SEED Labs – Environment Variable and Set-UID Program Lab

57119130 马伟军

2021/7/7

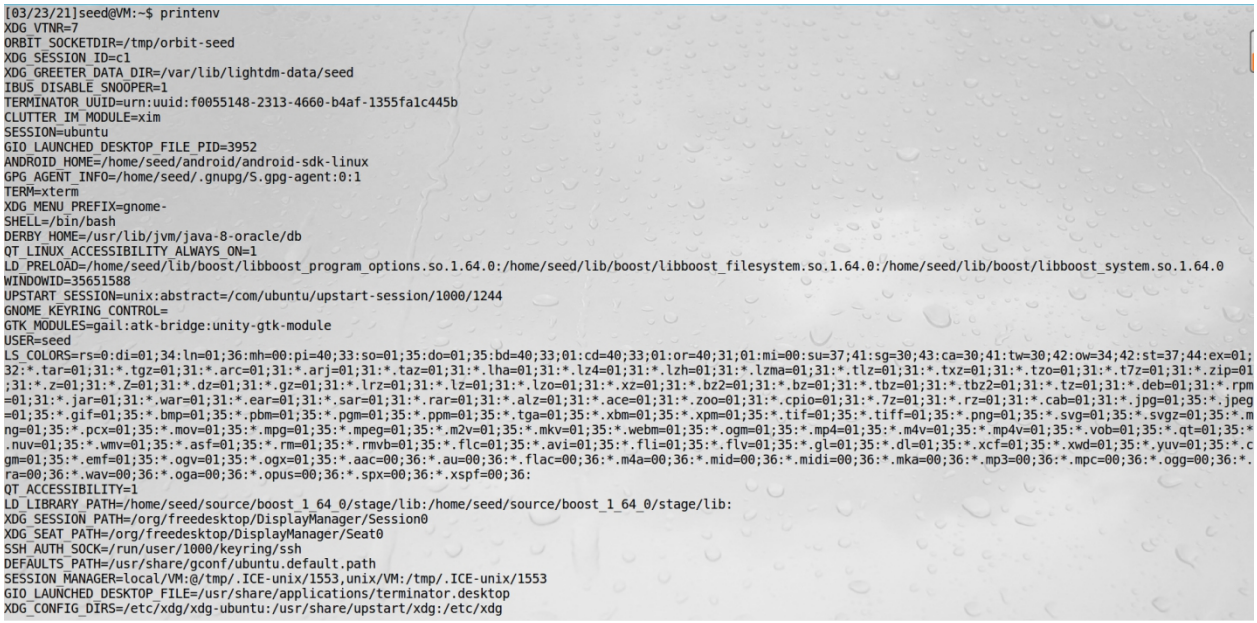
实验目的：

通过复现 SET_UID 实验，提高自己的动手能力，了解基本虚拟机的操作。

实验内容：

Task 1: Manipulating Environment Variables

用 printenv 命令打印出了所有的环境变量



```
[03/23/21]seed@VM:~$ printenv
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:f0055148-2313-4660-b4af-1355fa1c445b
CLUTTER_IM_MODULE=xim
SESSION=ubuntu
GIO_LAUNCHED_DESKTOP_FILE_PID=3952
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=35651588
UPSTART_SESSION=unix:abstract=/com/ubuntu/upstart-session/1000/1244
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:*.m
ng=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:*.c
gm=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/1553,unix/VM:/tmp/.ICE-unix/1553
GIO_LAUNCHED_DESKTOP_FILE=/usr/share/applications/terminator.desktop
XDG_CONFIG_DIRS=/etc/xdg/xdg-ubuntu:/usr/share/upstart/xdg:/etc/xdg
```

```
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=
XDG_SESSION_DESKTOP=ubuntu
UPSTART_EVENTS=xsession started
LOGNAME=seed
COMPIZ_BIN_PATH=/usr/bin/
DBUS_SESSION_BUS_ADDRESS=unix:abstract=/tmp/dbus-nVwFgoZhKQ
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
```

