Design of Secure Computer Systems

Lab 05

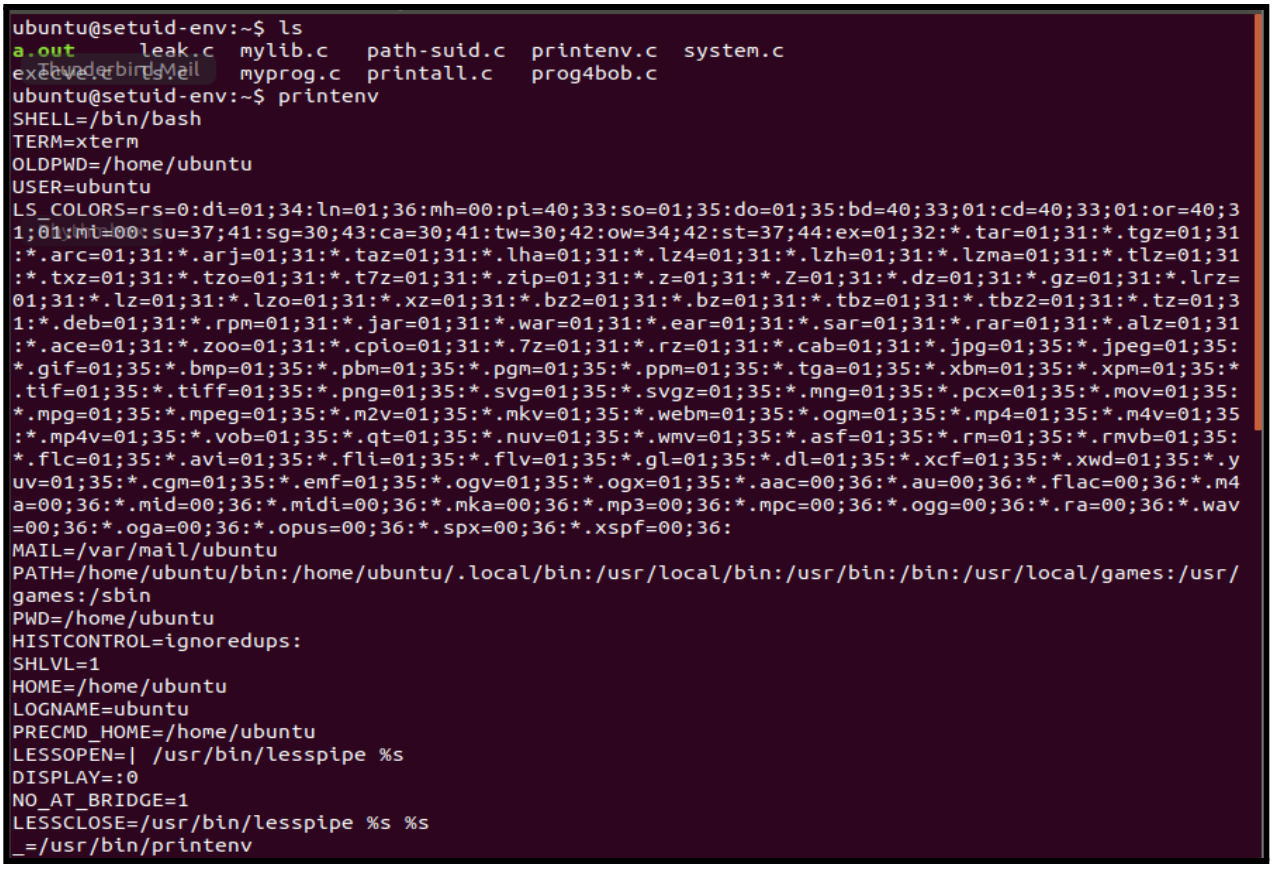
Setuid-env

The learning objective of this lab is to understand how environmental variables affect program and system behavior.

