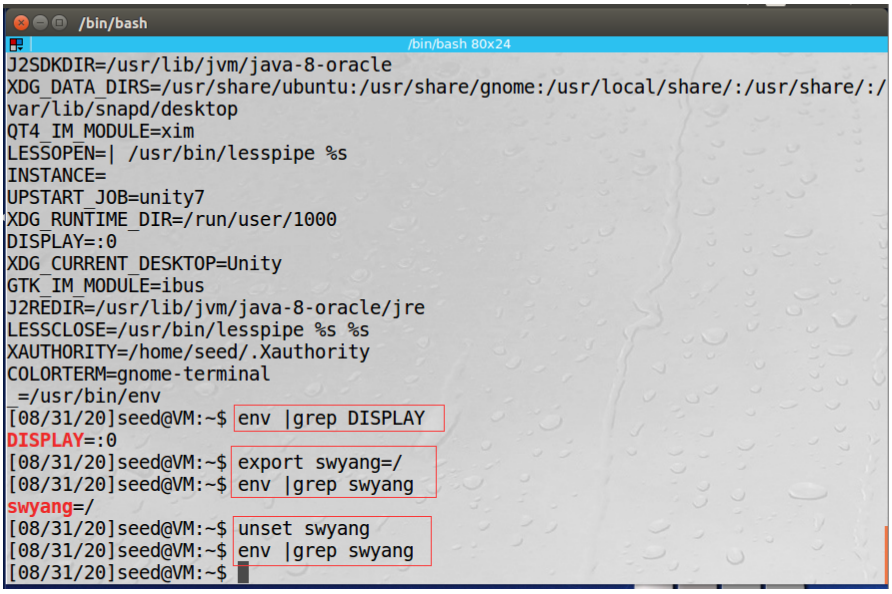
Set-UID Program Lab

Task1：Manipulating Environment Variables



```
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/env
[08/31/20]seed@VM:~$ env |grep DISPLAY
DISPLAY=:0
[08/31/20]seed@VM:~$ export swyang=/
[08/31/20]seed@VM:~$ env |grep swyang
swyang=/
[08/31/20]seed@VM:~$ unset swyang
[08/31/20]seed@VM:~$ env |grep swyang
[08/31/20]seed@VM:~$
```

Task2：Passing Environment Variables from ParentProcess to ChildProcess

1、child file

```
XDG_VTNR=7
ORBIT_SOCKETDIR=/tmp/orbit-seed
XDG_SESSION_ID=c1
XDG_GREETER_DATA_DIR=/var/lib/lightdm-data/seed
IBUS_DISABLE_SNOOPER=1
TERMINATOR_UUID=urn:uuid:d57ac218-c10f-4ff5-894a-db0f83810d9e
CLUTTER_IM_MODULE=xim
SESSION=ubuntu
GIO_LAUNCHED_DESKTOP_FILE_PID=2618
ANDROID_HOME=/home/seed/android/android-sdk-linux
GPG_AGENT_INFO=/home/seed/.gnupg/S.gpg-agent:0:1
TERM=xterm
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/b
oost/libboost_filesystem.so.1.64.0:/home/seed/lib/boost/libboost_system.so.1.64.0
WINDOWID=58720260
```

```
UPSTART_SESSION=unix:abstract=/com/ubuntu/upstart-session/1000/1415
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/lab0
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=
XDG_SESSION_DESKTOP=ubuntu
UPSTART_EVENTS=xsession started
LOGNAME=seed
COMPIZ_BIN_PATH=/usr/bin/
DBUS_SESSION_BUS_ADDRESS=unix:abstract=/tmp/dbus-oqDRYTXndx
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
_=./a.out
OLDPWD=/home/seed
```

