Syscalls

openSUSE Conference 2016

By Bernhard M. Wiedemann
bwiedemann@SUSE

© ScotXW / Wikipedia License: CC BY-SA 3.0
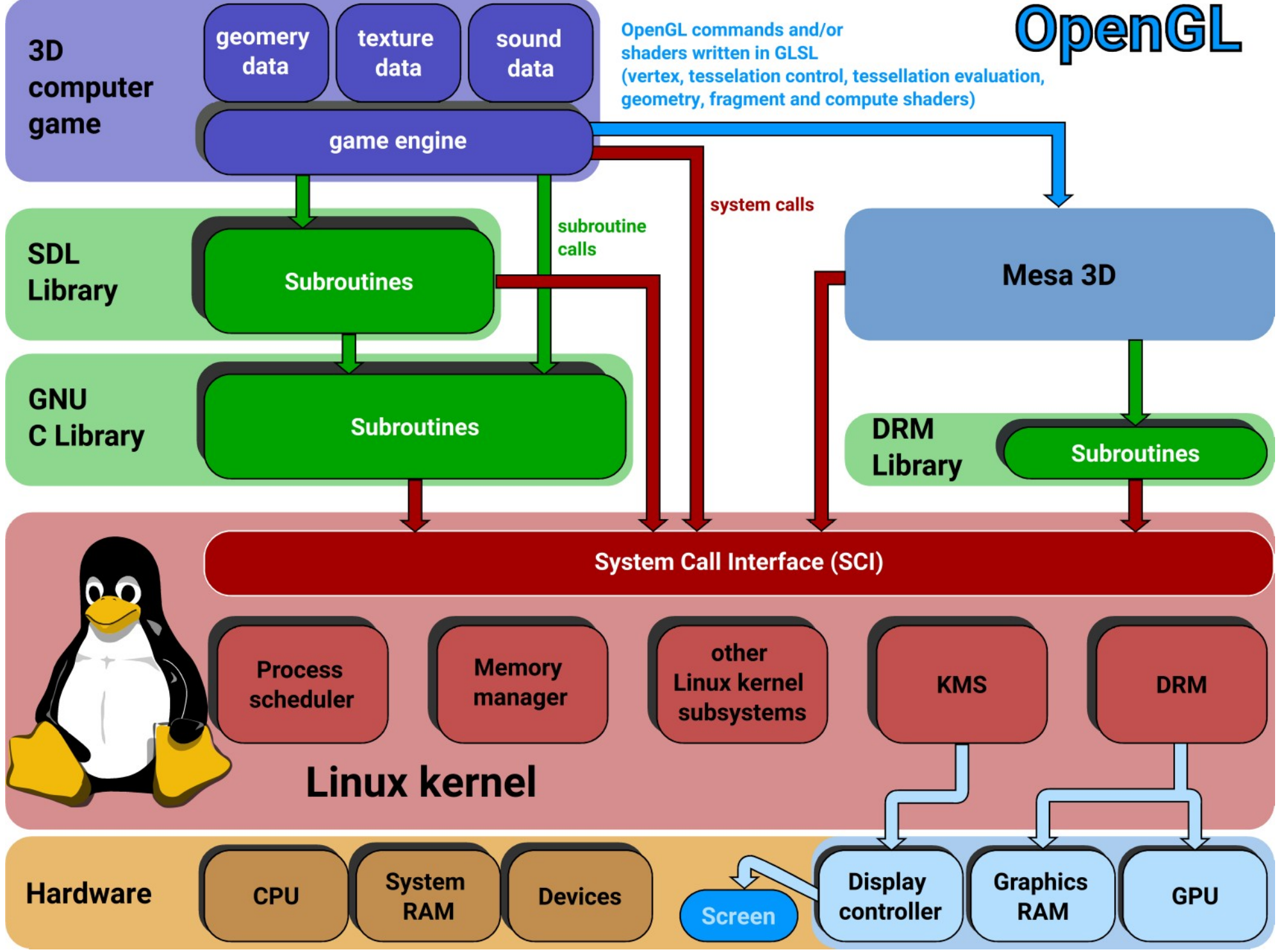
An Example

```c
#include <stdio.h>

int main()
{
        printf("Hello World!\n");
        return 0;
}
```

In the glibc

- /usr/include/asm-generic/unistd.h:

#define __NR_write 64
__SYSCALL(__NR_write, sys_write)

vDSO

> ldd hello1

      linux-vdso.so.1 (0x00007fffa07e2000)

      libc.so.6 => /lib64/libc.so.6 (0x00007fb892c48000)

      /lib64/ld-linux-x86-64.so.2 (0x00007fb893018000)

On the Kernel-Side

- http://lxr.free-electrons.com/source/fs/open.c#L1023

```
SYSCALL_DEFINE3(open,
    const char __user *, filename, int, flags, umode_t, mode)
{
    if (force_o_largefile())
        flags |= O_LARGEFILE;

    return do_sys_open(AT_FDCWD, filename, flags, mode);
}
```

What else you can do with syscalls

```
bootcd:/ # echo newuser::500:500:TestUser:/home/newuser:/bin/bash >>/etc/passwd
bash: /etc/passwd: Read-only file system
bootcd:/ # insmod translucency
Using /lib/modules/2.4.18-4GB/kernel/fs/translucency.o
bootcd:/ # echo "/ -> /var/tmp" > /proc/sys/translucency/0
bootcd:/ # echo newuser::500:500:TestUser:/home/newuser:/bin/bash >>/etc/passwd
bootcd:/ # tail -3 /etc/passwd
perforce:x:68:60:perfoce admin:/var/lib/perforce:/bin/false
nobody:x:65534:65534:nobody:/var/lib/nobody:/bin/bash
newuser::500:500:TestUser:/home/newuser:/bin/bash
bootcd:/ # echo > /proc/sys/translucency/0
bootcd:/ # rmmod translucency
bootcd:/ # tail -3 /etc/passwd
pop:x:67:100:pop admin:/var/lib/pop:/bin/false
perforce:x:68:60:perfoce admin:/var/lib/perforce:/bin/false
nobody:x:65534:65534:nobody:/var/lib/nobody:/bin/bash
bootcd:/ # ls -l /var/tmp/etc/
total 4
drwxr-xr-x    2 root     root            0 May 11 15:51 .
drwxrwxrwt    6 root     root            0 May 11 15:51 ..
-rw-r--r--    1 root     root         2852 May 11 15:51 passwd
bootcd:/ #
```

Thanks

- Questions?