

CSCI 476: Computer Security

Lecture 6: Set-UID and Environment Variables (Part 3)

Reese Pearsall
Spring 2023

Set-UID In a Nutshell


Set-UID allows a user to run a program with the program owner's privilege

- User runs a program w/ temporarily elevated privileges

Created to deal with inflexibilities of UNIX access control

Example: The **passwd** program

```
[seed@VM][~]$ ls -al /usr/bin/passwd  
-rwsr-xr-x 1 root root 68208 May 28 2020 /usr/bin/passwd
```



RUID vs EUID

Real User ID (RUID) and **Effective User ID (EUID)** are values that are tracked by OS for each process. These IDs are used for access control decisions

ex. Should this process be allowed to do _____ ?

RUID refers to the user that created the process

ex. A normal user running `./hello_world`, the RUID == seed

EUID refers to the current privilege of the process, and is used for most permission checks

ex. A normal user running `./hello_world`, the EUID == seed

RUID vs EUID

RUID refers to the user that created the process

EUID refers to the current privilege of the process, and is used for most permission checks

When running a process, generally RUID and EUID will be the same

However, when the process is a Set UID program, the EUID now becomes the owner of the program, which will typically be **root** (now RUID != EUID)

RUID vs EUID

RUID refers to the user that created the process

EUID refers to the current privilege of the process, and is used for most permission checks

However, when the process is a Set UID program, the EUID now becomes the owner of the program, which will typically be **root** (now RUID != EUID)

There are shell countermeasures (`/bin/dash`) that prevents a process from doing things when it detects that the RUID != EUID, which is why we must disable the countermeasure before starting the lab

```
sudo ln -sf /bin/zsh /bin/sh
```

```
./audit "my_info.txt; /bin/sh"
```



```
system (/bin/cat my_info.txt; /bin/sh)
```

```
[09/15/22]seed@VM:~/lab2$ ./audit "my_info.txt; /bin/sh"  
I have some information  
#
```

`system()` interprets this as *two separate* commands

Environment variable are a set of dynamic named values that affect the way a running process will behave

(key-value pairs)

Example: The `PATH` variable

- We use command such as `ls` and `passwd`

We could be in any directory.

How does it know to run `/bin/ls` ?

If the full path is not provided, the shell process will use the `PATH` env. variable to search for it!

```
PATH=/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin:/usr/games:/usr/local/games:/snap/bin:.
```

Tells the OS to look for the `ls` program in `/usr/local/bin`

Exploiting a Set-UID program with environment variables

(Task 5 on lab 1)

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

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

This program uses the `system()` command to run the `ls` program

However, this program does *not* use the absolute path of the `ls` program (`/bin/ls`)

... which means it will use the `PATH` environment variable to locate the `ls` program

Important reminder: We can set the value of the `PATH` env variable



Linking finds the external library code referenced in a program

Static Linking – Linker combines program code/external code into final executable

Dynamic Linking- linker uses env variables to locate external dependencies

This program uses the `sleep` function. When compiling this program, how does it know where to find the source code for the `sleep()` function ?

```
// Demo program that calls sleep.
#include <unistd.h>

int main(void)
{
    sleep(1);
    return 0;
}
```

Linking finds the external library code referenced in a program

Static Linking – Linker combines program code/external code into final executable