2、parent file

```
XDG_VTNR=7
ORBIT_SOCKETDIR=/tmp/orbit-seed
XDG_SESSION_ID=c1
XDG_GREETER_DATA_DIR=/var/lib/lightdm-data/seed
IBUS_DISABLE_SNOOPER=1
TERMINATOR_UUID=urn:uuid:8e03884e-b1cf-4f07-9555-f50111a6c13e
CLUTTER_IM_MODULE=xim
SESSION=ubuntu
GIO_LAUNCHED_DESKTOP_FILE_PID=3565
ANDROID_HOME=/home/seed/android/android-sdk-linux
GPG_AGENT_INFO=/home/seed/.gnupg/S.gpg-agent:0:1
TERM=xterm
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=58720260
UPSTART_SESSION=unix:abstract=/com/ubuntu/upstart-session/1000/1415
GNOME_KEYRING_CONTROL=
GTK_MODULES=gail:atk-bridge:unity-gtk-module
```

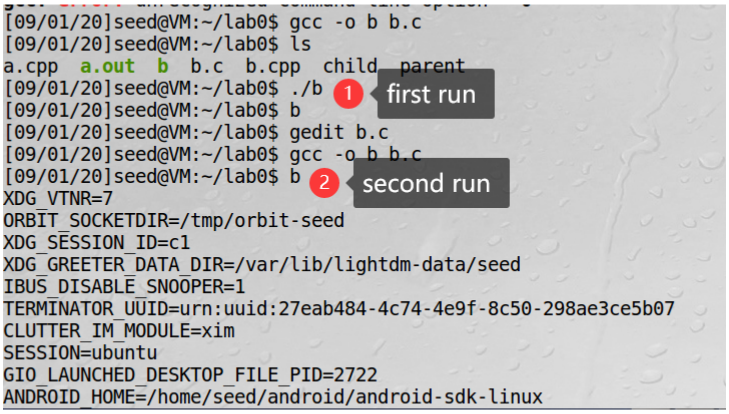
```
USER=seed
LS_COLORS=rs=0:di=01;34:ln=01;36:mh=00:pi=40;33:so=01;35:do=01;35:bd=40;33;01:cd=40
;33;01:or=40;31;01:mi=00:su=37;41:sg=30;43:ca=30;41:tw=30;42:ow=34;42:st=37;44:ex=0
1;32:*.tar=01;31:*.tgz=01;31:*.arc=01;31:*.arj=01;31:*.taz=01;31:*.lha=01;31:*.lz4=
01;31:*.lzh=01;31:*.lzma=01;31:*.tlz=01;31:*.txz=01;31:*.tzo=01;31:*.t7z=01;31:*.zi
p=01;31:*.z=01;31:*.Z=01;31:*.dz=01;31:*.gz=01;31:*.lrz=01;31:*.lz=01;31:*.lzo=01;3
1:*.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;3
1:*.ace=01;31:*.zoo=01;31:*.cpio=01;31:*.7z=01;31:*.rz=01;31:*.cab=01;31:*.jpg=01;3
5:*.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:*.m
kv=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;3
6:*.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:/u
sr/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/lab0
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=
XDG_SESSION_DESKTOP=ubuntu
UPSTART_EVENTS=xsession started
LOGNAME=seed
COMPIZ_BIN_PATH=/usr/bin/
DBUS_SESSION_BUS_ADDRESS=unix:abstract=/tmp/dbus-oqDRYTXndx
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
OLDPWD=/home/seed
_=./a.out
```

3、conclusion

From the child file and parent file, we can learn that when parentprocess create a childprocess, parent's environment vaiables are inherited by the child process.