Name: Rakshita Mathur

Task 1: Manipulating environment variables

Using printenv or env command to print out the environment variables. Used export and unset to set or unset environment variables



```
ubuntu@setuid-env:~$ printenv |grep -i PWD
OLDPWD=/home/ubuntu
PWD=/home/ubuntu
ubuntu@setuid-env:~$ export NEWVARIABLE=2
ubuntu@setuid-env:~$ echo $NEWVARIABLE 2
2 2
ubuntu@setuid-env:~$ printenv
SHELL=/bin/bash
TERM=xterm
OLDPWD=/home/ubuntu
NEWVARIABLE=2
USER=ubuntu
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;3
1;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;3
1:*.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:*.y
uv=01;35:*.cgm=01;35:*.emf=01;35:*.ogv=01;35:*.ogx=01;35:*.aac=00;36:*.au=00;36:*.flac=00;36:*.m4
a=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:
MAIL=/var/mail/ubuntu
PATH=/home/ubuntu/bin:/home/ubuntu/.local/bin:/usr/local/bin:/usr/bin:/bin:/usr/local/games:/usr/
games:/sbin
PWD=/home/ubuntu
HISTCONTROL=ignoredups:
SHLVL=1
HOME=/home/ubuntu
LOGNAME=ubuntu
PRECMD_HOME=/home/ubuntu
LESSOPEN=| /usr/bin/lesspipe %s
DISPLAY=:0
NO_AT_BRIDGE=1
LESSCLOSE=/usr/bin/lesspipe %s %s
_=/usr/bin/printenv
ubuntu@setuid-env:~$ echo $NEWVARIABLE
2
```

```
ubuntu@setuid-env:~$ unset NEWVARIABLE
ubuntu@setuid-env:~$ printenv
SHELL=/bin/bash
TERM=xterm
OLDPWD=/home/ubuntu
USER=ubuntu
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;3
1;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;3
1:*.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:*.y
uv=01;35:*.cgm=01;35:*.emf=01;35:*.ogv=01;35:*.ogx=01;35:*.aac=00;36:*.au=00;36:*.flac=00;36:*.m4
a=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:
MAIL=/var/mail/ubuntu
PATH=/home/ubuntu/bin:/home/ubuntu/.local/bin:/usr/local/bin:/usr/bin:/bin:/usr/local/games:/usr/
games:/sbin
PWD=/home/ubuntu
HISTCONTROL=ignoredups:
SHLVL=1
HOME=/home/ubuntu
LOGNAME=ubuntu
PRECMD_HOME=/home/ubuntu
LESSOPEN=| /usr/bin/lesspipe %s
DISPLAY=:0
NO_AT_BRIDGE=1
LESSCLOSE=/usr/bin/lesspipe %s %s
_=/usr/bin/printenv
ubuntu@setuid-env:~$ echo $NEWVARIABLE

ubuntu@setuid-env:~$
```

Task 2: Inheriting environment variables from parents

Compiling and runingthe printenv.c program.

```
ubuntu@setuid-env:~$ cat printenv.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);
   }
}
ubuntu@setuid-env:~$ gccc printenv.c -o printenv
-su: gccc: command not found
ubuntu@setuid-env:~$ gcc printenv.c -o printenv
ubuntu@setuid-env:~$ ls
a.out     leak.c  mylib.c   path-suid.c  printenv    prog4bob.c
execve.c  ls.c    myprog.c  printall.c   printenv.c  system.c
ubuntu@setuid-env:~$ ./printenv
ubuntu@setuid-env:~$ ./printenv >child
ubuntu@setuid-env:~$ ls
a.out  execve.c  ls.c     myprog.c     printall.c  printenv.c  system.c
child  leak.c    mylib.c  path-suid.c  printenv    prog4bob.c
```

Commenting out the printenv() statement in the child process case, and uncomment the printenv() statement in the parent process case. Compile and run the code, and describe your observation. Save the output in another file

On comparing the difference of these two files using the diff command. We observed that child and parent are different.

```
ubuntu@setuid-env:~$ cat printenv.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);
   }
}
ubuntu@setuid-env:~$ nano printenv.c
ubuntu@setuid-env:~$ gcc printenv.c -o parent
ubuntu@setuid-env:~$ ls
a.out  execve.c  ls.c     myprog.c  path-suid.c  printenv    prog4bob.c
child  leak.c    mylib.c  parent    printall.c   printenv.c  system.c
ubuntu@setuid-env:~$ diff child parent
Binary files child and parent differ
ubuntu@setuid-env:~$
```

Task 3: Environment variables and execve()