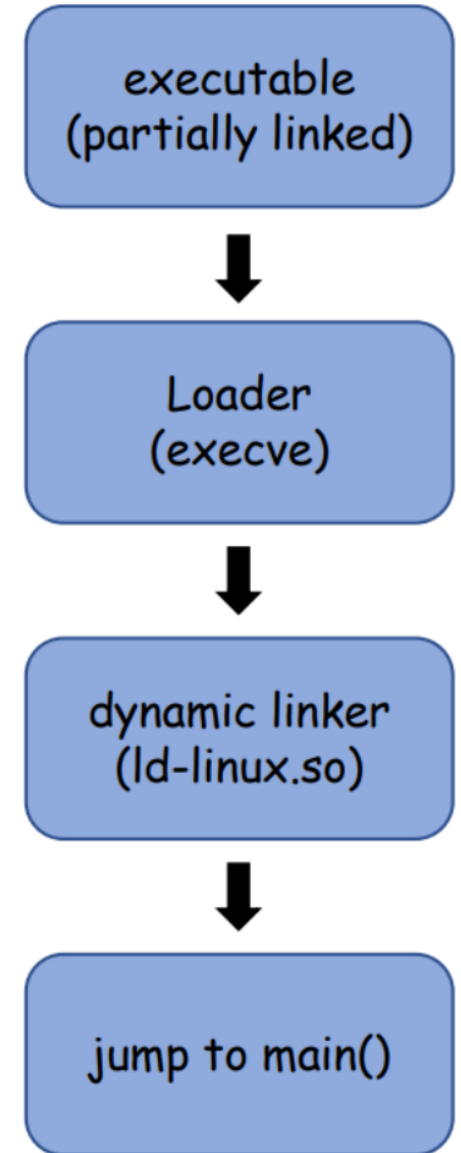
Dynamic Linking- linker uses env variables to locate external dependencies

This program uses the `sleep` function. When compiling this program, how does it know where to find the source code for the `sleep()` function ?

```
// Demo program that calls sleep.
#include <unistd.h>

int main(void)
{
    sleep(1);
    return 0;
}
```

It will use
**environment
variables !**



Linking finds the external library code referenced in a program

Static Linking – Linker combines program code/external code into final executable

Dynamic Linking- linker uses env variables to locate external dependencies

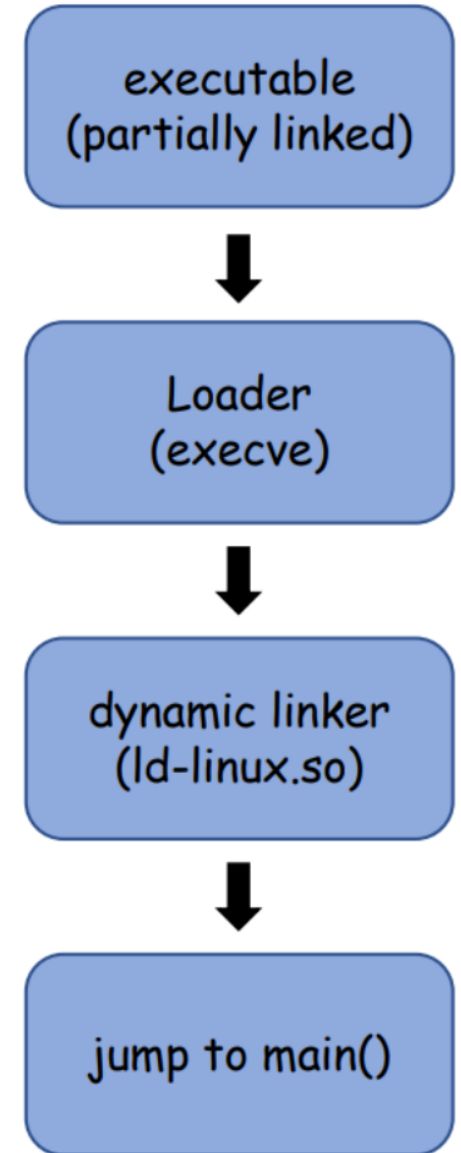
This program uses the `sleep` function. When compiling this program, how does it know where to find the source code for the `sleep()` function ?

```
// Demo program that calls sleep.
#include <unistd.h>

int main(void)
{
    sleep(1);
    return 0;
}
```

It will use
**environment
variables !**

Specifically, it will use the
LD_PRELOAD env variable



Dynamic Linking- linker uses env variables to locate external dependencies

LD_PRELOAD contains a list of shared libraries to search through during the linking process