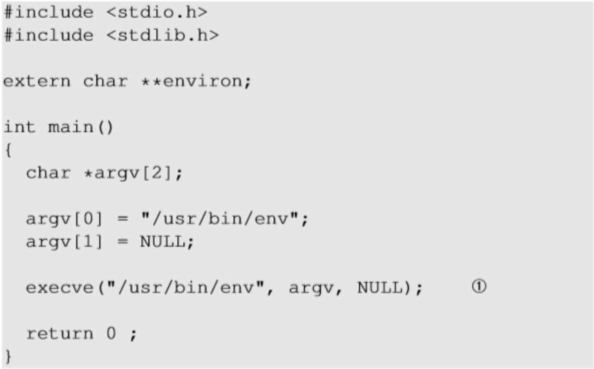
Task3: Environment Variables and execve()



```
[09/01/20]seed@VM:~/lab0$ gcc -o b b.c
[09/01/20]seed@VM:~/lab0$ ls
a.cpp  a.out  b  b.c  b.cpp  child  parent
[09/01/20]seed@VM:~/lab0$ ./b
[09/01/20]seed@VM:~/lab0$ b
[09/01/20]seed@VM:~/lab0$ gedit b.c
[09/01/20]seed@VM:~/lab0$ gcc -o b b.c
[09/01/20]seed@VM:~/lab0$ b
XDG_VTNR=7
ORBIT_SOCKETDIR=/tmp/orbit-seed
XDG_SESSION_ID=c1
XDG_GREETER_DATA_DIR=/var/lib/lightdm-data/seed
IBUS_DISABLE_SNOOPER=1
TERMINATOR_UUID=urn:uuid:27eab484-4c74-4e9f-8c50-298ae3ce5b07
CLUTTER_IM_MODULE=xim
SESSION=ubuntu
GIO_LAUNCHED_DESKTOP_FILE_PID=2722
ANDROID_HOME=/home/seed/android/android-sdk-linux
```

1、frist run

At first, we compile and run the following program

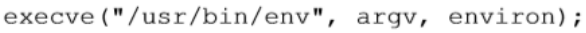


```
#include <stdio.h>
#include <stdlib.h>

extern char **environ;

int main()
{
  char *argv[2];

  argv[0] = "/usr/bin/env";
  argv[1] = NULL;

  execve("/usr/bin/env", argv, NULL);    ①

  return 0 ;
}
```

From the above picture,we can find the program outputs nothing.

2、second run

Second， we change the invocation of `execve()` in line 1 to the following



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

From the above picture, we can find the program outputs the user environment variables.

3、conclusion

a new program can get its environment variables by use the environ-user environment.

we can declare in C code like this:

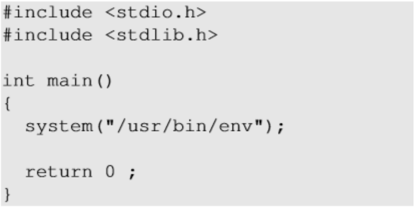
```
extern char**environ;
```

Then， use the function `execve` to get its environment variables:

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

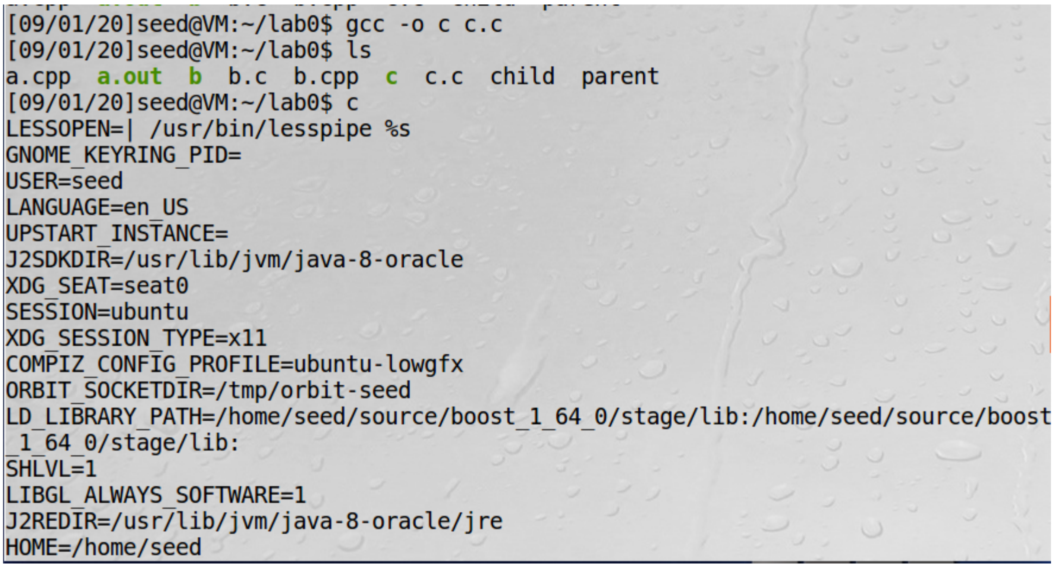
Task4: Environment Variables and system()

First we compile and run the following program.



