CPSC 3220 – Quiz #2 January 31, 2018 Name: _**Answer Key**_

1. (2 points) When a user process is interrupted or causes a processor exception, the x86 hardware switches the stack pointer to a kernel stack, before saving the current process state. Explain why.

The user stack pointer may be corrupted. Switching to the kernel stack ensures that heir is a valid memory region to store the process state.

The kernel stack is inaccessible to the user and is protected. The kernel is able to store state information safely.

2. (2 points) For the "Hello World!" program, we mention that the kernel must copy the string from the user program to screen memory. Why must the screen's buffer memory be protected?

A malicious/flawed application could insert bad code into the protected memory. The O/S could then execute this bad code causing a system crash or a malicious app could gain control of the O/S.

3. (2 points) Explain the steps that an operating system goes through when the CPU receives an interrupt.

Several steps occur simultaneous (atomically):

Save the PC, IR, and PSR (Save the process state)

Switch to Kernel Mode

Disable/Defer future interrupts.

Load new PC from the Interrupt Vector Table

Continued on Back

4. (2points) How does an O/S keep user application from directly access hardware without controls?

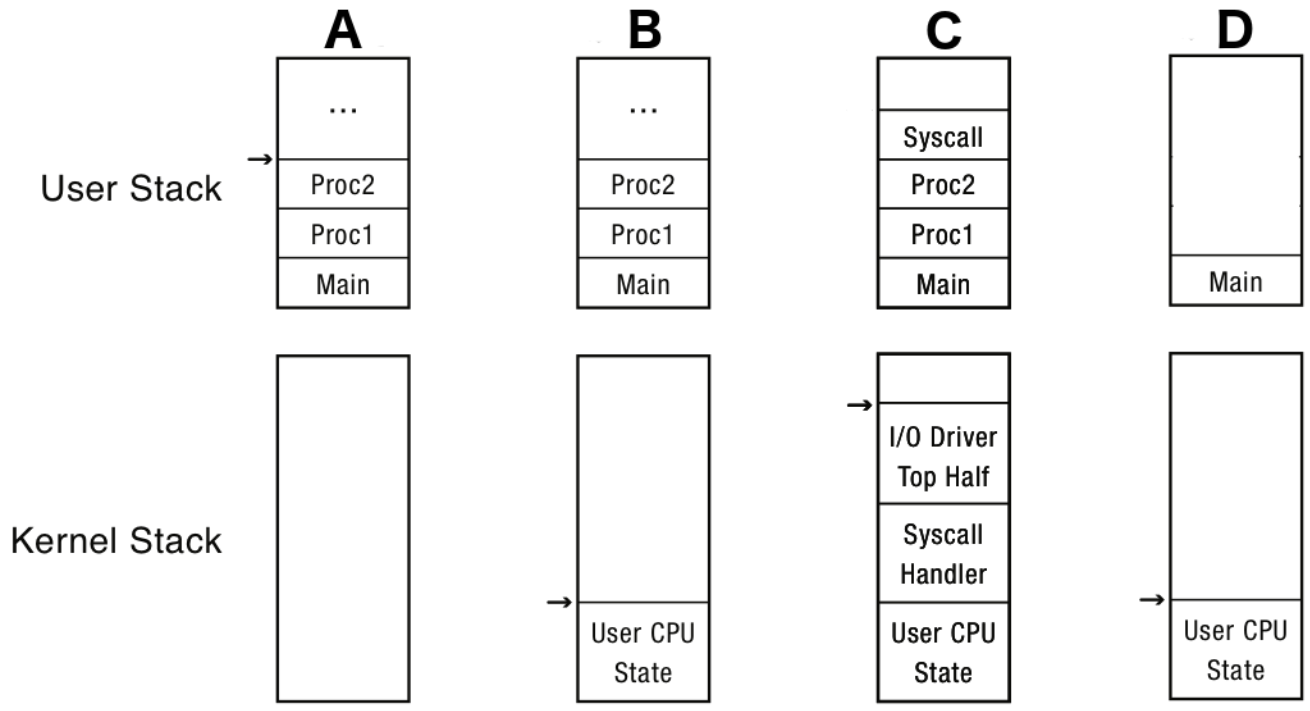
The O/S implements protection through Dual-Mode Operation: Kernel/User.

Instructions that access hardware directly are considered privileged instructions.

User Mode cannot execute privileged instruction.

5. (4 points) Interrupt Stacks

For each description of a process, match the matching stack diagram.



__D__ New Process

__A__ Running Process

__B__ Ready Process

__C__ Waiting Process