Provides precedent over standard functions calls (malloc, free, etc)

If functions are not found, it will consult the location specified in **LD_LIBRARY_PATH**

Because these are just environment variables, we can set both of these values (LD_PRELOAD, LD_LIBRARY_PATH)

```
// Demo program that calls sleep.
#include <unistd.h>

int main(void)
{
    sleep(1);
    return 0;
}
```



Any ideas how we could exploit this program?

sleep_prog.c

```
// Demo program that calls sleep.  
#include <unistd.h>  
  
int main(void)  
{  
    sleep(1);  
    return 0;  
}
```

Let's write our own sleep() function!



```
#include <stdio.h>  
void sleep(int s)  
{  
    printf("I'm not sleeping!\n");  
}
```

mylib.c

We could put any code here (printf is not very malicious...)

sleep_prog.c

```
// Demo program that calls sleep.
#include <unistd.h>

int main(void)
{
    sleep(1);
    return 0;
}
```

1 Let's write our own sleep() function!



```
#include <stdio.h>
void sleep(int s)
{
    printf("I'm not sleeping!\n");
}
```

mylib.c

2

Add code to a shared library, libmylib.so.1.0.1

```
$ gcc -fPIC -g -c mylib.c
$ gcc -shared -o libmylib.so.1.0.1 mylib.o -lc
```

sleep_prog.c

```
// Demo program that calls sleep.
#include <unistd.h>

int main(void)
{
    sleep(1);
    return 0;
}
```

1 Let's write our own sleep() function!



```
#include <stdio.h>
void sleep(int s)
{
    printf("I'm not sleeping!\n");
}
```

mylib.c

2

Add code to a shared library, libmylib.so.1.0.1

```
$ gcc -fPIC -g -c mylib.c
$ gcc -shared -o libmylib.so.1.0.1 mylib.o -lc
```

3

Set the `LD_PRELOAD` environment variable, which tells linker to use our malicious library instead of the default one

```
$ export LD_PRELOAD=./libmylib.so.1.0.1
```

`sleep_prog.c` (the program we are exploiting)

```
// Demo program that calls sleep.
#include <unistd.h>

int main(void)
{
    sleep(1);
    return 0;
}
```

1 Let's write our own `sleep()` function! `mylib.c`

```
#include <stdio.h>
void sleep(int s)
{
    printf("I'm not sleeping!\n");
}
```

2 Add code to a shared library, `libmylib.so.1.0.1`

```
$ gcc -fPIC -g -c mylib.c
$ gcc -shared -o libmylib.so.1.0.1 mylib.o -lc
```

3 Set the `LD_PRELOAD` environment variable, which tells linker to use our malicious library instead of the default one

```
$ export LD_PRELOAD=./libmylib.so.1.0.1
```

Task 6 Lab 1:

What if run this program as a normal user?

```
$ gcc -shared -o libmylib.so.1.0.1 mylib.o -lc
$ export LD_PRELOAD=./libmylib.so.1.0.1
$ gcc sleep_prog.c -o sleep_prog
$ ./sleep_prog
```

```
[02/03/23]seed@VM:~/.../01_envvars_setuid$ ./sleep_prog
I'm not sleeping!
```

The program uses our sleep function!!



`sleep_prog.c` (the program we are exploiting)

```
// Demo program that calls sleep.
#include <unistd.h>

int main(void)
{
    sleep(1);
    return 0;
}
```

1 Let's write our own `sleep()` function! `mylib.c`

```
#include <stdio.h>
void sleep(int s)
{
    printf("I'm not sleeping!\n");
}
```

2 Add code to a shared library, `libmylib.so.1.0.1`

```
$ gcc -fPIC -g -c mylib.c
$ gcc -shared -o libmylib.so.1.0.1 mylib.o -lc
```

3 Set the `LD_PRELOAD` environment variable, which tells linker to use our malicious library instead of the default one

```
$ export LD_PRELOAD=./libmylib.so.1.0.1
```

