Problem Set 2.1

CS 311

Due Feb. 10, 2014

Due at the beginning of class in hardcopy.

1. Processes can interrupt each other via a signal mechanism. There are various types of signals that one process can send to another (see the man page for signal for details). A process can have the operating system install signal handlers that are invoked when signals are received by the process. Signals are the software equivalent of hardware interrupts. CPUs enter kernel mode when they receive interrupts, just as they do when they execute a syscall instruction. For this question, let's assume that the CPU enters kernel mode when a process receives a signal.

   (a) How could a malicious user exploit this transition to the CPU's kernel mode caused by the receipt of a signal?

   (b) How can the operating system prevent this exploitation from happening?

2. What are the two models of interprocess communication? What are the strengths and weaknesses of the two models?