BING-HAO LI
N19732011

CS6233 Introduction to Operating Systems HW1

1. What are kernel APIs? What is the difference between kernel APIs and system calls?

Kernel APIs:
They are the interfaces for user-space applications. They can invoke user-space application and control the output.

System calls:
They allow user-space programs to invoke methods defined in the kernel.

2. What are roles of files in /boot/ (vmlinuz-*, initrd.img-*, grub, config*)?

vmlinuz-*:
It is a compressed file of Linux kernel. The first thing computer will do is loads this file into memory.

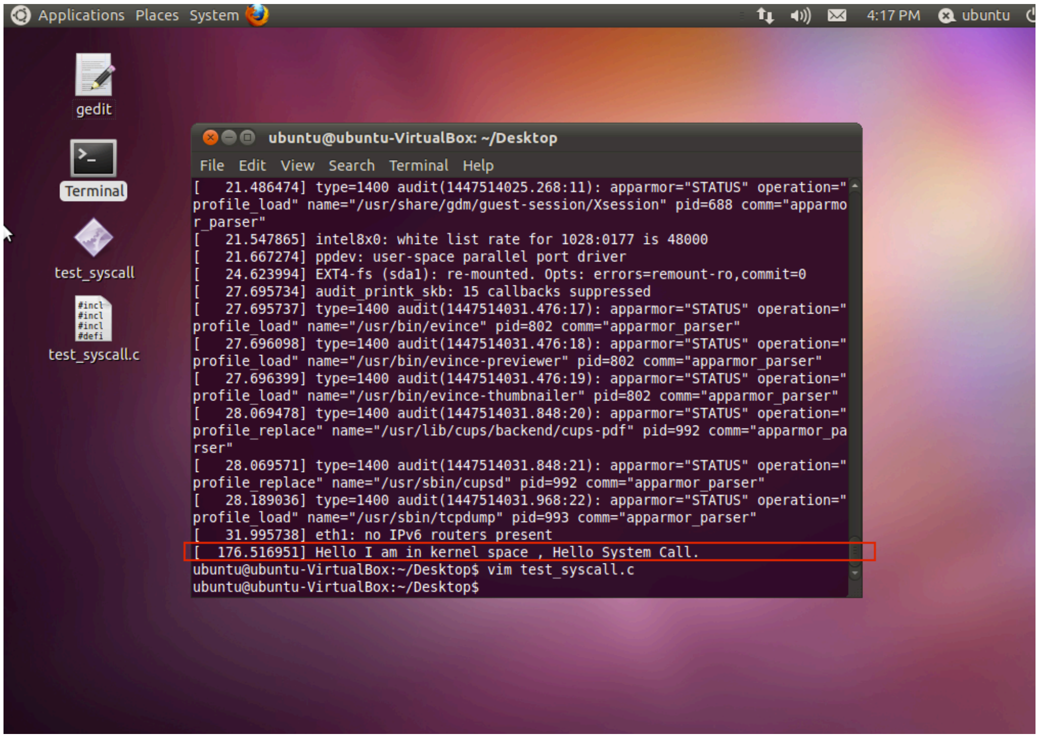
initrd.img-*:
It is a temporary root file system. It is mounted during system boot to support the two-state boot process. It also contains various executables and drivers which permit the root file system to be mounted successfully.

grub:
It is a boot loader. It is used to load the kernel when starting the system.

config*:
It is the configuration file of the kernel. In this file, we can choose which modules or drivers should be added into kernel. Therefore, we can decide the size and functionality of the linux system.

Include the screenshots from tasks 1, 2, and 3 below:

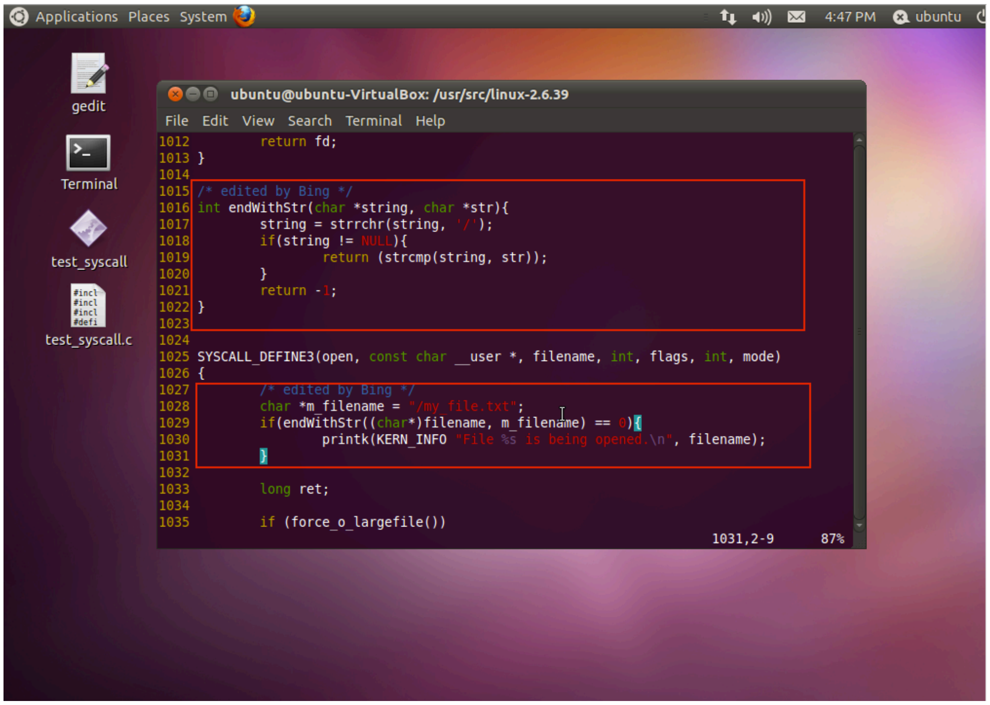
Task 1:


Applications Places System
4:17 PM
ubuntu
gedit
Terminal
test_syscall
test_syscall.c
ubuntu@ubuntu-VirtualBox: ~/Desktop
File Edit View Search Terminal Help

```
[   21.486474] type=1400 audit(1447514025.268:11): apparmor="STATUS" operation="
profile_load" name="/usr/share/gdm/guest-session/Xsession" pid=688 comm="apparmo
r_parser"
[   21.547865] intel8x0: white list rate for 1028:0177 is 48000
[   21.667274] ppdev: user-space parallel port driver
[   24.623994] EXT4-fs (sda1): re-mounted. Opts: errors=remount-ro,commit=0
[   27.695734] audit_printk_skb: 15 callbacks suppressed
[   27.695737] type=1400 audit(1447514031.476:17): apparmor="STATUS" operation="
profile_load" name="/usr/bin/evince" pid=802 comm="apparmor_parser"
[   27.696098] type=1400 audit(1447514031.476:18): apparmor="STATUS" operation="
profile_load" name="/usr/bin/evince-previewer" pid=802 comm="apparmor_parser"
[   27.696399] type=1400 audit(1447514031.476:19): apparmor="STATUS" operation="
profile_load" name="/usr/bin/evince-thumbnailer" pid=802 comm="apparmor_parser"
[   28.069478] type=1400 audit(1447514031.848:20): apparmor="STATUS" operation="
profile_replace" name="/usr/lib/cups/backend/cups-pdf" pid=992 comm="apparmor_pa
rser"
[   28.069571] type=1400 audit(1447514031.848:21): apparmor="STATUS" operation="
profile_replace" name="/usr/sbin/cupsd" pid=992 comm="apparmor_parser"
[   28.189036] type=1400 audit(1447514031.968:22): apparmor="STATUS" operation="
profile_load" name="/usr/sbin/tcpdump" pid=993 comm="apparmor_parser"
[   31.995738] eth1: no IPv6 routers present
[  176.516951] Hello I am in kernel space , Hello System Call.
ubuntu@ubuntu-VirtualBox:~/Desktop$ vim test_syscall.c
ubuntu@ubuntu-VirtualBox:~/Desktop$
```

Task 2:

I edit the file: /usr/src/linux2.6.39/fs/open.c


Applications Places System
4:47 PM
ubuntu
gedit
Terminal
test_syscall
test_syscall.c
ubuntu@ubuntu-VirtualBox: /usr/src/linux-2.6.39
File Edit View Search Terminal Help

