:/tmp/.ICE-unix/2367

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/1000/1913

XDG\_VTNR=7

QT\_IM\_MODULE=ibus

PWD=/home/seed/Desktop/task 4

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

**结论：**

system函数定义为 int system（const char \* string），该函数调用/bin/sh来执行参数指定的命令,/bin/sh一般是一个软连接，指向某个具体的shell，比如bash,-c 选项是告诉shell从字符串command中读取命令；在该command执行期间，SIGCHLD信号会被暂时搁置，SIGINT和SIGQUIT则会被忽略，意思是进程收到这两个信号后没有任何动作。system（）函数的函数返回值有些复杂。为了更好地理解system（）函数的返回值，需要了解其执行过程，实际上system（）函数执行了三步操作：

1 fork一个子进程；  
2 在子进程中调用exec函数去执行command；  
3 在父进程中调用wait去等待子进程结束。

若fork失败，system（）函数返回-1。如果exec执行成功，也即command顺利执行完毕，则返回command通过exit或return返回的值。（注意，command顺利执行不代表执行成功，例如command：“rm debuglog.txt”，不管文件存不存在该command都顺利执行了）如果exec执行失败，也即command没有顺利执行，比如信号被中断，或者command命令根本不存在，system（）函数返回127，如果command为NULL，则system（）函数返回值非0，一般为1。

System（）函数的具体实现：



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

**运行结果：**

[09/02/20]seed@VM:~/.../task 5$ gcc -o a.out a.c

[09/02/20]seed@VM:~/.../task 5$ ./a.out

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=18874378

UPSTART\_SESSION=unix:abstract=/com/ubuntu/upstart-session/1000/2010

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/2368,unix/VM:/tmp/.ICE-unix/2368

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/Desktop/task 5

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

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

XDG\_SESSION\_DESKTOP=ubuntu

LOGNAME=seed

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

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

[09/02/20]seed@VM:~/.../task 5$ sudo chown root a.c

[09/02/20]seed@VM:~/.../task 5$ sudo chmod 4755 a.c

[09/02/20]seed@VM:~/.../task 5$ export PATH="$PATH:/usr/local/"

[09/02/20]seed@VM:~/.../task 5$ export LD\_LIBRARY\_PATH="$LD\_LIBRARY\_PATH:/usr/local/"

[09/02/20]seed@VM:~/.../task 5$ export ANY\_NAME="/usr/local"

[09/02/20]seed@VM:~/.../task 5$ gcc -o a.out a.c

[09/02/20]seed@VM:~/.../task 5$ ./a.out

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=18874378

UPSTART\_SESSION=unix:abstract=/com/ubuntu/upstart-session/1000/2010

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::/usr/local/

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/2368,unix/VM:/tmp/.ICE-unix/2368

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:/usr/local/

QT\_IM\_MODULE=ibus

QT\_QPA\_PLATFORMTHEME=appmenu-qt5

XDG\_SESSION\_TYPE=x11

PWD=/home/seed/Desktop/task 5

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

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

XDG\_SESSION\_DESKTOP=ubuntu

LOGNAME=seed

ANY\_NAME=/usr/local

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

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

可知，修改的三个环境变量已包含在shell中

**Task 6: The PATH Environment Variable and** Set-UID **Programs**

**实验步骤：**

[09/02/20]seed@VM:~/.../task6$ export PATH=/home/seed/Desktop/task6:$PATH

[09/02/20]seed@VM:~/.../task 6$ sudo rm /bin/sh

[09/02/20]seed@VM:~/.../task 6$ sudo ln -s /bin/zsh /bin/sh

[09/02/20]seed@VM:~/.../task 6$ sudo gcc -o a.out a.c

[09/02/20]seed@VM:~/.../task 6$ sudo chown root a.out

[09/02/20]seed@VM:~/.../task 6$ sudo chmod 4755 a.out

[09/02/20]seed@VM:~/.../task 6$ ls -l a.out

-rwsr-xr-x 1 root root 7344 Sep 2 11:15 a.out

//使用ls -l demo6语句查看文件的权限，验证操作确实成功完成，符合题设条件

[09/02/20]seed@VM:~/.../task 6$ cp /bin/sh ls

[09/02/20]seed@VM:~/.../task 6$ a.out

VM% printenv PATH

/home/seed/Desktop/task6:/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

//将bin/sh复制到当前目录并命名为ls，执行demo6就会获得root权限。详细分析，先看一下PATH环境变量，它的命令找寻顺序是先找寻当前目录，而当前目录我们自己编造了一个ls，所以程序就会直接执行伪造的ls。sh原本的作用是创建一个新shell，在执行此命令后我们就会一直停留在子进程中，知道我们主动退出这个程序，我们才会回到原来的权限。

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

以普通用户的身份运行myprog程序时，输出：I am not sleeping!  
以普通用户运行拥有root权限的myprog程序时，无输出。  
在user2用户中再次设置LD\_PRELOAD环境变量并运行myprog程序时，输出：I am not sleeping!