用 export 命令设置环境变量

```
[03/23/21]seed@VM:~$ export
declare -x ANDROID_HOME="/home/seed/android/android-sdk-linux"
declare -x CLUTTER_IM_MODULE="xim"
declare -x COLORTERM="gnome-terminal"
declare -x COMPIZ_BIN_PATH="/usr/bin/"
declare -x COMPIZ_CONFIG_PROFILE="ubuntu-lowgfx"
declare -x DBUS_SESSION_BUS_ADDRESS="unix:abstract=/tmp/dbus-nVwFgoZhKQ"
declare -x DEFAULTS_PATH="/usr/share/gconf/ubuntu.default.path"
declare -x DERBY_HOME="/usr/lib/jvm/java-8-oracle/db"
declare -x DESKTOP_SESSION="ubuntu"
declare -x DISPLAY=":0"
declare -x GDMSESSION="ubuntu"
declare -x GDM_LANG="en_US"
declare -x GIO_LAUNCHED_DESKTOP_FILE="/usr/share/applications/terminator.desktop"
declare -x GIO_LAUNCHED_DESKTOP_FILE_PID="3952"
declare -x GNOME_DESKTOP_SESSION_ID="this-is-deprecated"
declare -x GNOME_KEYRING_CONTROL=""
declare -x GNOME_KEYRING_PID=""
declare -x GPG_AGENT_INFO="/home/seed/.gnupg/S.gpg-agent:0:1"
declare -x GTK2_MODULES="overlay-scrollbar"
declare -x GTK_IM_MODULE="ibus"
declare -x GTK_MODULES="gail:atk-bridge:unity-gtk-module"
declare -x HOME="/home/seed"
declare -x IBUS_DISABLE_SNOOPER="1"
declare -x IM_CONFIG_PHASE="1"
declare -x INSTANCE=""
declare -x J2REDIR="/usr/lib/jvm/java-8-oracle/jre"
declare -x J2SDKDIR="/usr/lib/jvm/java-8-oracle"
declare -x JAVA_HOME="/usr/lib/jvm/java-8-oracle"
declare -x JOB="unity-settings-daemon"
declare -x LANG="en_US.UTF-8"
declare -x LANGUAGE="en_US"
declare -x LD_LIBRARY_PATH="/home/seed/source/boost_1_64_0/stage/lib:/home/seed/source/boost_1_64_0/stage/lib:"
declare -x 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"
declare -x LESSCLOSE="/usr/bin/lesspipe %s %s"
declare -x LESSOPEN="| /usr/bin/lesspipe %s"
declare -x LIBGL_ALWAYS_SOFTWARE="1"
declare -x LOGNAME="seed"
declare -x 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=
```

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

task1.c × task1m.c ×

```
1  #include <unistd.h>
2  #include <stdio.h>
3  #include <stdlib.h>
4
5  extern char **environ;
6
7  void printenv()
8  {
9
10 int i = 0;
11 while (environ[i] != NULL)
12 {
13 printf("%s\n", environ[i]);
14 i++;
15 }
16
17 }
18 void main()
19 {
20
21 pid_t childPid;
22
23 switch(childPid = fork())
24 {
25 case 0: /* child process */
26 printenv();
27 exit(0);
28 default: /* parent process */
29 //printenv();
30 exit(0);
31 }
32
33 }
```