Compiling and run the execve.c program.

```
ubuntu@setuid-env:~$ cat execve.c
#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);
   return 0 ;
}
ubuntu@setuid-env:~$ gcc execve.c -o execve1
execve.c: In function 'main':
execve.c:9:4: warning: implicit declaration of function 'execve' [-Wimplicit-function-declaration
]
    execve("/usr/bin/env", argv, NULL);
    ^
```

changed the invocation of execve() to the following execve("/usr/bin/env", argv, environ); , changed the invocation of execve() to the following, execve("/usr/bin/env", argv, environ)

```
 GNU nano 2.5.3                    File: execve.c

#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, environ);
   return 0 ;
}
```

```
ubuntu@setuid-env:~$ nano execve.c
ubuntu@setuid-env:~$ gcc execve.c -o execve2
execve.c: In function 'main':
execve.c:9:4: warning: implicit declaration of function 'execve' [-Wimplicit-function-declaration
]
    execve("/usr/bin/env", argv, environ);
    ^
ubuntu@setuid-env:~$ ./execve2
TERM=xterm
SHELL=/bin/bash
USER=ubuntu
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;3
1;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;3
1:*.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:*.y
uv=01;35:*.cgm=01;35:*.emf=01;35:*.ogv=01;35:*.ogx=01;35:*.aac=00;36:*.au=00;36:*.flac=00;36:*.m4
a=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:
PATH=/home/ubuntu/bin:/home/ubuntu/.local/bin:/usr/local/bin:/usr/bin:/bin:/usr/local/games:/usr/
games:/sbin
MAIL=/var/mail/ubuntu
PWD=/home/ubuntu
HISTCONTROL=ignoredups:
HOME=/home/ubuntu
SHLVL=2
LOGNAME=ubuntu
PRECMD_HOME=/home/ubuntu
LESSOPEN=| /usr/bin/lesspipe %s
DISPLAY=:0
LESSCLOSE=/usr/bin/lesspipe %s %s
NO_AT_BRIDGE=1
_=./execve2
ubuntu@setuid-env:~$ ./execve1
```

Task 4: Environment variables and system()

We look at the implementation of the system() function, we saw that it uses execl() to execute /bin/sh; excel() calls execve(), passing to it the environment variables array. Therefore, using system(), the environment variables of the calling process are passed to the new program /bin/sh.]

```
ubuntu@setuid-env:~$ cat system.c
#include <stdio.h>
#include <stdlib.h>
int main()
{
    system("/usr/bin/env");
    return 0 ;
}
ubuntu@setuid-env:~$ gcc system.c -o system
ubuntu@setuid-env:~$ ls
a.out  execve.c  execve2  ls.c     myprog.c  path-suid.c  printenv    prog4bob.c  system.c
child  execve1   leak.c   mylib.c  parent    printall.c   printenv.c  system
```

```
ubuntu@setuid-env:~$ ./system
LESSOPEN=| /usr/bin/lesspipe %s
MAIL=/var/mail/ubuntu
USER=ubuntu
SHLVL=2
HOME=/home/ubuntu
PRECMD_HOME=/home/ubuntu
LOGNAME=ubuntu
_=./system
TERM=xterm
HISTCONTROL=ignoredups:
PATH=/home/ubuntu/bin:/home/ubuntu/.local/bin:/usr/local/bin:/usr/bin:/bin:/usr/local/games:/usr/
games:/sbin
DISPLAY=:0
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;3
1;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;3
1:*.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:*.y
uv=01;35:*.cgm=01;35:*.emf=01;35:*.ogv=01;35:*.ogx=01;35:*.aac=00;36:*.au=00;36:*.flac=00;36:*.m4
a=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:
SHELL=/bin/bash
NO_AT_BRIDGE=1
LESSCLOSE=/usr/bin/lesspipe %s %s
PWD=/home/ubuntu
ubuntu@setuid-env:~$ export ENVX2="Test"
ubuntu@setuid-env:~$ ./system | grep ENVX2
ENVX2=Test
```

Task 5: Environmental Variable and Set-UID program

Set-UID is an important security mechanism in Unix operating systems. When a Set-UID program runs, it assumes the owner's privileges.

