– the thread context is changed so that:

* the program counter is set to a fixed (determined by the hardware) memory address, which is within the kernel’s address space

* the stack pointer is pointed at a stack in the kernel’s address space

**System Call Execution and Return**

- Once a system call occurs, the calling thread will be executing a system call handler, which is part of the kernel, in system mode.

- The kernel’s handler determines which service the calling process wanted, and performs that service.

- When the kernel is finished, it returns from the system call. This means:
  – restore the key parts of the thread context that were saved when the system call was made
  – switch the processor back to unprivileged (user) execution mode

- Now the thread is executing the calling process’ program again, picking up where it left off when it made the system call.