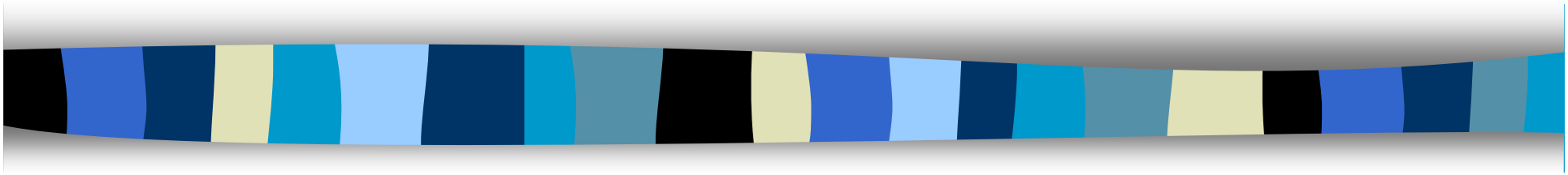
Computer Security
CS 426
Lecture 7



Operating System Security Basics

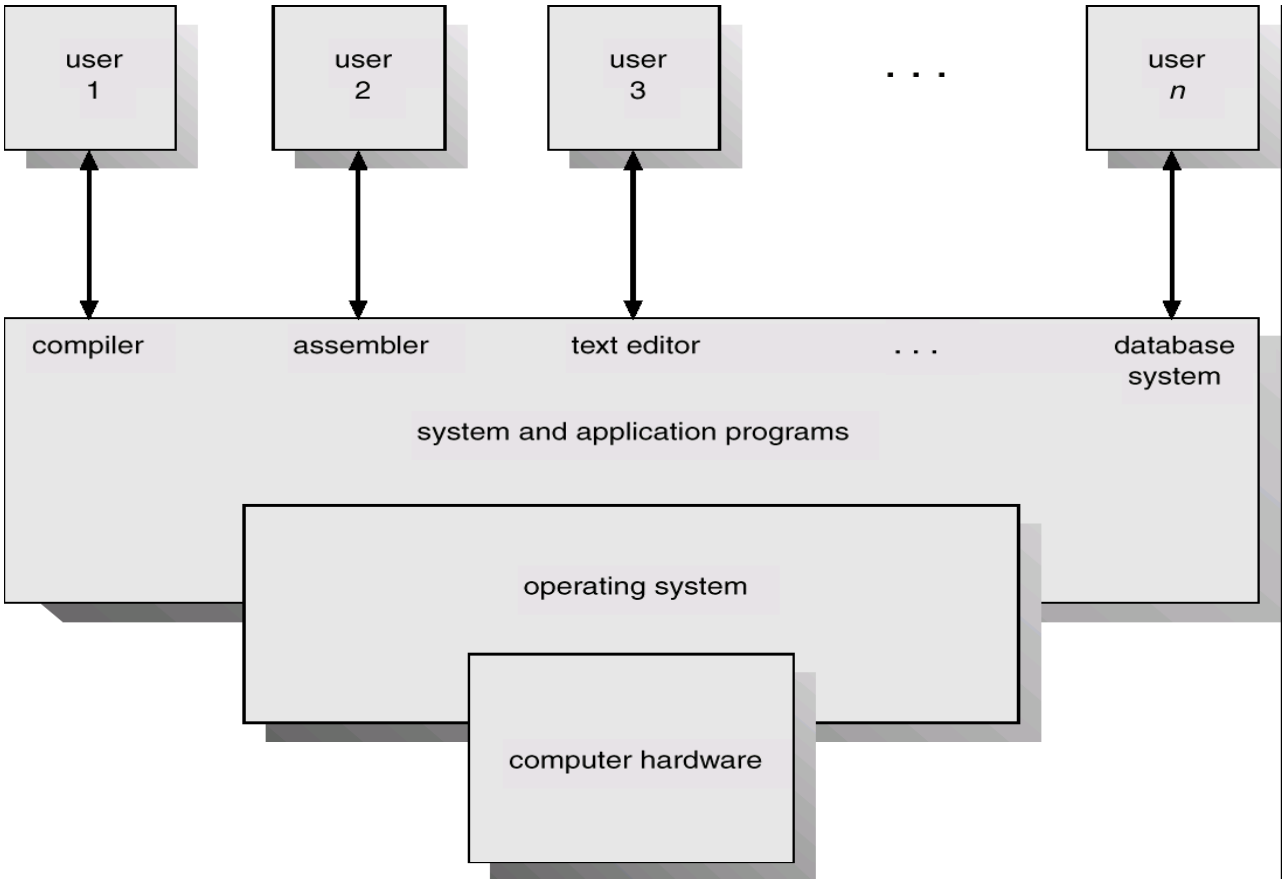
Announcements

- Homework 1 due on Sept 10
- Will have first quiz near the end of lecture
- Form a two-person team for the projects, and send team member info and preferred login for the team to the TA

Computer System Components

- Hardware
  - Provides basic computing resources (CPU, memory, I/O devices).
- Operating system
  - Controls and coordinates the use of the hardware among the various application programs.
- Applications programs
  - Define the ways in which the system resources are used to solve the computing problems of the users.
- Users
  - E.g., people, machines, other computers.

Abstract View of System Components



What Security Goals Does Operating System Provide?

- Goal 1: enabling multiple users securely share a computer
  - Separation and sharing of processes, memory, files, devices, etc.
- What do C, I, A, mean here?
- What is the threat model?
- How to achieve the security goals?
  - Memory protection
  - Processor modes
  - User authentication
  - File access control

What Security Goals Does Operating System Provide?

- Goal 2: ensure secure operation in networked environment
- What do C, I, A mean here?
- What is the threat model?
- How to achieve the security goals?
  - Authentication
  - Access Control
  - Secure Communication (using cryptography)
  - Logging & Auditing
  - Intrusion Prevention and Detection
  - Recovery

Security is About Controlled Sharing

- Ensure separation
  - Physical
  - Temporal
  - Logical
  - Cryptographical
- OS also need to ensure sharing
- Reconcile sharing and separation

Memory Protection: access control to memory

- Ensures that one user's process cannot access other's memory
  - fence
  - relocation
  - base/bounds register
  - segmentation
  - paging
  - …
- Operating system and user processes need to have different privileges

CPU Modes (a.k.a. processor modes or privilege

- System mode (privileged mode, master mode, supervisor mode, kernel mode)
  - Can execute any instruction
  - Can access any memory locations, e.g., accessing hardware devices,
  - Can enable and disable interrupts,
  - Can change privileged processor state,
  - Can access memory management units,
  - Can modify registers for various descriptor tables .

Reading: http://en.wikipedia.org/wiki/CPU_modes

User Mode

- User mode
  - Access to memory is limited,
  - Cannot execute some instructions
  - Cannot disable interrupts,
  - Cannot change arbitrary processor state,
  - Cannot access memory management units
- Transition from user mode to system mode must be done through well defined call gates (system calls)

