CS3013\_Project 2

Yuan Wang & Yuanda Song

Part1(NOTE: BECAUSE syslog size was too large. We just select some of them )

In part1, we intercepted the new added syscall cs3013\_syscall1, then we created a program cs3013\_syscall1.c to intercept the original open can close syscalls. To test our program, in the direct dictionary, open the terminal, type ‘make’ commend to generate the kernel modules, the ‘sudo insmod <module\_name>’ to insert the module into the kernel. Besides, we also have a program called ‘part1test.c’ you need to compile it first and type ‘./part1test to test cs3013\_syscall1’ and if you want to check the logfile, you can type ‘tail –n 3 /var/log/syslog’. After the testing, please remove all the modules by typing ‘sudo rmmod <module\_name>’.

Part2:

In part2, we intercepted the syscall cs3013\_syscall2. When the interception done, we are able to print the information as the instructions required(parent and child processes by using the cs3013-syscall2).Just like what we did in the first part. ‘make’ the kernel modul, ‘sudo insmod <module\_name>, ’ then using the test program (you need to compile first) ./part2test to the test the module. After the testing, please remove all the modules by typing ‘sudo rmmod <module\_name>’.