运行此段代码，打印出了子进程的环境变量：

```
XDG_VTNR=7
XDG_SESSION_ID=c1
CLUTTER_IM_MODULE=xim
XDG_GREETER_DATA_DIR=/var/lib/lightdm-data/seed
SESSION=ubuntu
GIO_LAUNCHED_DESKTOP_FILE_PID=2282
GPG_AGENT_INFO=/home/seed/.gnupg/S.gpg-agent:0:1
SHELL=/bin/bash
DERBY_HOME=/usr/lib/jvm/java-8-oracle/db
QT_LINUX_ACCESSIBILITY_ALWAYS_ON=1
GNOME_KEYRING_CONTROL=
UPSTART_SESSION=unix:abstract=/com/ubuntu/upstart-session/1000/1244
GTK_MODULES=gail:atk-bridge:unity-gtk-module
USER=seed
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/sublime_text.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
QT_QPA_PLATFORMTHEME=appmenu-qt5
QT_IM_MODULE=ibus
XDG_SESSION_TYPE=x11
PWD=/home/seed/Downloads
JOB=unity-settings-daemon
JAVA_HOME=/usr/lib/jvm/java-8-oracle
XMODIFIERS=@im=ibus
GNOME_KEYRING_PID=
LANG=en_US.UTF-8
MANDATORY_PATH=/usr/share/gconf/ubuntu.mandatory.path
GDM_LANG=en_US
COMPIZ_CONFIG_PROFILE=ubuntu-lowgfx
IM_CONFIG_PHASE=1
GDMSESSION=ubuntu
SESSIONTYPE=gnome-session
GTK2_MODULES=overlay-scrollbar
HOME=/home/seed
SHLVL=1
XDG_SEAT=seat0
LANGUAGE=en_US
GNOME_DESKTOP_SESSION_ID=this-is-deprecated
LIBGL_ALWAYS_SOFTWARE=1
UPSTART_INSTANCE=
XDG_SESSION_DESKTOP=ubuntu
LOGNAME=seed
```

```
UPSTART_EVENTS=xsession started
COMPIZ_BIN_PATH=/usr/bin/
QT4_IM_MODULE=xim
XDG_DATA_DIRS=/usr/share/ubuntu:/usr/share/gnome:/usr/local/share/:/usr/share/:/var/lib/snapd/desktop
DBUS_SESSION_BUS_ADDRESS=unix:abstract=/tmp/dbus-nVwFgoZhKQ
J2SDKDIR=/usr/lib/jvm/java-8-oracle
INSTANCE=
UPSTART_JOB=unity7
DISPLAY=:0
XDG_RUNTIME_DIR=/run/user/1000
XDG_CURRENT_DESKTOP=Unity
J2REDIR=/usr/lib/jvm/java-8-oracle/jre
GTK_IM_MODULE=ibus
XAUTHORITY=/home/seed/.Xauthority
_=/home/seed/Downloads/task1m
[Finished in 0.1s]
```

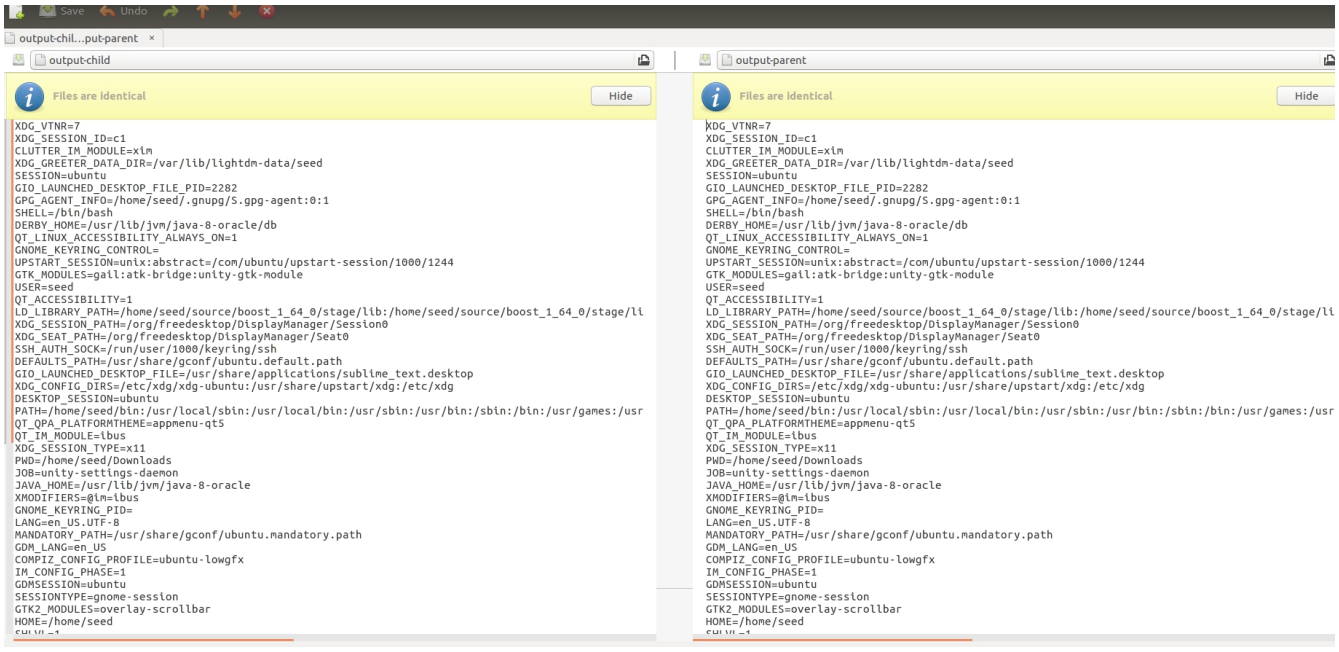
task1.c × task1m.c ×

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

extern char **environ;