Task 6 Lab 1:

What if we make the program a **Set-UID** program and run as a normal user?

```
$ gcc -shared -o libmylib.so.1.0.1 mylib.o -lc
$ export LD_PRELOAD=./libmylib.so.1.0.1
$ gcc sleep_prog.c -o sleep_prog
$ ./sleep_prog

$ sudo chown root sleep_prog
$ sudo chmod 4755 sleep_prog
```

```
[02/03/23] seed@VM:~/.../01_envvars_setuid$ ./sleep_prog
[02/03/23] seed@VM:~/.../01_envvars_setuid$
```

The program sleeps normally (it does **not** use our sleep function)



`sleep_prog.c` (the program we are exploiting)

```
// Demo program that calls sleep.
#include <unistd.h>

int main(void)
{
    sleep(1);
    return 0;
}
```

1 Let's write our own `sleep()` function! `mylib.c`

```
#include <stdio.h>
void sleep(int s)
{
    printf("I'm not sleeping!\n");
}
```

2 Add code to a shared library, `libmylib.so.1.0.1`

```
$ gcc -fPIC -g -c mylib.c
$ gcc -shared -o libmylib.so.1.0.1 mylib.o -lc
```

3 Set the `LD_PRELOAD` environment variable, which tells linker to use our malicious library instead of the default one

```
$ export LD_PRELOAD=./libmylib.so.1.0.1
```

Task 6 Lab 1:

What if we make the program a **Set-UID** program and run as the **root** user?

```
$ gcc -shared -o libmylib.so.1.0.1 mylib.o -lc
$ export LD_PRELOAD=./libmylib.so.1.0.1
$ gcc sleep_prog.c -o sleep_prog
$ ./sleep_prog
```

```
$ sudo chown root sleep_prog
$ sudo chmod 4755 sleep_prog
```

```
$ sudo su root
# export LD_PRELOAD=./libmylib.so.1.0.1
```

```
root@VM:/home/seed/csci476-code/01_envvars_setuid# ./sleep_prog
I'm not sleeping!
```



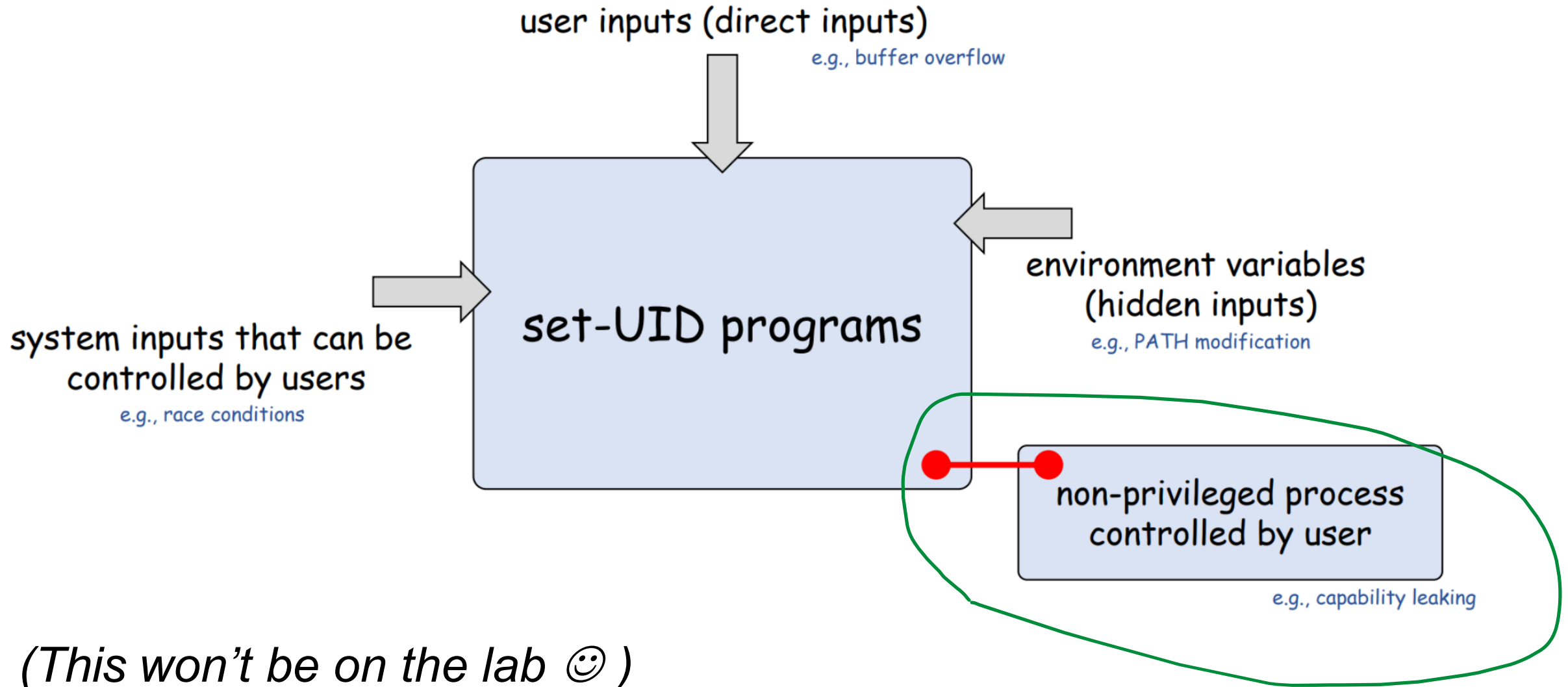
The program uses our sleep function!!

