CS302 OS Lab10 - Report

Name: 刘仁杰
SID: 11911808

Answers

1.代码中通过何种方式从S mode 进入U mode?

1. 通过ebreak指令进入trap处理，再通过trap.c中的处理函数转发至do_execve()执行，
2. 在do_execve()函数中，调用load_icode()为用户进程分配新的资源，同时将进程中断帧的epc寄存器内写入了可执行文件的程序入口，将sstatus的SPP域置0，使得中断处理结束sret返回时返回至Umode，
3. 这样在终端结束返回调用sret时，会切换上下文把epc的值写 入pc，从而下一步执行可执行文件的程序；并且sret还会根据SPP的值，返回到原本的权限，此时SPP为0，所以会从S态切换到用户态。

2.代码中用户进程调用系统调用的过程是怎样的?

1. 在用户态，通过内联汇编进行ecall调用，产生trap进入S态进行异常处理，
2. 在trap.c中，ecall handler调用先将epc寄存器指向下一条指令，然后调用syscall()，
3. 然后在syscall()中，根据指令序号调用对应sys指令并传入参数。

3.代码中用户进程执行结束后发生了什么，模式是否切换?

1. 用户进程执行结束后，首先执行 lcr3(boot_cr3); 切换到内核的页表上（S mode），这样用户进程就只能在内核的虚拟地址空间上执行，如果被调用数为0，则开始进行资源回收的操作，释放内存，页表，vma和mm。
2. 然后设置进程的状态为 PROC_ZOMBIE，如果父进程在等待状态，将父进程wake up来回收内核栈和进程控制块。
3. 最后开启中断，执行schedule函数，选择新的进程执行。

4.进程如何变成僵尸进程?

进程的资源已经回收完毕，并且将进程的状态设置为PROC_ZOMBIE，而父进程并没有进入等待状态，该进程的内核栈和进程控制块还没有被回收，则此时该进程为僵尸进程。

5.load_icode()都做了什么?

将ELF格式的二进制文件中的context导入成当前进程的context。

1. 为当前进程创建一个新的mm，
2. 创建一个新的PDT，并且设置mm->pgdir为PDT的kernel虚拟地址，
3. 复制二进制文件里的text和data段，在进程的内存空间构建BSS，
4. 在内存中创建用户栈，
5. 设置进程的mm，cr3，并且将cr3寄存器设置为页表目录的物理地址，
6. 在用户态运行环境中创建trapframe。