导致他们不同的原因就在于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。比较这三次实验，第一次和第三次实验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

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

**实验步骤：**

[09/02/20]seed@VM:~/.../task 8$ sudo gcc -o a.out a.c

[09/02/20]seed@VM:~/.../task 8$ sudo chown root a.out

[09/02/20]seed@VM:~/.../task 8$ sudo chmod 4755 a.out

[09/02/20]seed@VM:~/.../task 8$ chmod u=rwx,g=---,o=--- MY

[09/02/20]seed@VM:~/.../task 8$ ls -l MY

-rwx------ 1 seed seed 0 Sep 2 12:07 MY

[09/02/20]seed@VM:~/.../task 8$ a.out "MY;mv MY my"

[09/02/20]seed@VM:~/.../task 8$ ls

1. c a.out my

新建一个名为MY的文件，并设置其权限为仅root用户可读、写、执行。  
执行demo8，发现原本只有root用户才具有读、写、执行的MY文件，已经更名为my

注释掉system(command)语句，并取消execve（）语句的注释

[09/02/20]seed@VM:~/.../task 8$ gcc -o a.out a.c

a.c: In function ‘main’:

a.c:17:1: warning: implicit declaration of function ‘execve’ [-Wimplicit-function-declaration]

execve(v[0], v, NULL);

^

[09/02/20]seed@VM:~/.../task 8$ sudo chown root a.out

[09/02/20]seed@VM:~/.../task 8$ sudo chmod 4755 a.out

[09/02/20]seed@VM:~/.../task 8$ chmod u=rwx,g=---,o=--- MY

[09/02/20]seed@VM:~/.../task 8$ ls

a.c a.out MY

因为execve()函数会把file; mv file file\_new 看成是一个文件名，系统会提示不存在这个文件，system()则不会。

**Task 9: Capability Leaking**

**实验步骤：**[09/02/20]seed@VM:~/.../task 9$ sudo chmod u=rwx,g=r-x,o=r-x /etc/zzz

chmod: cannot access '/etc/zzz': No such file or directory

[09/02/20]seed@VM:~/.../task 9$ sudo touch /etc/zzz

[09/02/20]seed@VM:~/.../task 9$ sudo chmod u=rwx,g=r--,o=r-- /etc/zzz

[09/02/20]seed@VM:~/.../task 9$ sudo ls -l /etc/zzz

-rwxr--r-- 1 root root 0 Sep 2 12:20 /etc/zzz

[09/02/20]seed@VM:~/.../task 9$ sudo gcc -o a.out a.c

a.c: In function ‘main’:

a.c:15:1: warning: implicit declaration of function ‘sleep’ [-Wimplicit-function-declaration]

sleep(1);

^

a.c:18:1: warning: implicit declaration of function ‘setuid’ [-Wimplicit-function-declaration]

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

^

a.c:18:8: warning: implicit declaration of function ‘getuid’ [-Wimplicit-function-declaration]

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

^

a.c:19:5: warning: implicit declaration of function ‘fork’ [-Wimplicit-function-declaration]

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

^

a.c:20:1: warning: implicit declaration of function ‘close’ [-Wimplicit-function-declaration]

close (fd);

^

a.c:25:1: warning: implicit declaration of function ‘write’ [-Wimplicit-function-declaration]

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

^

[09/02/20]seed@VM:~/.../task 9$ sudo chown root a.out

[09/02/20]seed@VM:~/.../task 9$ sudo chmod 4755 a.out

执行a.out，查看内容，发现被写入信息

[09/02/20]seed@VM:~/.../task 9$ a.out

[09/02/20]seed@VM:~/.../task 9$ cat /etc/zzz

Malicious Data

因为在取消权限前并没有关闭文件，导致seed用户任然可以进行root用户才可以执行的写入操作。