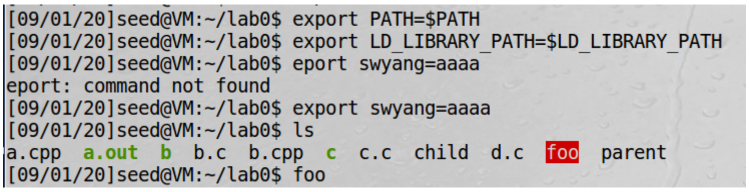
```
#include <stdio.h>
#include <stdlib.h>

int main()
{
  system("/usr/bin/env");

  return 0 ;
}
```

The result is as follows, we can see that the program outputs the user's environment variables.We can learn that the environment variables of the calling process is passed to the newprogram /bin/sh.



```
[09/01/20]seed@VM:~/lab0$ gcc -o c c.c
[09/01/20]seed@VM:~/lab0$ ls
a.cpp  a.out  b  b.c  b.cpp  c  c.c  child  parent
[09/01/20]seed@VM:~/lab0$ c
LESSOPEN=| /usr/bin/lesspipe %s
GNOME_KEYRING_PID=
USER=seed
LANGUAGE=en_US
UPSTART_INSTANCE=
J2SDKDIR=/usr/lib/jvm/java-8-oracle
XDG_SEAT=seat0
SESSION=ubuntu
XDG_SESSION_TYPE=x11
COMPIZ_CONFIG_PROFILE=ubuntu-lowgfx
ORBIT_SOCKETDIR=/tmp/orbit-seed
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
```

*Task5: Environment Variableand Set-UID Programs



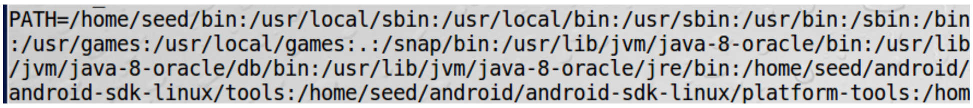
```
[09/01/20]seed@VM:~/lab0$ export PATH=$PATH
[09/01/20]seed@VM:~/lab0$ export LD_LIBRARY_PATH=$LD_LIBRARY_PATH
[09/01/20]seed@VM:~/lab0$ eport swyang=aaaa
eport: command not found
[09/01/20]seed@VM:~/lab0$ export swyang=aaaa
[09/01/20]seed@VM:~/lab0$ ls
a.cpp  a.out  b  b.c  b.cpp  c  c.c  child  d.c  foo  parent
[09/01/20]seed@VM:~/lab0$ foo
```

After get the foo file, we use the command `export` to set the PATH, LD LIBRARY PATH and swyang environment variables.

2、result

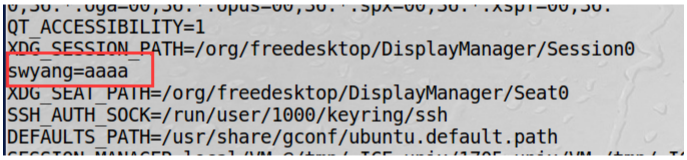
when we run foo,we found the PATH and swyang environment variables that we set in the output:

1. PATH



```
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:/hom
```

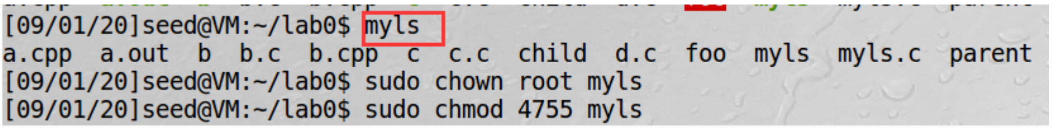
2. swyang



```
QT_ACCESSIBILITY=1
XDG_SESSION_PATH=/org/freedesktop/DisplayManager/Session0
swyang=aaaa
XDG_SEAT_PATH=/org/freedesktop/DisplayManager/Seat0
SSH_AUTH_SOCK=/run/user/1000/keyring/ssh
DEFAULTS_PATH=/usr/share/gconf/ubuntu.default.path
```

