User mode and Kernel Mode

1 GB

Stack
Heap
Data
Code

User Stack

Memory-mapped region for shared libraries (libc.so)

Heap

Read/Write segment (.data, .bss)

Read only segment (.init, .text, .rodata)

0x08048000

brk

3 GB
Mode bit

Control register.

if mode bit = 1 ⇒ Process is running in Kernel mode (or) Supervisor mode.

Kernel mode process

1. Can execute any instruction in the instruction set.

2. Can access any memory location in the system.

if mode bit = 0.

Process is in user mode.

1. Not allowed to execute privileged instructions, eg. change mode bit, initiate an I/O op.

2. Cannot access code or data in the kernel area of the address space.

⇒ Protection Fault.

user programs system calls Kernel code
User mode → Kernel mode

User process → Exception

Exception handler (Kernel mode)

Resume user process

Kernel mode address space

User mode address space

Exception
Context Switches

Kernel maintains a context for each process.

Context
1. Values in General purpose CPU registers, Floating point regs, PC, status registers
2. User's stack
3. Kernel's stack
4. Kernel data structures
   i) page table
   ii) file table (list of files open by the process)

Scheduler

Context Switch
1. Save the context of the current process.
2. Restore " " " some other process
3. Pass control to the newly restored process.
Flow of control in context switch

1. User system call
2. Kernel
3. Switch
4. User
5. Process A

Time line:
- disk interrupt
- return from read
- user code
- kernel code

User code