



深圳大学
Shenzhen University

操作系统

操作系统大作业： part I-6

谭舜泉

计算机与软件学院

大作业Part I

- 大作业**Part I** 由六部分组成。六部分均为阅读xv6中文文档，理解对应的xv6源代码，并回答大作业中提出的代码理解问题。
 1. （第二周）第0章：操作系统接口；
 2. （第四周）第1章：第一个进程；
 3. （第六周）附录A/B：PC硬件及引导加载器；
 4. （第八周）第2章：页表；
 5. （第十周）第4章：锁；
 6. （第十二周）第3章：陷入、中断和驱动程序。



大作业Part I

- 注意上半学期的大作业分为两部分汇总提交。
- 其中**1-3**提交一份实验报告，而**4-6**提交另一份实验报告。



实验报告

- 实验报告要求使用深大实验报告模板填写。
- 允许两至三人组成一个小组，撰写实验报告。
- 请按照实验要求，完成实验并撰写实验报告。
把实验报告电子版上传到**BLACKBOARD**。本实验分组完成。每个实验小组完成一份实验报告即可。但要求小组中每个成员都把实验报告的副本上传到**BLACKBOARD**，并注明同组成员的名字和学号。



第3章：陷入，中断和驱动程序

- 系统调用，异常和中断都由内核管理，而不是进程。
- 中断终止正常的处理器循环然后开始执行中断处理程序中的代码。在开始中断处理程序之前，处理器保存寄存器，这样在操作系统从中断中返回时就可以恢复他们。
- 处理器需要在用户模式和内核模式之间切换。
- 陷入(系统调用)由在 CPU 上运行的当前进程导致。
- 中断是由设备导致的，可能与当前进程毫无关系。



第3章：陷入，中断和驱动程序

■ X86 的保护机制

- x86 有四个特权级，从 0（特权最高）编号到 3（特权最低）。大多数的操作系统都使用两个特权级，0 和 3，他们被称为内核模式和用户模式。
- 一个程序要在 x86 上进行一个系统调用/中断，需要调用 `int n` 指令，x86 允许 256 个不同的中断。
- 中断 0-31：软件异常，(如除 0 错误和访问非法的内存页)
- 中断号 32-63：硬件中断；
- 中断号 64：系统调用的中断号。（`traps.h`）
- `#define T_IRQ0 32`（Interrupt Request 硬件中断请求）



第3章：陷入，中断和驱动程序

- 当陷入发生时，如果处理器在用户模式下运行，它会从任务段描述符中加载 `%esp` 和 `%ss`，把老的 `%ss` 和 `%esp` 压入新的栈中。如果处理器在内核模式下运行，上面的事件就不会发生。
- 而后，处理器从相应 IDT 表项中加载新的 `%eip` 和 `%cs`。
- 相继压入寄存器后，内核栈上压入一个 `trapframe`（中断帧）结构体。
- 中断帧包含了所有处理器从当前进程的内核态恢复到用户态需要的信息，所以处理器可以恰如中断开始时那样继续执行。



第3章：陷入， 中断和驱动程序

- 建立中断帧后，调用 C 函数 `trap` (`trap.c`)。
- `trap` 查看硬件中断号 `tf->trapno`来判断自己为什么被调用以及应该做些什么。如果中断是 **T_SYSCALL**，`trap` 调用系统调用处理程序 **syscall**。



第3章：代码理解问题

- 在zombie.c中，sleep(5); (L12)。sleep是一个系统调用。请分析代码，阐述在代码中，这一系统调用如何一步步的转化为一个对核心函数sleep (proc.c / L343) 的调用？
- sleep(5)代表zombie进程总共睡眠多少毫秒？请通过代码分析给出你的答案。



代码理解问题

- 这些问题，如果不能理解的话也不用担心。我将在两周后的课堂上（在实验报告提交前）给予解答。