Compiling the printall.c program, change its ownership to root, and make it a Set-UID program.

sudo chown root:root a.out , sudo chmod a+s a.out

```
ubuntu@setuid-env:~$ gcc printenv.c -o step5.1
ubuntu@setuid-env:~$ nano printenv.c
ubuntu@setuid-env:~$ gcc printenv.c -o step5.2
ubuntu@setuid-env:~$ ./step5.1
TERM=xterm
SHELL=/bin/bash
ENVX2=Test
USER=ubuntu
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:
did_pipe=NO
PATH=/home/ubuntu/bin:/home/ubuntu/.local/bin:/usr/local/bin:/usr/bin:/bin:/usr/local/games:/usr/games:/sbin
MAIL=/var/mail/ubuntu
PWD=/home/ubuntu
HISTCONTROL=ignoredups:
HOME=/home/ubuntu
SHLVL=2
LOGNAME=ubuntu
PRECMD_HOME=/home/ubuntu
LESSOPEN=| /usr/bin/lesspipe %s
DISPLAY=:0
LESSCLOSE=/usr/bin/lesspipe %s %s
NO_AT_BRIDGE=1
_=./step5.1
```

Task6: The system() function and set-UID program

One of many changes made to the setuid feature over the years relates to its interaction with the system() function. Since the results of system() are dependent on environment variables, it was a source of increased risk.

export PATH=˜/:$PATH would cause the shell to first look in your home directory for a program of a given name.

```
ubuntu@setuid-env:~$ cat path-suid.c
#include <stdlib.h>
#include <stdio.h>
#include <unistd.h>
#include <sys/types.h>
int main()
{
   uid_t euid = geteuid();
   printf("euid is %d\n", euid);
   system("ls");
   return 0;
}
ubuntu@setuid-env:~$ export PATH=/:$PATH
ubuntu@setuid-env:~$ gcc path-suid.c -o pathsuid
ubuntu@setuid-env:~$ sudi chown root:root pathsuid
-su: sudi: command not found
ubuntu@setuid-env:~$ sudo chown root:root pathsuid
ubuntu@setuid-env:~$ sudo chmod a+s pathsuid
ubuntu@setuid-env:~$ sudo chmod 4755 pathsuid
ubuntu@setuid-env:~$ ls -l pathsuid
-rwsr-xr-x 1 root root 8712 Oct 18 00:09 pathsuid
ubuntu@setuid-env:~$ ./pathsuid
euid is 0
a.out     execve1  ls.c      parent       printall    printenv.c  step5.2
child     execve2  mylib.c   path-suid.c  printall.c  prog4bob.c  system
execve.c  leak.c   myprog.c  pathsuid     printenv    step5.1     system.c
ubuntu@setuid-env:~$ export PATH=.:$PATH
ubuntu@setuid-env:~$ echo PATH
PATH
ubuntu@setuid-env:~$ echo $PATH
.:/:/home/ubuntu/bin:/home/ubuntu/.local/bin:/usr/local/bin:/usr/bin:/bin:/usr/local/games:/usr/g
ames:/sbin
ubuntu@setuid-env:~$ ./pathsuid
euid is 0
a.out     execve1  ls.c      parent       printall    printenv.c  step5.2
child     execve2  mylib.c   path-suid.c  printall.c  prog4bob.c  system
execve.c  leak.c   myprog.c  pathsuid     printenv    step5.1     system.c
ubuntu@setuid-env:~$ ls -l pathsuid
-rwsr-xr-x 1 root root 8712 Oct 18 00:09 pathsuid
ubuntu@setuid-env:~$ export PATH=.:$PATH
ubuntu@setuid-env:~$ echo :PATH
:PATH
ubuntu@setuid-env:~$ export PATH=.:PATH
ubuntu@setuid-env:~$ echo :PATH
-su: date: command not found
-su: basename: command not found
```

```
ubuntu@setuid-env:~$ ls -l pathsuid
-rwsr-xr-x 1 root root 8712 Oct 18 00:09 pathsuid
ubuntu@setuid-env:~$ export PATH=.:$PATH
ubuntu@setuid-env:~$ echo :PATH
:PATH
ubuntu@setuid-env:~$ export PATH=.:PATH
ubuntu@setuid-env:~$ echo :PATH
-su: date: command not found
-su: basename: command not found
:PATH
ubuntu@setuid-env:~$ ls
-su: date: command not found
-su: basename: command not found
-su: ls: command not found
ubuntu@setuid-env:~$ ./pathsuid
-su: date: command not found
-su: basename: command not found
euid is 0
sh: 1: ls: not found
ubuntu@setuid-env:~$ cat path-suid.c
-su: date: command not found
-su: basename: command not found
-su: cat: command not found
ubuntu@setuid-env:~$
```