void printenv()
{

int i = 0;
while (environ[i] != NULL)
{
printf("%s\n", environ[i]);
i++;
}

}
void main()
{

pid_t childPid;

switch(childPid = fork())
{
case 0: /* child process */
//printenv();
exit(0);
default: /* parent process */
printenv();
exit(0);
}

}
```

运行此段代码，打印出了父进程的环境变量：

```
XDG_VTNR=7
XDG_SESSION_ID=c1
CLUTTER_IM_MODULE=xim
XDG_GREETER_DATA_DIR=/var/lib/lightdm-data/seed
SESSION=ubuntu
GIO_LAUNCHED_DESKTOP_FILE_PID=2282
GPG_AGENT_INFO=/home/seed/.gnupg/S.gpg-agent:0:1
SHELL=/bin/bash
DERBY_HOME=/usr/lib/jvm/java-8-oracle/db
QT_LINUX_ACCESSIBILITY_ALWAYS_ON=1
GNOME_KEYRING_CONTROL=
UPSTART_SESSION=unix:abstract=/com/ubuntu/upstart-session/1000/1244
GTK_MODULES=gail:atk-bridge:unity-gtk-module
USER=seed
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/sublime_text.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
QT_QPA_PLATFORMTHEME=appmenu-qt5
QT_IM_MODULE=ibus
XDG_SESSION_TYPE=x11
PWD=/home/seed/Downloads
JOB=unity-settings-daemon
JAVA_HOME=/usr/lib/jvm/java-8-oracle
XMODIFIERS=@im=ibus
GNOME_KEYRING_PID=
LANG=en_US.UTF-8
MANDATORY_PATH=/usr/share/gconf/ubuntu.mandatory.path
GDM_LANG=en_US
COMPIZ_CONFIG_PROFILE=ubuntu-lowgfx
IM_CONFIG_PHASE=1
GDMSESSION=ubuntu
SESSIONTYPE=gnome-session
GTK2_MODULES=overlay-scrollbar
HOME=/home/seed
SHLVL=1
XDG_SEAT=seat0
LANGUAGE=en_US
GNOME_DESKTOP_SESSION_ID=this-is-deprecated
LIBGL_ALWAYS_SOFTWARE=1
UPSTART_INSTANCE=
XDG_SESSION_DESKTOP=ubuntu
LOGNAME=seed
UPSTART_EVENTS=xsession started
COMPIZ_BIN_PATH=/usr/bin/
QT4_IM_MODULE=xim
XDG_DATA_DIRS=/usr/share/ubuntu:/usr/share/gnome:/usr/local/share/:/usr/share/:/var/lib/snapd/desktop
DBUS_SESSION_BUS_ADDRESS=unix:abstract=/tmp/dbus-nVwFgoZhKQ
J2SDKDIR=/usr/lib/jvm/java-8-oracle
INSTANCE=
UPSTART_JOB=unity7
DISPLAY=:0
XDG_RUNTIME_DIR=/run/user/1000
XDG_CURRENT_DESKTOP=Unity
J2REDIR=/usr/lib/jvm/java-8-oracle/jre
GTK_IM_MODULE=ibus
XAUTHORITY=/home/seed/.Xauthority
_=/home/seed/Downloads/task1m
[Finished in 0.1s]
```

使用 meld 命令：meld output-child output-parent 对比发现父进程和子进程的环境变量完全一致，说明子进程从父进程继承了环境变量：



Task 3: Environment Variables and execve()

task2.c

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

extern char **environ;

int main()
{
char *argv[2];
argv[0] = "/usr/bin/env";
argv[1] = NULL;
execve("/usr/bin/env", argv, NULL);
return 0 ;
}
```

运行此段代码，无任何输出。

task2.c

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

extern char **environ;

int main()
{
char *argv[2];
argv[0] = "/usr/bin/env";
argv[1] = NULL;
execve("/usr/bin/env", argv, environ);
return 0 ;
}
```

将 12 行的 NULL 改为 environ 后再次执行，输出了当前所有的环境变量：

