Jared Strand
CS 460 Diagram
LAB 5 PreWork

(4). Draw a diagram to show the control flow of P1, which executes:

     int pid = getpid();   in Umode space

Required steps: YOU explain how each step leads to the next:

SETUP AND STEPS:
The user calls ugetpid() → we call int pid = getpid(); →

This calls syscall(0,0,0,0) to have kernel mode get the pid →

In assembly file us.s we call syscall which saves the local stack of user with stmfd then calls swi #0 →

swi #0 generates a software interrupt that sends us into svc_entry after checking the vector table for who caused interrupt →

Our vector table points at the address of svc_entry which is then set to run →

In svc_entry we sve lr stack of svc mode, then save current ksp, change to sys mode, then change to svc mode by moving cpsr register, re-enable interrupts →

Once be branch link to svc_handler we go into C code mode to execute kgetpid() →

kgetpid() returns running→pid as its return value stored on it’s stack →

Next we enter goUmode, set r0 to return from kgetpid(), restore the stacks and switch back to umode with ldmfd sp!, {r0-r12, pc}^

We have now completed our syscall and returned to user mode.