Reading: http://en.wikipedia.org/wiki/CPU_modes

System Calls

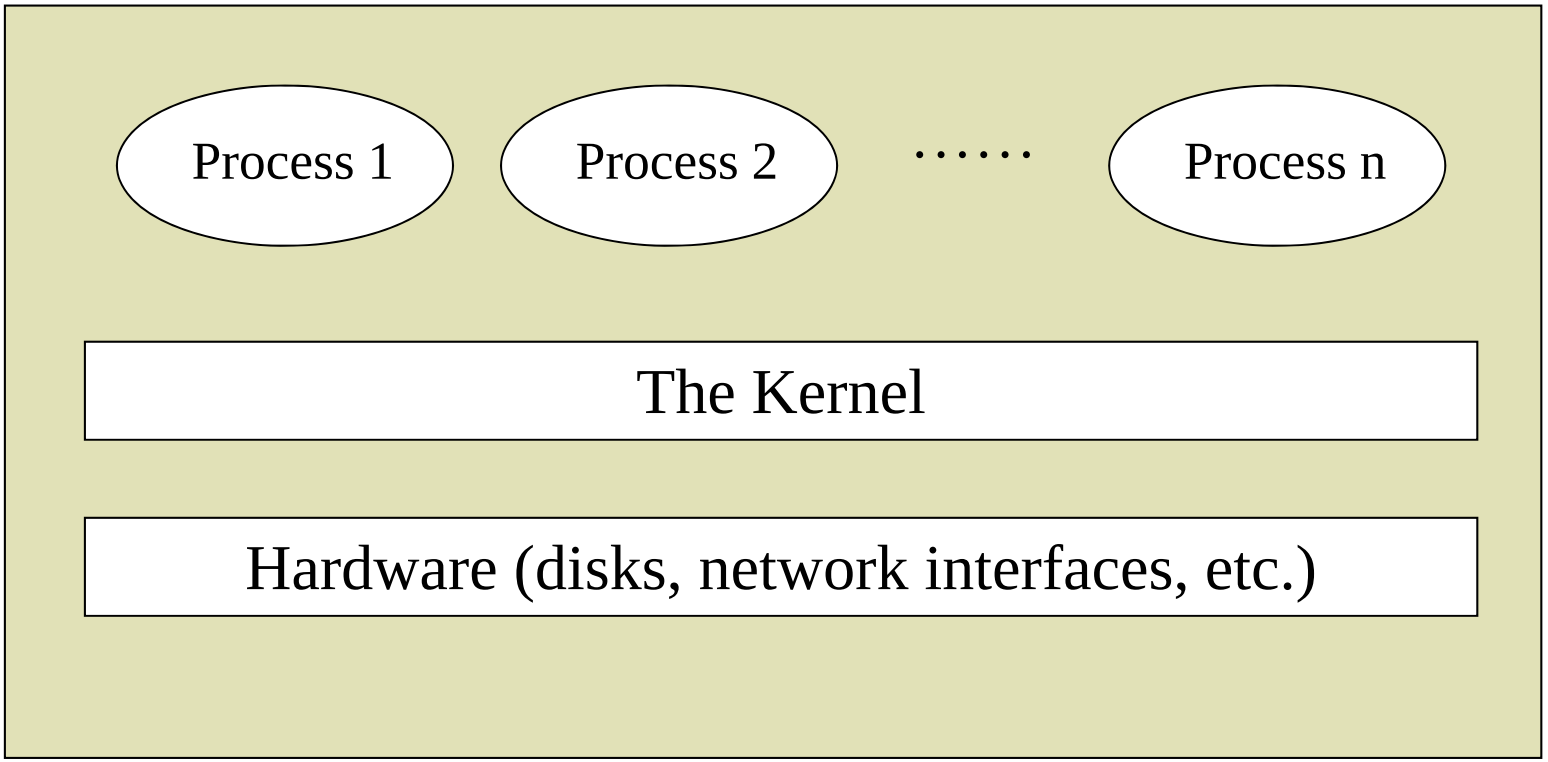
- Guarded gates from user mode (space, land) into kernel mode (space, land)
  - use a special CPU instruction (often an interruption), transfers control to predefined entry point in more privileged code; allows the more privileged code to specify where it will be entered as well as important processor state at the time of entry.
  - the higher privileged code, by examining processor state set by the less privileged code and/or its stack, determines what is being requested and whether to allow it.

http://en.wikipedia.org/wiki/System_call

Kernel space vs User space

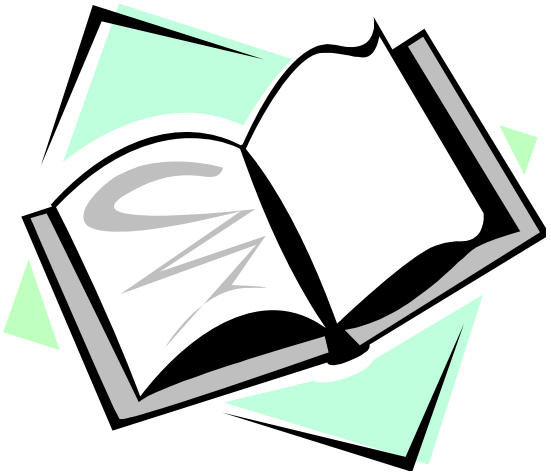
- Part of the OS runs in the kernel model
  - known as the OS kernel
- Other parts of the OS run in the user mode, including service programs (daemon programs), user applications, etc.
  - they run as processes
  - they form the user space (or the user land)
- Difference between kernel mode and processes running as root (or superuser, administrator)

High-level View of Kernel Space vs. User Space



Readings for This Lecture

- Wikipedia
  - CPU modes
  - System call



Coming Attractions …

- User Authentication