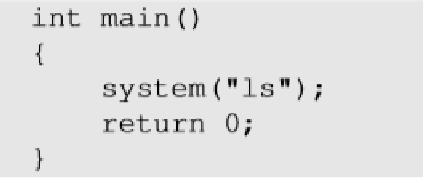
Task6：The PATH Environment Variable and Set-UID Programs

1、create a file named myls.c and compile it.we can see that the myls lists the current files in current directory



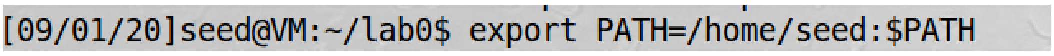
```
[09/01/20]seed@VM:~/lab0$ myls
a.cpp  a.out  b  b.c  b.cpp  c  c.c  child  d.c  foo  myls  myls.c  parent
[09/01/20]seed@VM:~/lab0$ sudo chown root myls
[09/01/20]seed@VM:~/lab0$ sudo chmod 4755 myls
```

the code in myls is as follows:



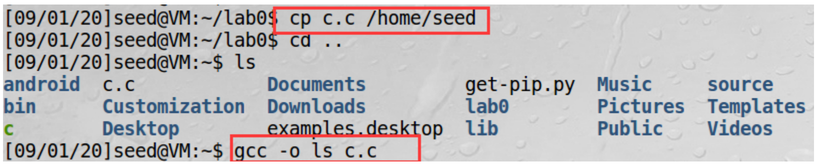
```
int main()
{
    system("ls");
    return 0;
}
```

2、First,we change the environment variables by export:



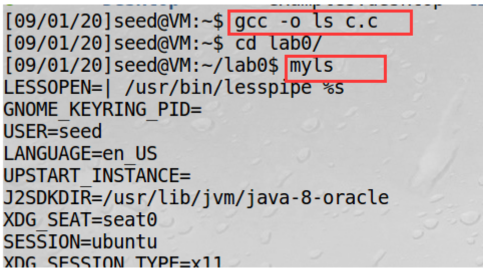
```
[09/01/20]seed@VM:~/lab0$ export PATH=/home/seed:$PATH
```

3、 Then, we enter in the directory /home/seed， copy the file c.c in lab0 directory to the /home/seed and com pile it



```
[09/01/20]seed@VM:~/lab0$ cp c.c /home/seed
[09/01/20]seed@VM:~/lab0$ cd ..
[09/01/20]seed@VM:~$ ls
android  c.c            Documents         get-pip.py  Music     source
bin      Customization  Downloads         lab0        Pictures  Templates
c        Desktop        examples.desktop  lib         Public    Videos
[09/01/20]seed@VM:~$ gcc -o ls c.c
```

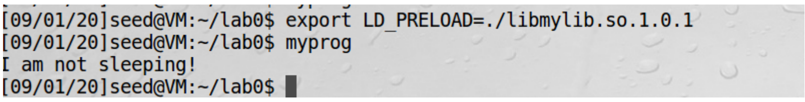
4、come back directory lab0 and run myls, we can see that the output is environment variables rhther than file name.



```
[09/01/20]seed@VM:~$ gcc -o ls c.c
[09/01/20]seed@VM:~$ cd lab0/
[09/01/20]seed@VM:~/lab0$ myls
LESSOPEN=| /usr/bin/lesspipe %s
GNOME_KEYRING_PID=
USER=seed
LANGUAGE=en_US
UPSTART_INSTANCE=
J2SDKDIR=/usr/lib/jvm/java-8-oracle
XDG_SEAT=seat0
SESSION=ubuntu
XDG_SESSION_TYPE=x11
```

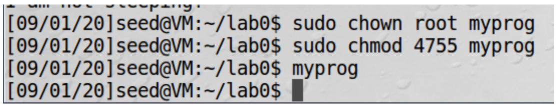
Task7：The LD_PRELOAD Environment Variableand Set-UID Programs

1、The first condition,we can see that program outputs the string "I am not sleeping"



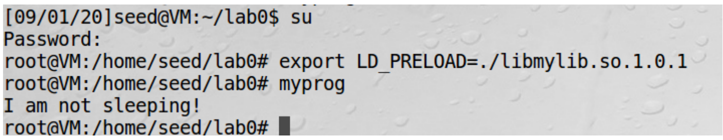
```
[09/01/20]seed@VM:~/lab0$ export LD_PRELOAD=./libmylib.so.1.0.1
[09/01/20]seed@VM:~/lab0$ myprog
I am not sleeping!
[09/01/20]seed@VM:~/lab0$ 
```

2、The second condition,we can see that the system have a one seond sleep.