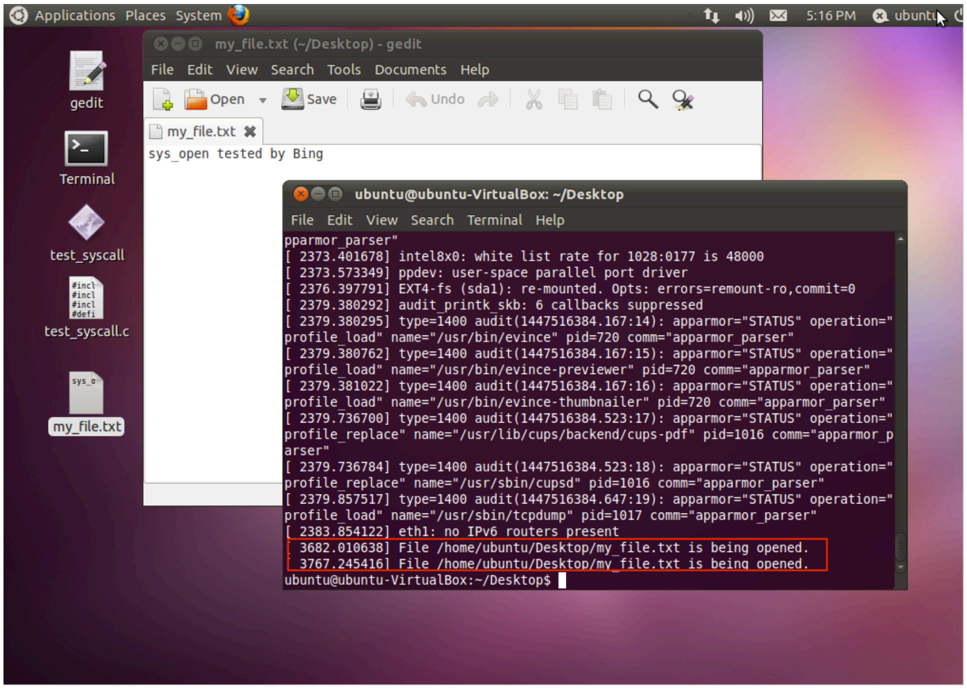
```
        return fd;
}

/* edited by Bing */
int endWithStr(char *string, char *str){
        string = strrchr(string, '/');
        if(string != NULL){
                return (strcmp(string, str));
        }
        return -1;
}

SYSCALL_DEFINE3(open, const char __user *, filename, int, flags, int, mode)
{
        /* edited by Bing */
        char *m_filename = "/my_file.txt";
        if(endWithStr((char*)filename, m_filename) == 0){
                printk(KERN_INFO "File %s is being opened.\n", filename);
        }

        long ret;

        if (force_o_largefile())
                                                              1031,2-9      87%
```

