

OS 第二次作業

一、分工

鄧智宇：撰寫報告、相關資料查找

黃信維：撰寫程式、相關資料查找

二、作業步驟以及遇到問題

1. 一開始執行基本的步驟，編輯、新增新的 system call 等，還有重燒作業系統

```
}  
/* for __ARCH_WANT_SYS_IPC */  
long ksys_senrtimedop(int semid, struct sembuf __user *tsops,  
    unsigned int nsops,  
    const struct __kernel_timespec __user *timeout);  
long ksys_semget(key_t key, int nsems, int semflg);  
long ksys_old_semctl(int semid, int semnum, int cmd, unsigned long arg);  
long ksys_msgget(key_t key, int msgflg);  
long ksys_old_msgctl(int msqid, int cmd, struct msqid_ds __user *buf);  
long ksys_msgrcv(int msqid, struct msgbuf __user *msgp, size_t msgsz,  
    long msgtyp, int msgflg);  
long ksys_msgsnd(int msqid, struct msgbuf __user *msgp, size_t msgsz,  
    int msgflg);  
long ksys_shmget(key_t key, size_t size, int shmflg);  
long ksys_shmctl(char __user *shmaddr);  
long ksys_old_shmctl(int shmid, int cmd, struct shmid_ds __user *buf);  
long compat_ksys_senrtimedop(int semid, struct sembuf __user *tsems,  
    unsigned int nsops,  
    const struct old_timespec32 __user *timeout);  
asmlinkage long sys_myCall(void);  
#endif
```

```
20.388969] fbcon: svgadrmfb (fb0) is primary device  
20.391419] Console: switching to colour frame buffer device 100x37  
20.396684] [drm] Initialized vmwgfx 2.18.0 20200114 for 0000:00:02.0 on minor 0  
21.670963] snd_intel8x0 0000:00:05.0: white list rate for 1028:0177 is 48000  
29.918353] e1000: enp0s3 NIC Link is Up 1000 Mbps Full Duplex, Flow Control: RX  
29.918691] IPv6: ADDRCONF(NETDEV_CHANGE): enp0s3: link becomes ready  
55.173265] rfkill: input handler disabled  
402.154037] This is my new syscall!  
hfs840173@hfs840173-VirtualBox:~/linux-5.7.9/mySyscall$
```

```
hfs840173@hfs840173-VirtualBox: ~/linux-5.7.9/mySyscall  
檔案(F) 編輯(E) 檢視(V) 搜尋(S) 終端機(T) 求助(H)  
hfs840173@hfs840173-VirtualBox:~$ cd linux-5.7.9/  
hfs840173@hfs840173-VirtualBox:~/linux-5.7.9$ cd mySyscall  
hfs840173@hfs840173-VirtualBox:~/linux-5.7.9/mySyscall$ vim test_call.c  
hfs840173@hfs840173-VirtualBox:~/linux-5.7.9/mySyscall$ gcc -static -g test_call.c -o test_call.o  
hfs840173@hfs840173-VirtualBox:~/linux-5.7.9/mySyscall$ ./test_call.o  
Hello! (from printf syscall)  
hfs840173@hfs840173-VirtualBox:~/linux-5.7.9/mySyscall$
```

測試程式可成功執行。

2. 遇到的第一個問題是每次燒的速度太慢，經過助教提醒，可將虛擬機的核心樹調高，並使用 make -j2，就快多了。

3. 在撰寫 syscall 的時候，一開始想用直接使用組合語言的方式，但是發現印不出任何東西。後來經提醒，去查了 SYSTEM_DEFINE 的用法，並在 syscalls.h 內找到相關定義。
4. 因為我們要傳入四個參數，所以是用 SYSTEM_DEFINE4，然後把加減號、和兩個整數和答案分別傳入自定義的 system call 裡，並在 system call 內運算。運算完再傳回 user space 後印出。
5. 另外我們也查詢了 copy_to_user 的使用方式，以把內容從 kernel space 複製到 user space。
6. 在編譯時出現下面的訊息：

```
from mySyscall/sys_new_call.c:1:
In function 'check_copy_size',
    inlined from 'copy_to_user' at ./include/linux/uaccess.h:151:6,
    inlined from '__do_sys_mycall.isra.0' at mySyscall/sys_new_call.c:13:7,
    inlined from '__se_sys_mycall.isra.1' at mySyscall/sys_new_call.c:4:1,
    inlined from '__x64_sys_mycall' at mySyscall/sys_new_call.c:4:1:
./include/linux/thread_info.h:145:4: error: call to '__bad_copy_from' declared with attribute error: copy source size is too small
__bad_copy_from();
~~~~~
In function 'check_copy_size',
    inlined from 'copy_to_user' at ./include/linux/uaccess.h:151:6,
    inlined from '__do_sys_mycall.isra.0' at mySyscall/sys_new_call.c:13:7,
    inlined from '__se_sys_mycall.isra.1' at mySyscall/sys_new_call.c:4:1,
    inlined from '__ia32_sys_mycall' at mySyscall/sys_new_call.c:4:1:
./include/linux/thread_info.h:145:4: error: call to '__bad_copy_from' declared with attribute error: copy source size is too small
__bad_copy_from();
~~~~~
```