Task 7: The LD_PRELOAD environmental variable and SET-UID Programs

```
ubuntu@setuid-env:~$ ls
a.out     execve1  ls.c      parent       printall    printenv.c  step5.2
child     execve2  mylib.c   path-suid.c  printall.c  prog4bob.c  system
execve.c  leak.c   myprog.c  pathsuid     printenv    step5.1     system.c
ubuntu@setuid-env:~$ cat mylib.c
#include <stdio.h>
void sleep (int s)
{
   /* If this is invoked by a privileged program, you can do damage here!  */
   printf("I am not sleeping!\n");
}
```

```
ubuntu@setuid-env:~$ gcc -fPIC -g -c mylib.c
ubuntu@setuid-env:~$ gcc -shared -o libmylib.so.1.0.1 mylib.o -lc
ubuntu@setuid-env:~$ export LD_PRELOAD=./libmylib.so.1.0.1
ubuntu@setuid-env:~$ cat myprog.c
#include <unistd.h>
/* myprog.c */
int main()
{
    sleep(1);
    return 0;
}
ubuntu@setuid-env:~$ gcc myprog.c -o myprog
ubuntu@setuid-env:~$ ./myprog
I am not sleeping!
ubuntu@setuid-env:~$ sudo chown root myprog
ubuntu@setuid-env:~$ sudo chmod 4755 myprog
ubuntu@setuid-env:~$ ls -l
total 80
-rwxrwxr-x 1 ubuntu ubuntu 8736 Feb  7  2018 a.out
-rw-rw-r-- 1 ubuntu ubuntu  198 Feb  7  2018 execve.c
-rw-rw-r-- 1 ubuntu ubuntu 1058 Feb  7  2018 leak.c
-rwxrwxr-x 1 ubuntu ubuntu 9160 Oct 14 21:18 libmylib.so.1.0.1
-rw-rw-r-- 1 ubuntu ubuntu  164 Feb  7  2018 ls.c
-rw-rw-r-- 1 ubuntu ubuntu  155 Jan  9  2018 mylib.c
-rw-rw-r-- 1 ubuntu ubuntu 3312 Oct 14 21:18 mylib.o
-rwsr-xr-x 1 root   ubuntu 8608 Oct 14 21:20 myprog
-rw-rw-r-- 1 ubuntu ubuntu   78 Feb  7  2018 myprog.c
-rw-rw-r-- 1 ubuntu ubuntu  187 Feb  7  2018 path-suid.c
-rw-rw-r-- 1 ubuntu ubuntu  175 Jan  9  2018 printall.c
-rw-rw-r-- 1 ubuntu ubuntu  422 Jan  9  2018 printenv.c
-rw-rw-r-- 1 ubuntu ubuntu  463 Jan  9  2018 prog4bob.c
-rw-rw-r-- 1 ubuntu ubuntu   97 Jan  9  2018 system.c
ubuntu@setuid-env:~$ ./myprog
ubuntu@setuid-env:~$ pwd
/home/ubuntu
```

```
ubuntu@setuid-env:~$ ./myprog
ubuntu@setuid-env:~$ pwd
/home/ubuntu
ubuntu@setuid-env:~$ sudo su -
root@setuid-env:~# cd /home/ubuntu
root@setuid-env:/home/ubuntu# ./myprog
root@setuid-env:/home/ubuntu# export LD_PRELOAD=./libmylib.so.1.0.1
root@setuid-env:/home/ubuntu# ./myprog
I am not sleeping!
root@setuid-env:/home/ubuntu# logout
ubuntu@setuid-env:~$
```