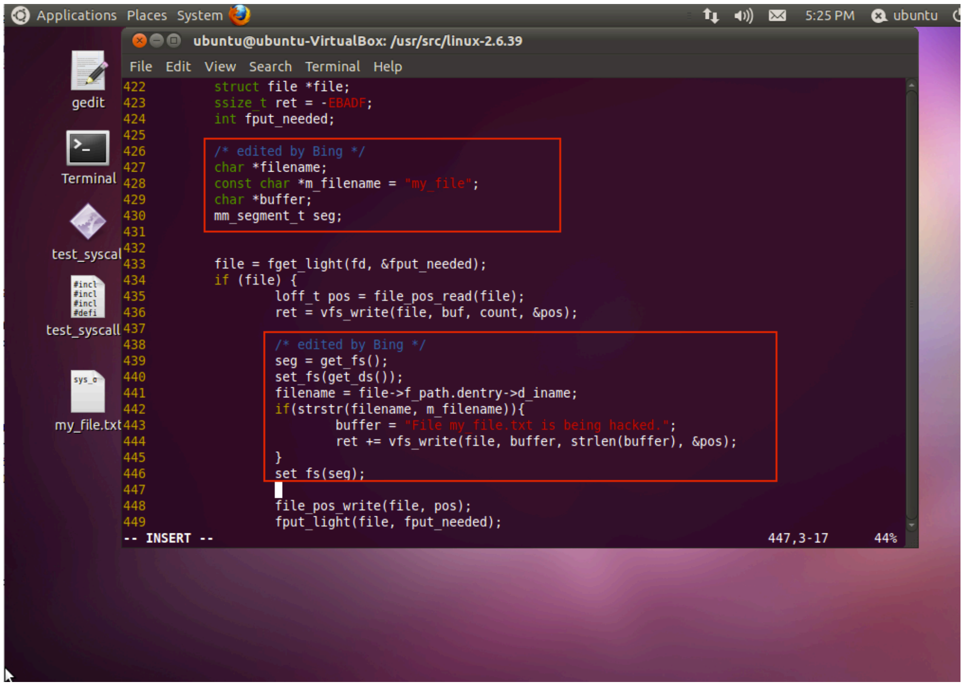

Applications Places System
5:16 PM
ubuntu
gedit
Terminal
test_syscall
test_syscall.c
my_file.txt
my_file.txt (~/Desktop) - gedit
File Edit View Search Tools Documents Help
Open
Save
Undo
ubuntu@ubuntu-VirtualBox: ~/Desktop
File Edit View Search Terminal Help

```
sys_open tested by Bing
```

```
pparmor_parser"
[ 2373.401678] intel8x0: white list rate for 1028:0177 is 48000
[ 2373.573349] ppdev: user-space parallel port driver
[ 2376.397791] EXT4-fs (sda1): re-mounted. Opts: errors=remount-ro,commit=0
[ 2379.380292] audit_printk_skb: 6 callbacks suppressed
[ 2379.380295] type=1400 audit(1447516384.167:14): apparmor="STATUS" operation="
profile_load" name="/usr/bin/evince" pid=720 comm="apparmor_parser"
[ 2379.380762] type=1400 audit(1447516384.167:15): apparmor="STATUS" operation="
profile_load" name="/usr/bin/evince-previewer" pid=720 comm="apparmor_parser"
[ 2379.381022] type=1400 audit(1447516384.167:16): apparmor="STATUS" operation="
profile_load" name="/usr/bin/evince-thumbnailer" pid=720 comm="apparmor_parser"
[ 2379.736700] type=1400 audit(1447516384.523:17): apparmor="STATUS" operation="
profile_replace" name="/usr/lib/cups/backend/cups-pdf" pid=1016 comm="apparmor_p
arser"
[ 2379.736784] type=1400 audit(1447516384.523:18): apparmor="STATUS" operation="
profile_replace" name="/usr/sbin/cupsd" pid=1016 comm="apparmor_parser"
[ 2379.857517] type=1400 audit(1447516384.647:19): apparmor="STATUS" operation="
profile_load" name="/usr/sbin/tcpdump" pid=1017 comm="apparmor_parser"
[ 2383.854122] eth1: no IPv6 routers present
[ 3682.010638] File /home/ubuntu/Desktop/my_file.txt is being opened.
[ 3767.245416] File /home/ubuntu/Desktop/my_file.txt is being opened.
ubuntu@ubuntu-VirtualBox:~/Desktop$
```

Task 3:

I edit the file: /usr/src/linux2.6.39/fs/read_write.c


Applications Places System
5:25 PM
ubuntu
gedit
Terminal
test_syscal
test_syscall
my_file.txt
ubuntu@ubuntu-VirtualBox: /usr/src/linux-2.6.39
File Edit View Search Terminal Help

