CS334 Lab6 Report

代码中通过何种方式从S mode 进入U mode?

通过将 sstatus 的 SPP 域置零，使得中断处理结束 sret 返回时返回至用户态，U mode

代码中用户进程调用系统调用的过程是怎样的?

首先需要进行模式的切换，则需要通过内联汇编进行 `ecall` 环境调用，产生 trap 进入 S mode 进行异常处理，并且在 `trap` 中实现系统调用的执行。即在 `trap.c` 当中转发系统调用

代码中用户进程执行结束后发生了什么，模式是否切换?

在进程执行完工作之后，会退出进程并且释放资源。这是通过调用 `do_exit()` 实现的。

如果是内核线程就不需要回收空间;

如果是用户进程就需要开始回收空间。

之后设置进程的状态为 PROC_ZOMBIE，等待父进程来回收资源，回收内核栈和进程控制块。

如果当前进程的父进程处于等待子进程的状态，则唤醒父进程来进行子进程资源的回收。

如果进程还有子进程，就指向第一个孩子，把后面的孩子全部置为空，将孩子过继给内核线程。将回收资源的任务交给过继后的父进程。

之后开启中断，执行 `schedule` 函数，选择新的进程执行。

模式会从 U mode 切换到 S mode

进程如何变成僵尸进程?

父进程没有调用 `wait` 函数，且父进程会在子进程结束之前结束，之后子进程会因为结束后没有被回收而变成僵尸进程。子进程的控制块并没有从两个进程队列 `proc_list` 和 `hash_list` 中删除，且子进程的内核堆栈和进程控制块也没有被释放。即资源没有被完全消除，这样的进程就会变成僵尸进程。