We have mixed results. Sometimes the program used our malicious sleep function, other times it did not

Process Owner	Set-UID program?	Success?
seed		
seed		
root		

Any ideas what could be causing this?

Exploiting Set-UID programs via capability leaking



Exploiting Set-UID programs via capability leaking

Often times, a process will *downgrade* its privileges when it no longer needs them

It can do this by using the `setuid()` function

```
/*  
 * After the task, elevated privileges are no longer needed;  
 * it is time to relinquish these privileges!  
 * NOTE: getuid() returns the real UID (RUID)  
 */  
setuid(getuid());
```

Capability leaking can occur when a privilege process does not properly clean up its privileges when downgrading

```

int main()
{
    int fd;

    /*
     * Assume that /etc/zxx is an important system file,
     * and it is owned by root with permission 0644.
     * Before running this program, you should create
     * the file /etc/zxx first.
     */
    fd = open("/etc/zxx", O_RDWR | O_APPEND);
    if (fd == -1) {
        printf("Cannot open /etc/zxx\n");
        exit(0);
    }

    // Simulate the tasks conducted by the program
    sleep(1);

    /*
     * After the task, elevated privileges are no longer needed;
     * it is time to relinquish these privileges!
     * NOTE: getuid() returns the real UID (RUID)
     */
    setuid(getuid());

    if (fork()) { /* parent process */
        close (fd);
        exit(0);
    } else { /* child process */

        /*
         * Now, assume that the child process is compromised, and that
         * malicious attackers have injected the following statements into this process
         */
        write (fd, "Malicious Data\n", 15);
        close (fd);
    }
}

```

First opens a file descriptor (`fd`) for “`/etc/zxx`”, which is only writeable by root