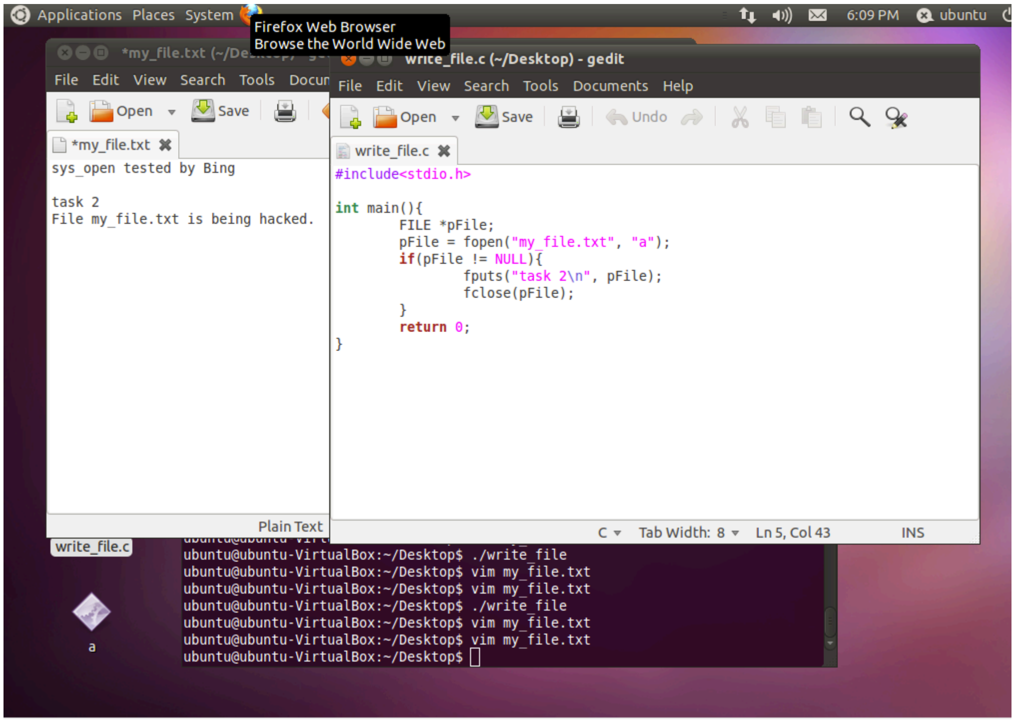
```
        struct file *file;
        ssize_t ret = -EBADF;
        int fput_needed;

        /* edited by Bing */
        char *filename;
        const char *m_filename = "my_file";
        char *buffer;
        mm_segment_t seg;


        file = fget_light(fd, &fput_needed);
        if (file) {
                loff_t pos = file_pos_read(file);
                ret = vfs_write(file, buf, count, &pos);

                /* edited by Bing */
                seg = get_fs();
                set_fs(get_ds());
                filename = file->f_path.dentry->d_iname;
                if(strstr(filename, m_filename)){
                        buffer = "File my_file.txt is being hacked.";
                        ret += vfs_write(file, buffer, strlen(buffer), &pos);
                }
                set_fs(seg);

                file_pos_write(file, pos);
                fput_light(file, fput_needed);
-- INSERT --                                                  447,3-17      44%
```


Applications Places System
Firefox Web Browser
Browse the World Wide Web
6:09 PM
ubuntu
*my_file.txt (~/De
File Edit View Search Tools Docun
Open
Save
*my_file.txt
Plain Text
write_file.c (~/Desktop) - gedit
File Edit View Search Tools Documents Help
Open
Save
Undo
write_file.c
C
Tab Width: 8
Ln 5, Col 43
INS
write_file.c
a

```
sys_open tested by Bing

task 2
File my_file.txt is being hacked.
```

```c
#include<stdio.h>

int main(){
        FILE *pFile;
        pFile = fopen("my_file.txt", "a");
        if(pFile != NULL){
                fputs("task 2\n", pFile);
                fclose(pFile);
        }
        return 0;
}
```

```
ubuntu@ubuntu-VirtualBox:~/Desktop$ ./write_file
ubuntu@ubuntu-VirtualBox:~/Desktop$ vim my_file.txt
ubuntu@ubuntu-VirtualBox:~/Desktop$ vim my_file.txt
ubuntu@ubuntu-VirtualBox:~/Desktop$ ./write_file
ubuntu@ubuntu-VirtualBox:~/Desktop$ vim my_file.txt
ubuntu@ubuntu-VirtualBox:~/Desktop$ vim my_file.txt
ubuntu@ubuntu-VirtualBox:~/Desktop$ 
```

All the files I modify:
linux-2.6.39 / kernel / my_system_call.c
linux-2.6.39 / arch / x86 / kernel / syscall_table_32.S
linux-2.6.39 / arch / x86 / include / asm / unistd_32.h
linux-2.6.39 / arch / x86 / include / asm / unistd_64.h
linux-2.6.39 / include / linux / syscalls.h
linux-2.6.39 / kernel / Makefile
linux-2.6.39 / fs / open.c
linux-2.6.39 / fs / read_write.c

Test code:
test_syscall.c
write_file.c

Test file:
my_file.txt