• Made myprog a regular program, and run it as a normal user.
• Made myprog a Set-UID root program, and run it as a normal user.
• Become root with sudo su, export the LD PRELOAD environment variable again and run the myprog program again.
• Made myprog a Set-UID user1 program (i.e., the owner is user1, which is another user account), export the LD PRELOAD environment variable again as the user1 user and run it.

```
ubuntu@setuid-env:~$ cp myprog myprog1
ubuntu@setuid-env:~$ ls -l
total 92
-rwxrwxr-x 1 ubuntu ubuntu 8736 Feb  7  2018 a.out
-rw-rw-r-- 1 ubuntu ubuntu  198 Feb  7  2018 execve.c
-rw-rw-r-- 1 ubuntu ubuntu 1058 Feb  7  2018 leak.c
-rwxrwxr-x 1 ubuntu ubuntu 9160 Oct 14 21:18 libmylib.so.1.0.1
-rw-rw-r-- 1 ubuntu ubuntu  164 Feb  7  2018 ls.c
-rw-rw-r-- 1 ubuntu ubuntu  155 Jan  9  2018 mylib.c
-rw-rw-r-- 1 ubuntu ubuntu 3312 Oct 14 21:18 mylib.o
-rwsr-xr-x 1 root   ubuntu 8608 Oct 14 21:20 myprog
-rw-rw-r-- 1 ubuntu ubuntu   78 Feb  7  2018 myprog.c
-rwxr-xr-x 1 ubuntu ubuntu 8608 Oct 14 21:26 myprog1
-rw-rw-r-- 1 ubuntu ubuntu  187 Feb  7  2018 path-suid.c
-rw-rw-r-- 1 ubuntu ubuntu  175 Jan  9  2018 printall.c
-rw-rw-r-- 1 ubuntu ubuntu  422 Jan  9  2018 printenv.c
-rw-rw-r-- 1 ubuntu ubuntu  463 Jan  9  2018 prog4bob.c
-rw-rw-r-- 1 ubuntu ubuntu   97 Jan  9  2018 system.c
ubuntu@setuid-env:~$ sudo chown user1 myprog1
ubuntu@setuid-env:~$ ls -l myprog1
-rwxr-xr-x 1 user1 ubuntu 8608 Oct 14 21:26 myprog1
ubuntu@setuid-env:~$ ./myprog1
I am not sleeping!
```