```
XDG_VTNR=7
XDG_SESSION_ID=c1
CLUTTER_IM_MODULE=xim
XDG_GREETER_DATA_DIR=/var/lib/lightdm-data/seed
SESSION=ubuntu
GIO_LAUNCHED_DESKTOP_FILE_PID=2282
GPG_AGENT_INFO=/home/seed/.gnupg/S.gpg-agent:0:1
SHELL=/bin/bash
DERBY_HOME=/usr/lib/jvm/java-8-oracle/db
QT_LINUX_ACCESSIBILITY_ALWAYS_ON=1
GNOME_KEYRING_CONTROL=
UPSTART_SESSION=unix:abstract=/com/ubuntu/upstart-session/1000/1244
GTK_MODULES=gail:atk-bridge:unity-gtk-module
USER=seed
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/sublime_text.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
QT_QPA_PLATFORMTHEME=appmenu-qt5
QT_IM_MODULE=ibus
XDG_SESSION_TYPE=x11
PWD=/home/seed/Downloads
JOB=unity-settings-daemon
JAVA_HOME=/usr/lib/jvm/java-8-oracle
XMODIFIERS=@im=ibus
GNOME_KEYRING_PID=
LANG=en_US.UTF-8
MANDATORY_PATH=/usr/share/gconf/ubuntu.mandatory.path
GDM_LANG=en_US
COMPIZ_CONFIG_PROFILE=ubuntu-lowgfx
IM_CONFIG_PHASE=1
GDMSESSION=ubuntu
SESSIONTYPE=gnome-session
GTK2_MODULES=overlay-scrollbar
HOME=/home/seed
SHLVL=1
XDG_SEAT=seat0
LANGUAGE=en_US
GNOME_DESKTOP_SESSION_ID=this-is-deprecated
LIBGL_ALWAYS_SOFTWARE=1
UPSTART_INSTANCE=
XDG_SESSION_DESKTOP=ubuntu
LOGNAME=seed

SHLVL=1
XDG_SEAT=seat0
LANGUAGE=en_US
GNOME_DESKTOP_SESSION_ID=this-is-deprecated
LIBGL_ALWAYS_SOFTWARE=1
UPSTART_INSTANCE=
XDG_SESSION_DESKTOP=ubuntu
LOGNAME=seed
UPSTART_EVENTS=xsession started
COMPIZ_BIN_PATH=/usr/bin/
QT4_IM_MODULE=xim
XDG_DATA_DIRS=/usr/share/ubuntu:/usr/share/gnome:/usr/local/share/:/usr/share/:/var/lib/snapd/desktop
DBUS_SESSION_BUS_ADDRESS=unix:abstract=/tmp/dbus-nVwFgoZhKQ
J2SDKDIR=/usr/lib/jvm/java-8-oracle
INSTANCE=
UPSTART_JOB=unity7
DISPLAY=:0
XDG_RUNTIME_DIR=/run/user/1000
XDG_CURRENT_DESKTOP=Unity
J2REDIR=/usr/lib/jvm/java-8-oracle/jre
GTK_IM_MODULE=ibus
XAUTHORITY=/home/seed/.Xauthority
_=/home/seed/Downloads/task2
[Finished in 0.1s]
```

environ 是一个指针变量，指向了包含所有环境变量的一个列表，新程序通过调用指针 environ 获取当前的环境变量。

Task 4: Environment Variables and system()

task4.c

```c
#include <stdio.h>
#include <stdlib.h>
int main()
{
system("/usr/bin/env");
return 0 ;
}
```

运行此段代码，通过系统调用获得了所有的环境变量：

