

Creating our own Syscall

In this Assignment , I had implemented my own system call **sh_task_info** using C which is used to print all the fields of the task corresponding to pid on the terminal as well as in file.

User Input:

My program takes two arguments: First one is the PID of the process and the other one is FILENAME in which data corresponding to that PID is stored. Both pid and filename is given by user as an input & file will be created in the directory where test.c is run by the user.

How SYSCALL is Implemented:

I implemented my syscall in Kernel version 5.9.1 in which I created a folder named **custom_syscall**. In that folder I created sh_task_info.c file in which I define my syscall as follows:

First I used SYSCALL_DEFINE2(sh_task_info,int,pid,char *,filename) to create my syscall where SYSCALL_DEFINE is used to define syscall and here 2 means that it takes two arguments .

- 1) Pid of type int
- 2) Filename of type string

I used task_struct a 'C- structure' to store the task corresponding to the given pid.

And a file pointer to create a file from the kernel.

Helping function:

- 1) pid_task(find_vpid(pid), PIDTYPE_PID) : it is used to get the task_struct of a given pid.
- 2) filp_open(file_name, O_WRONLY|O_CREAT, 0644) : it is used to open a file of name file_name with two flags which means Write/Read only and O_CREAT is used to create the file if it does not exist. Here 0644 is the permission.
- 3) vfs_write(fl, data, strlen(data), &fl->f_pos) : it is used to write data in a file where fl is file pointer , data is what we want to write in file, and offset.

Output:

To test the syscall I made a test.c which can be run by Makefile. It will print and put the following data in the terminal as well as in file.

Process Name

Process Id

Process State

Process Priority

Process Static Priority

Process utime

Process Group

Error handled

- If pid > 32768 or pid<=0 then -EINVAL error is returned by syscall which means Invalid Arguments.
- If the pid task doesn't exist.
- If the user enters char/string instead of int for pid.
- If syscall is unable to create file or write file then -EFAULT error is returned by the syscall.