Suppose this program does some stuff with the file before dropping privileges

```

int main()
{
    int fd;

    /*
     * Assume that /etc/zxx is an important system file,
     * and it is owned by root with permission 0644.
     * Before running this program, you should create
     * the file /etc/zxx first.
     */
    fd = open("/etc/zxx", O_RDWR | O_APPEND);
    if (fd == -1) {
        printf("Cannot open /etc/zxx\n");
        exit(0);
    }

    // Simulate the tasks conducted by the program
    sleep(1);

    /*
     * After the task, elevated privileges are no longer needed;
     * it is time to relinquish these privileges!
     * NOTE: getuid() returns the real UID (RUID)
     */
    setuid(getuid());

    if (fork()) { /* parent process */
        close (fd);
        exit(0);
    } else { /* child process */

        /*
         * Now, assume that the child process is compromised, and that
         * malicious attackers have injected the following statements into this process
         */
        write (fd, "Malicious Data\n", 15);
        close (fd);
    }
}

```

We then fork() and create a new process

- In the parent process, we close the file
- However, in the child process, the file descriptor is still open!


```

int 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 create
     * 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, elevated privileges are no longer needed;
     * it is time to relinquish these privileges!
     * NOTE: getuid() returns the real UID (RUID)
     */
    setuid(getuid());

    if (fork()) { /* parent process */
        close (fd);
        exit(0);
    } else { /* child process */

        /*
         * Now, assume that the child process is compromised, and that
         * malicious attackers have injected the following statements into this process
         */
        write (fd, "Malicious Data\n", 15);
        close (fd);
    }
}

```

If this a Set-UID program, then `fd` is a root-level file descriptor, and the child process inherits this!

Thus, the child process (which was created after dropping privileges) can write to `/etc/zzz` (bad!!!!)


```

int 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 create
     * 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, elevated privileges are no longer needed;
 * it is time to relinquish these privileges!
 * NOTE: getuid() returns the real UID (RUID)
 */
setuid(getuid());

if (fork()) { /* parent process */
    close (fd);
    exit(0);
} else { /* child process */

    /*
     * Now, assume that the child process is compromised, and that
     * malicious attackers have injected the following statements into this process
     */
    write (fd, "Malicious Data\n", 15);
    close (fd);
}
}

```

Capability leaking can occur when a privilege process does not properly clean up its privileges when downgrading

Always be careful about the privileges you are giving to a process!

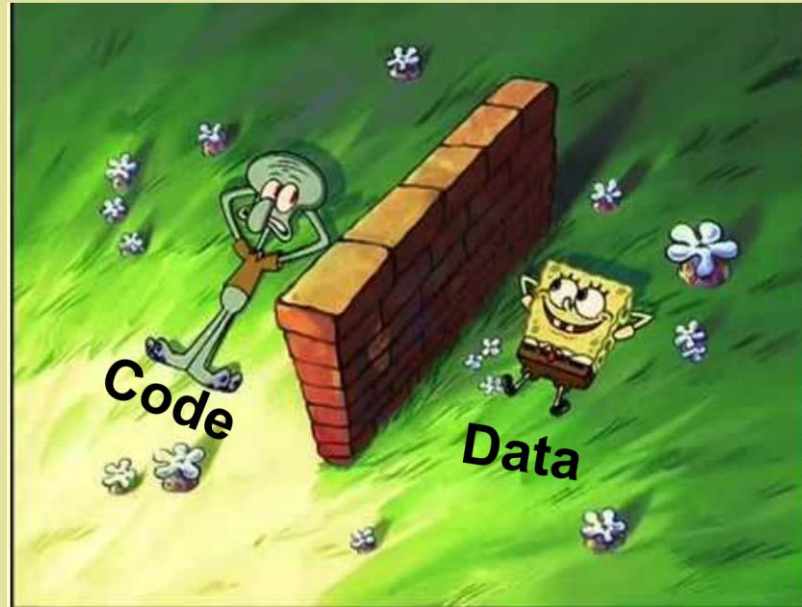
That's it for Set-UID Programs, but we will continue to use Set-UID programs in future sections

Did we learn any valuable lessons?

Principle of Isolation

There needs to be a clear separation of **data** and **code**

If user input is needed as data, it should **not** be interpreted as code



Principle of Least Privilege

Subjects and Programs should be given only the privileges needed to complete their task

Disable privileges when they are not needed