解決方式是將 copy_to_user 的參數改為 sizeof()，就可以成功編譯了

7. 但是在 make 的時候，卻跑出錯誤訊息如下

```
GEN      modules.builtins
LD        .tmp_vmlinux.kallsyms1
arch/x86/entry/syscall_64.o(.rodata+0xdb8): 未定義參考到 __x64_sys_myCall
arch/x86/entry/syscall_x32.o(.rodata+0xdb8): 未定義參考到 __x64_sys_myCall
Makefile:1109: recipe for target 'vmlinux' failed
make: *** [vmlinux] Error 1
```

查到的解決方法是，linux 的版本是新的，但 C 語言函式庫沒有同步更新所導致，所以我們更改 syscall_64.tbl 重新 make 一次，但因為時間來不及燒完，所以先交沒有 make 成功的。

三、浮點數是否能在 syscall 內使用？

大部分的觀點都是認為盡量不要，原因可能有浮點數的暫存器較耗空間和資源等，但仍可以使用。對於有 FPU 的處理器，因為 linux 會將浮點數轉成整數後運算，所以要讓 module 使用硬浮點，也就是先改 kernel 的配置(Makefile 內)，然後再行編譯；然後就可以執行了。但如果沒有 FPU，就只能用軟浮點來模擬期運算。

四、部份成功截圖：

```
hfs840173@hfs840173-VirtualBox:~/桌面/1$ cd ..
hfs840173@hfs840173-VirtualBox:~/桌面$ gcc -static -g test_call.c -o test_call.o
hfs840173@hfs840173-VirtualBox:~/桌面$ ./test_call.o
6 + 6 = 0
1 + 0 = 0
1 - 5 = 0
0 + (-15) = -0
(-55) + (-5) = -0
hfs840173@hfs840173-VirtualBox:~/桌面$
```

```
[ 23.748223] fbcon: svgadrmfb (fb0) is primary device
[ 23.922992] Console: switching to colour frame buffer device 100x37
[ 24.257439] [drm] Initialized vmwgfx 2.18.0 20200114 for 0000:00:02.0 on minor 0
[ 29.503747] snd_intel8x0 0000:00:05.0: white list rate for 1028:0177 is 48000
[ 38.797103] e1000: enp0s3 NIC Link is Up 1000 Mbps Full Duplex, Flow Control: RX
[ 38.797558] IPv6: ADDRCONF(NETDEV_CHANGE): enp0s3: link becomes ready
[ 92.117505] rkill: input handler disabled
[ 292.314083] This is my new syscall!
[ 292.314114] This is my new syscall!
[ 292.314117] This is my new syscall!
[ 292.314120] This is my new syscall!
[ 292.314123] This is my new syscall!
hfs840173@hfs840173-VirtualBox:~/桌面/1$
```

五、引用資料

查 copy_to_user、copy_from_user 的用法

<https://stackoverflow.com/questions/6515227/source-code-example-from-linux-kernel-programming>

<https://stackoverflow.com/questions/29397364/copy-to-user-and-copy-from-user-for-basic-data-type>

<https://elixir.bootlin.com/linux/v5.7.9/source/include/linux/uaccess.h#L149>

為了要查詢系統 SYSCALL_DEFINE 的定義

<http://gityuan.com/2016/05/21/syscall/>

<https://elixir.bootlin.com/linux/v5.7.9/source/include/linux/uaccess.h#L149>

能否使用浮點數

<https://stackoverflow.com/questions/15883947/why-am-i-able-to-perform-floating-point-operations-inside-a-linux-kernel-module/47056242>

<https://stackoverflow.com/questions/13886338/use-of-floating-point-in-the-linux-kernel>

<https://blog.csdn.net/k7arm/article/details/81406842>

<https://www.itread01.com/p/1389126.html>

編譯時參數問題的解決方式

<https://github.com/analogdevicesinc/linux/pull/206>

<https://blog.csdn.net/u013969018/article/details/86686842>

「未定義參考」解決方式

<https://stackoverflow.com/questions/29137244/undefined-reference-error-while-using-custom-system-call>