Operating Systems

Assignment 4

~ Shaunak Pal

A1) Code for Syscall_handler:

```
push %eax
push %ebx
push %edx
push %fs

mov $216, %ecx
mov %ecx, %fs
push %ebx
push %eax

call syscall_handler_k

pop %eax
pop %ebx
pop %fs
pop %edx
pop %ebx
pop %eax
```

A2) Code for syscall_u:

```
mov 4(%esp), %eax
mov 8(%esp), %ebx
```

A3) Code for register_syscall:

```
static void register_syscall(void)
{
   unsigned long syscall_addr = (unsigned long)syscall_handler;
   struct idt_desc newIDT;
   if(imp_copy_idt(&newIDT)) {
       struct idt_desc oldIDT = newIDT;
```

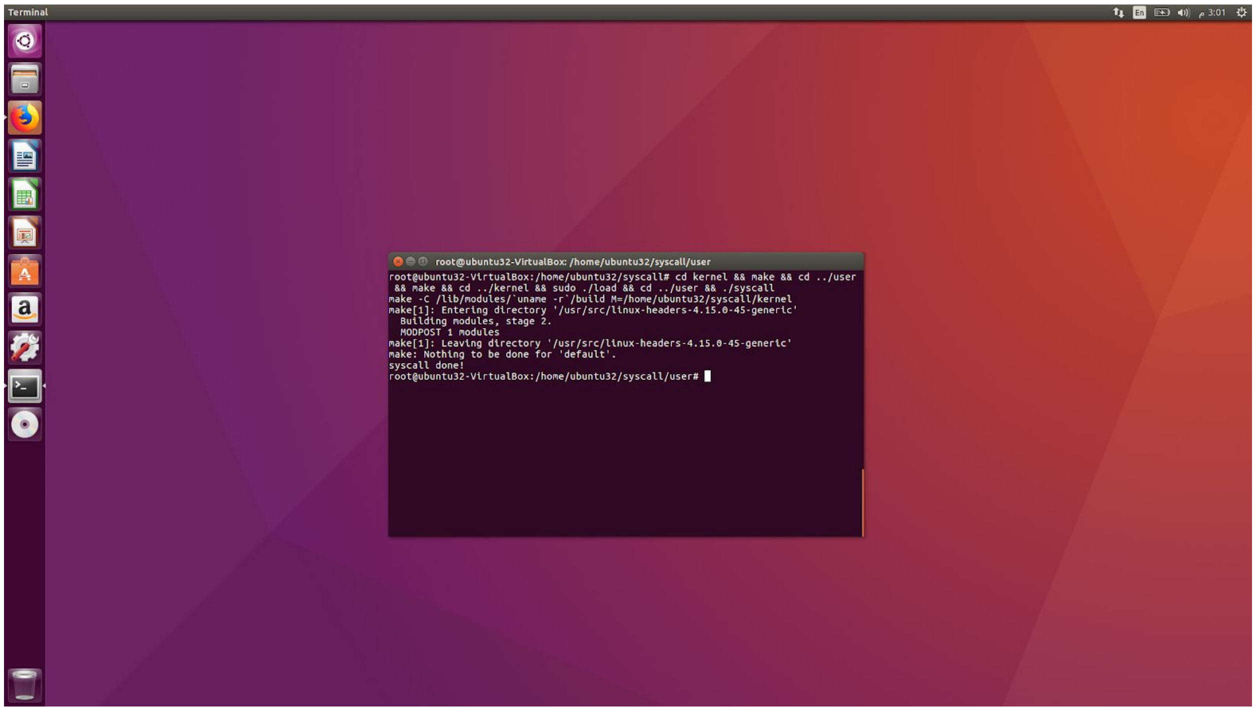
```
        newIDT.base[15]=oldIDT.base[128]
        (&newIDT)->base[15].lower16 = syscall_addr;
        (&newIDT)->base[15].higher16 = syscall_addr>>16;
        imp_load_idt(&newIDT, &oldIDT);
        originalIDT = oldIDT;
        printk("doing job\n");
    }
    else {
        printk("idt copy failed.\n");
    }
}
```

A4) Code for unregister_syscall:

```
static void unregister_syscall(void)
{
    struct idt_desc currentIDT;
    imp_copy_idt(&currentIDT);
    if (&currentIDT != &originalIDT) {
        imp_load_idt(&originalIDT, &currentIDT);
        imp_free_desc(&currentIDT);
    }
}
```

A5) Output of user-program:

```
root@ubuntu32-VirtualBox:/home/ubuntu32/Documents/syscall# cd kernel && make && cd
../user && make && cd ../kernel && ./load && cd ../user && ./syscall && cd ..
make -C /lib/modules/`uname -r`/build M=/home/ubuntu32/Documents/syscall/kernel
make[1]: Entering directory '/usr/src/linux-headers-4.15.0-45-generic'
  Building modules, stage 2.
  MODPOST 1 modules
make[1]: Leaving directory '/usr/src/linux-headers-4.15.0-45-generic'
make: Nothing to be done for 'default'.
syscall done!
```



```
root@ubuntu32-VirtualBox:/home/ubuntu32/syscall# cd kernel && make && cd ../user
 && make && cd ../kernel && sudo ./load && cd ../user && ./syscall
make -C /lib/modules/`uname -r`/build M=/home/ubuntu32/syscall/kernel
make[1]: Entering directory '/usr/src/linux-headers-4.15.0-45-generic'
  Building modules, stage 2.
  MODPOST 1 modules
make[1]: Leaving directory '/usr/src/linux-headers-4.15.0-45-generic'
make: Nothing to be done for 'default'.
syscall done!
root@ubuntu32-VirtualBox:/home/ubuntu32/syscall/user# 
```

A6) The original IDT was stored as a global variable. Its value is update in register_syscall function

A7) The current IDT is obtained from the given function imp_copy_idt with an empty struct idt_desc as parameter which copies the current idt to the empty struct and then we can use it.

A8) Neither of them happens because the if condition in unregister_syscall checks whether current IDT and original IDT are different. So since they will be the same the second time the program does not go inside the if condition so original IDT is not loaded twice and current IDT is not freed.