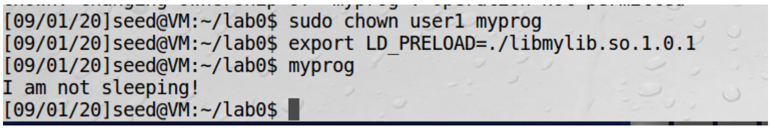
```
[09/01/20]seed@VM:~/lab0$ sudo chown root myprog
[09/01/20]seed@VM:~/lab0$ sudo chmod 4755 myprog
[09/01/20]seed@VM:~/lab0$ myprog
[09/01/20]seed@VM:~/lab0$ 
```

3、The third condition ,we can see that program outputs the string "I am not sleeping"



```
[09/01/20]seed@VM:~/lab0$ su
Password:
root@VM:/home/seed/lab0# export LD_PRELOAD=./libmylib.so.1.0.1
root@VM:/home/seed/lab0# myprog
I am not sleeping!
root@VM:/home/seed/lab0# 
```

4、The fourth condition,we can see thatprogram outputs the string "I am not sleeping"



```
chown: changing ownership of 'myprog': Operation not permitted
[09/01/20]seed@VM:~/lab0$ sudo chown user1 myprog
[09/01/20]seed@VM:~/lab0$ export LD_PRELOAD=./libmylib.so.1.0.1
[09/01/20]seed@VM:~/lab0$ myprog
I am not sleeping!
[09/01/20]seed@VM:~/lab0$ 
```

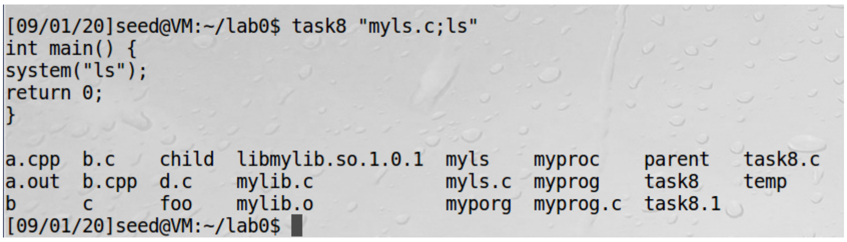
5、**reason**

We can see that only in the second condition,the system sleep. And The 3,4 conditons' output is the same as the first condition.

We can draw the conclusion that the environment variables is not be inherited by the child process.This makes LD_PRELOAD not changed， while 3 and 4 change the LD_PRELOAD by command `export`

Task8：Invoking External Programs Using system() versus execve()

1、can't compromist the integrity of the system,for example:

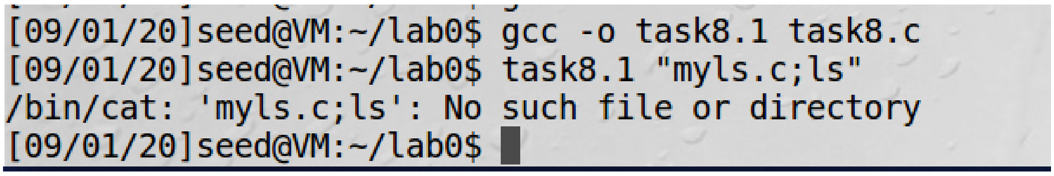


```
[09/01/20]seed@VM:~/lab0$ task8 "myls.c;ls"
int main() {
system("ls");
return 0;
}

a.cpp  b.c    child  libmylib.so.1.0.1  myls    myproc    parent  task8.c
a.out  b.cpp  d.c    mylib.c            myls.c  myprog    task8   temp
b      c      foo    mylib.o            myporg  myprog.c  task8.1
[09/01/20]seed@VM:~/lab0$ 
```

After compile the program named task8, we create a file named temp,and use the command `task8 "myls.c;ls"`, we can see that the program output the code in myls.c and also list the files in current directory.