```
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
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
DESKTOP_SESSION=ubuntu
GIO_LAUNCHED_DESKTOP_FILE=/usr/share/applications/sublime_text.desktop
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-nVwFgoZhKQ
GIO_LAUNCHED_DESKTOP_FILE_PID=2282
GNOME_KEYRING_CONTROL=
QT_QPA_PLATFORMTHEME=appmenu-qt5
MANDATORY_PATH=/usr/share/gconf/ubuntu.mandatory.path
IM_CONFIG_PHASE=1
SESSIONTYPE=gnome-session
UPSTART_JOB=unity7
LOGNAME=seed
GTK_IM_MODULE=ibus
_=/home/seed/Downloads/task4
DEFAULTS_PATH=/usr/share/gconf/ubuntu.default.path
XDG_SESSION_ID=c1
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
DERBY_HOME=/usr/lib/jvm/java-8-oracle/db
GDM_LANG=en_US
XDG_SESSION_PATH=/org/freedesktop/DisplayManager/Session0
XDG_RUNTIME_DIR=/run/user/1000
COMPIZ_BIN_PATH=/usr/bin/
DISPLAY=:0
LANG=en_US.UTF-8
XDG_CURRENT_DESKTOP=Unity
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
UPSTART_EVENTS=xsession started
GPG_AGENT_INFO=/home/seed/.gnupg/S.gpg-agent:0:1
UPSTART_SESSION=unix:abstract=/com/ubuntu/upstart-session/1000/1244
XDG_VTNR=7
QT_IM_MODULE=ibus
PWD=/home/seed/Downloads
JAVA_HOME=/usr/lib/jvm/java-8-oracle
CLUTTER_IM_MODULE=xim
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
JOB=unity-settings-daemon
[Finished in 0.1s]
```

Task 5: Environment Variable and Set-UID Programs

在账户为 seed 时，打印出环境变量
PATH 和 LD_LIBRARY_PATH:

```
declare -x 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/se
ed/android/android-ndk/android-ndk-r8d:/home/seed/.local/bin"
```

```
declare -x LD_LIBRARY_PATH="/home/seed/source/boost_1_64_0/stage/lib:/home/seed/source/boost_1_64_0/stage/lib:"
```

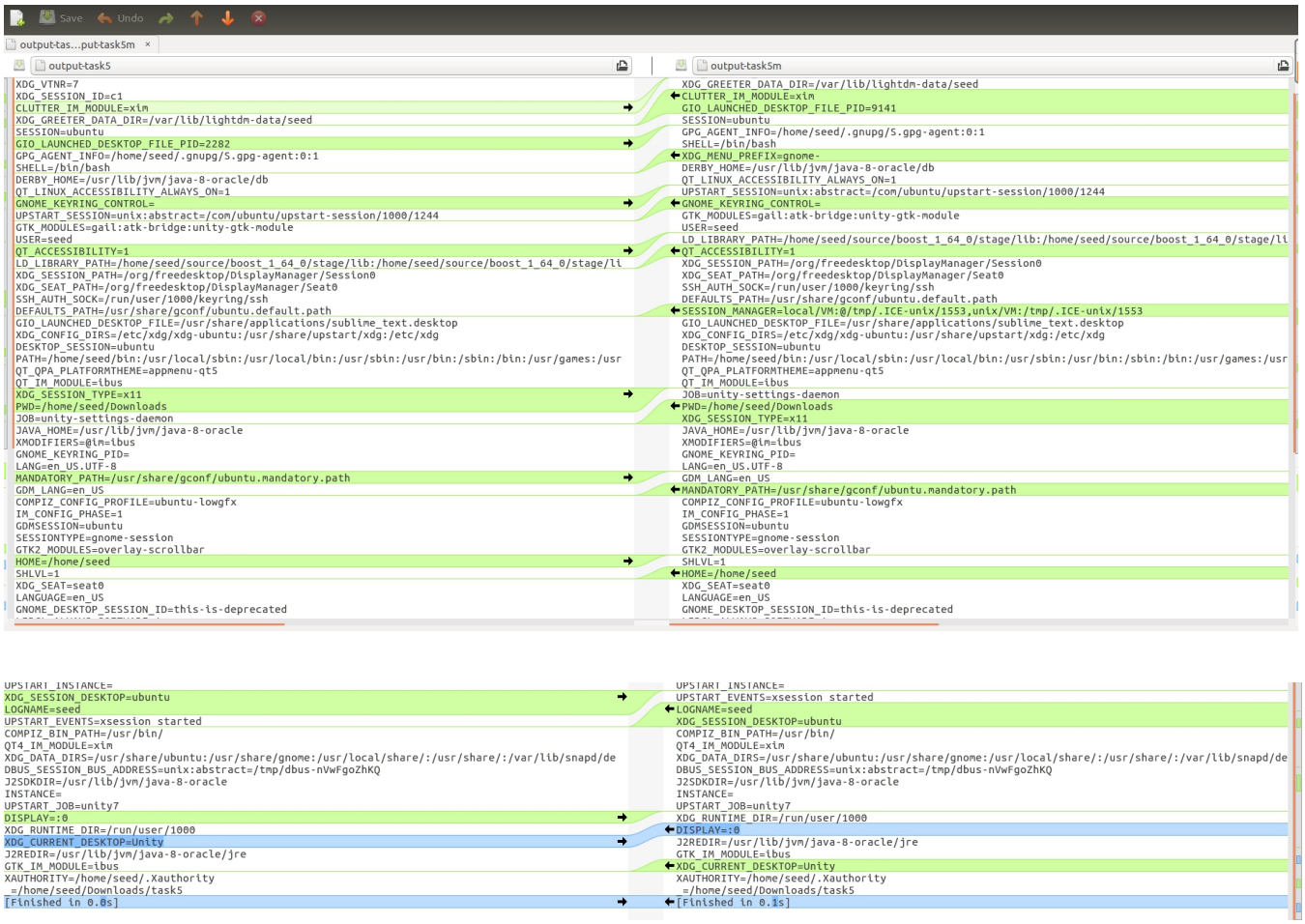
untitled task5.c

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

extern char **environ;

void main()
{
int i = 0;
while (environ[i] != NULL)
{
printf("%s\n", environ[i]);
i++;
} }
```