Task8: Capability Leaking

The setuid() system call can be used to revoke the privileges. According to the manual, “setuid() sets the effective user ID of the calling process. If the effective UID of the caller is root, the real UID and saved set-user-ID are also set”. Therefore, if a Set-UID program with effective UID 0 calls setuid(n), the process will become a normal process, with all its UIDs being set to n.

```
ubuntu@setuid-env:~$ cat leak.c
#include <stdio.h>
#include <stdlib.h>
#include <unistd.h>
#include <sys/types.h>
#include <fcntl.h>
void main()
{
   int fd;
   /* Assume that /etc/zzz is an important system file,
    *   and it is owned by root with permission 0644.
    *   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 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);
   }
}
ubuntu@setuid-env:~$ gcc leak.c -o leak
ubuntu@setuid-env:~$ ls
a.out  execve.c  leak  leak.c  libmylib.so.1.0.1  ls.c  mylib.c  mylib.o  myprog  myprog.c  myprog1  path-suid.c  printall.c  printenv.c  prog4bob.c  system.c
ubuntu@setuid-env:~$ ls -l leak
-rwxrwxr-x 1 ubuntu ubuntu 9008 Oct 14 21:31 leak
```

```
ubuntu@setuid-env:~$ sudo chown root leak
ubuntu@setuid-env:~$ sudo chmod 4755 invoke
chmod: cannot access 'invoke': No such file or directory
ubuntu@setuid-env:~$ sudo chmod 4755 leak
ubuntu@setuid-env:~$ ls -l leak
-rwsr-xr-x 1 root ubuntu 9008 Oct 14 21:31 leak
ubuntu@setuid-env:~$ sudo touch /etc/zzz
ubuntu@setuid-env:~$ ls -l /etc/zzz
-rw-rw-r-- 1 root root 29 Oct 14 21:32 /etc/zzz
ubuntu@setuid-env:~$ cat /etc/zzz
important stuff, not really.
```

```
ubuntu@setuid-env:~$ echo "I Want To Write Something" >/etc/zzz
-su: /etc/zzz: Permission denied
ubuntu@setuid-env:~$
```

```
ubuntu@setuid-env:~$ ./leak
ubuntu@setuid-env:~$ gcc leak.c -o leak
ubuntu@setuid-env:~$ ./leak
Cannot open /etc/zzz
ubuntu@setuid-env:~$ sudo chown root leak
ubuntu@setuid-env:~$ sudo chmod 4755 leak
ubuntu@setuid-env:~$ ls -l
total 104
-rwxrwxr-x 1 ubuntu ubuntu 8736 Feb  7  2018 a.out
-rw-rw-r-- 1 ubuntu ubuntu  198 Feb  7  2018 execve.c
-rwsr-xr-x 1 root   ubuntu 9008 Oct 14 21:35 leak
-rw-rw-r-- 1 ubuntu ubuntu 1058 Feb  7  2018 leak.c
-rwxrwxr-x 1 ubuntu ubuntu 9160 Oct 14 21:18 libmylib.so.1.0.1
-rw-rw-r-- 1 ubuntu ubuntu  164 Feb  7  2018 ls.c
-rw-rw-r-- 1 ubuntu ubuntu  155 Jan  9  2018 mylib.c
-rw-rw-r-- 1 ubuntu ubuntu 3312 Oct 14 21:18 mylib.o
-rwsr-xr-x 1 root   ubuntu 8608 Oct 14 21:20 myprog
-rw-rw-r-- 1 ubuntu ubuntu   78 Feb  7  2018 myprog.c
-rwxr-xr-x 1 user1  ubuntu 8608 Oct 14 21:26 myprog1
-rw-rw-r-- 1 ubuntu ubuntu  187 Feb  7  2018 path-suid.c
-rw-rw-r-- 1 ubuntu ubuntu  175 Jan  9  2018 printall.c
-rw-rw-r-- 1 ubuntu ubuntu  422 Jan  9  2018 printenv.c
-rw-rw-r-- 1 ubuntu ubuntu  463 Jan  9  2018 prog4bob.c
-rw-rw-r-- 1 ubuntu ubuntu   97 Jan  9  2018 system.c
ubuntu@setuid-env:~$
```

```
ubuntu@setuid-env:~$ ./leak
ubuntu@setuid-env:~$ cat /etc/zzz
important stuff, not really.
ubuntu@setuid-env:~$ ./leak
ubuntu@setuid-env:~$ gcc leak.c -o leak1
ubuntu@setuid-env:~$ ./leak1
Cannot open /etc/zzz
ubuntu@setuid-env:~$ sudo chown root leak1
ubuntu@setuid-env:~$ sudo chmod 4755 leak
ubuntu@setuid-env:~$ sudo chmod 4755 leak1
ubuntu@setuid-env:~$ ls -l
total 116
-rwxrwxr-x 1 ubuntu ubuntu 8736 Feb  7  2018 a.out
-rw-rw-r-- 1 ubuntu ubuntu  198 Feb  7  2018 execve.c
-rwsr-xr-x 1 root   ubuntu 9008 Oct 14 21:35 leak
-rw-rw-r-- 1 ubuntu ubuntu 1058 Feb  7  2018 leak.c
-rwsr-xr-x 1 root   ubuntu 9008 Oct 14 21:38 leak1
-rwxrwxr-x 1 ubuntu ubuntu 9160 Oct 14 21:18 libmylib.so.1.0.1
-rw-rw-r-- 1 ubuntu ubuntu  164 Feb  7  2018 ls.c
-rw-rw-r-- 1 ubuntu ubuntu  155 Jan  9  2018 mylib.c
-rw-rw-r-- 1 ubuntu ubuntu 3312 Oct 14 21:18 mylib.o
-rwsr-xr-x 1 root   ubuntu 8608 Oct 14 21:20 myprog
-rw-rw-r-- 1 ubuntu ubuntu   78 Feb  7  2018 myprog.c
-rwxr-xr-x 1 user1  ubuntu 8608 Oct 14 21:26 myprog1
-rw-rw-r-- 1 ubuntu ubuntu  187 Feb  7  2018 path-suid.c
-rw-rw-r-- 1 ubuntu ubuntu  175 Jan  9  2018 printall.c
-rw-rw-r-- 1 ubuntu ubuntu  422 Jan  9  2018 printenv.c
-rw-rw-r-- 1 ubuntu ubuntu  463 Jan  9  2018 prog4bob.c
-rw-rw-r-- 1 ubuntu ubuntu   97 Jan  9  2018 system.c
ubuntu@setuid-env:~$ ./leak1
```

Used stoplab command to stop the lab.