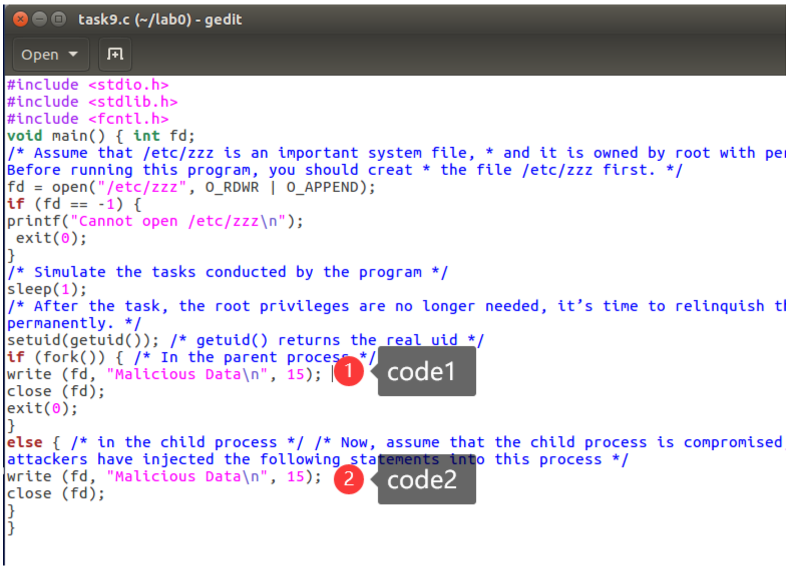
2、**not work**

we compile the program again,name it task8.1 and do the same operation, we can see that the attack can't be complished because the funciton `execve` finsh the separation between data and command.



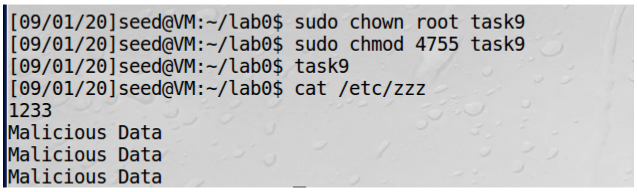
```
[09/01/20]seed@VM:~/lab0$ gcc -o task8.1 task8.c
[09/01/20]seed@VM:~/lab0$ task8.1 "myls.c;ls"
/bin/cat: 'myls.c;ls': No such file or directory
[09/01/20]seed@VM:~/lab0$ 
```

Task9：CapabilityLeaking



```
#include <stdio.h>
#include <stdlib.h>
#include <fcntl.h>
void main() { int fd;
/* Assume that /etc/zzz is an important system file, * and it is owned by root with pe
Before running this program, you should creat * the file /etc/zzz first. */
fd = open("/etc/zzz", O_RDWR | O_APPEND);
if (fd == -1) {
printf("Cannot open /etc/zzz\n");
 exit(0);
}
/* Simulate the tasks conducted by the program */
sleep(1);
/* After the task, the root privileges are no longer needed, it's time to relinquish t
permanently. */
setuid(getuid()); /* getuid() returns the real uid */
if (fork()) { /* In the parent process */
write (fd, "Malicious Data\n", 15);
close (fd);
exit(0);
}
else { /* in the child process */ /* Now, assume that the child process is compromised
attackers have injected the following statements into this process */
write (fd, "Malicious Data\n", 15);
close (fd);
}
}
```

From the above code,we can learn that parent process execute code1, child process execute code2. And in ParentProcess and Childprocess, Euid=ruid.But the handle fd is created before setuid()，so it still have privileged right and can wirte text into /etc/zzz.(The initial content of the file is "123\nMalicious Data\n")



```
[09/01/20]seed@VM:~/lab0$ sudo chown root task9
[09/01/20]seed@VM:~/lab0$ sudo chmod 4755 task9
[09/01/20]seed@VM:~/lab0$ task9
[09/01/20]seed@VM:~/lab0$ cat /etc/zzz
1233
Malicious Data
Malicious Data
Malicious Data
```