对于上述程序，改变拥有者为 root，设置成一个 SET_UID 程序：

```
[03/24/21]seed@VM:~$ sudo chown root task5
[03/24/21]seed@VM:~$ sudo chmod 4755 task5
```

运行 SET_UID 程序，输出的环境变量发生了变化，说明所有的环境变量都进入了子进程 SET_UID 程序里。



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

task6.c

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


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

对于上述程序，将其设置为 SET_UID 程序：

```
[03/24/21]seed@VM:~$ sudo chown root task6
```

```
[03/24/21]seed@VM:~$ sudo chmod 4755 task6
```

Can you let this Set-UID program run your code instead of /bin/ls? If you can, is your code running with the root privilege?

可以具有 root 权限，把/bin/sh 拷贝到/tmp 目录下面重命名为 ls（已将/bin/目录下的 sh 符号链接到 zsh），将环境变量 PATH 设置为当前目录/tmp，运行编译的程序 test。就可以获得 root 权限：

```
root@VM:/home/seed# cp /bin/sh /tmp/ls
```

```
root@VM:/home/seed#  export PATH=/tmp:$PATH
```

task6.c | test.c | task5.c

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


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

```
config-err-NBd9nB
ls
orbit-seed
systemd-private-7cc21b5a630b4a3cb7cf424d893964b5-colord.service-fhFbYD
systemd-private-7cc21b5a630b4a3cb7cf424d893964b5-rtkit-daemon.service-dJCF6O
Temp-745010b2-389c-4369-918b-1f541c1c5f84
test
test.c
unity_support_test.1
[Finished in 0.1s]
```

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

将上述程序设置为 SET_UID 程序：

```
[03/24/21]seed@VM:~$ sudo chown root task8
[03/24/21]seed@VM:~$ sudo chmod 4755 task8
```

If you were Bob, can you compromise the integrity of the system? For example, can you remove a file that is not writable to you?

可以破坏系统完整性，因为使用了 system（），可以修改 PATH 的值，使他指向自己所编写的程序，从而达到删除程序的目的。

将 system（command）注释掉，使用 execve（）

task8.c

```c
#include <string.h>
#include <stdio.h>
#include <stdlib.h>
#include <unistd.h>

int main(int argc, char *argv[])
{
char *v[3];
char *command;
if(argc < 2) {
printf("Please type a file name.\n");
return 1;
}

v[0] = "/bin/cat";
v[1] = argv[1];
 v[2] = NULL;

command = malloc(strlen(v[0]) + strlen(v[1]) + 2);
sprintf(command, "%s %s", v[0], v[1]);
// Use only one of the followings.
//system(command);
execve(v[0], v, NULL);
return 0 ;
}
```

不会再出现上述的问题，因为 execve（）不会使用 PTAH 环境变量。