Announcements/Reminders

- Handout from Friday available from the web site
- Lab 0 due Wednesday
- checkhw and java/javac are working on the EdLab machines
An operating system is the interface between the user and the architecture.

- History lesson in change.
- OS reacts to changes in hardware, and can motivate changes.
Today: OS and Computer Architecture

- Basic OS Functionality
- Basic Architecture reminder
- What the OS can do is dictated in part by the architecture.
- Architectural support can greatly simplify or complicate the OS.
Modern Operating System Functionality

1. **Concurrency**: Doing many things simultaneously (I/O, processing, multiple programs, etc.)
   - Several users work at the same time as if each has a private machine
   - Threads (unit of OS control) - one thread on the CPU at a time, but many threads active concurrently

2. **I/O devices**: Let the CPU work while a slow I/O device is working

3. **Memory management**: OS coordinates allocation of memory and moving data between disk and main memory.

4. **Files**: OS coordinates how disk space is used to store multiple files

5. **Distributed systems & networks**: Allow a group of workstations to work together on distributed hardware
Summary of Operating System Metaphors

- **OS as juggler**: providing the illusion of a dedicated machine with infinite memory and CPU.

- **OS as government**: protecting users from each other, allocating resources efficiently and fairly, and providing secure and safe communication.

- **OS as complex system**: keeping OS design and implementation as simple as possible is the key to getting the OS to work.

- **OS as history teacher**: learning from past to predict the future, i.e., OS design trade-offs change with technology.
Generic Computer Architecture

- CPU
- Disk Controller
- Printer Controller
- Tape Drive Controller
- Memory Controller
- Memory
- Disk
- Disk
- Printer
- Tape Drive

System Bus
Generic Computer Architecture (cont)

- CPU: the processor that performs the actual computation
- I/O devices: terminal, disks, video board, printer, etc.
- Memory: RAM containing data and programs used by the CPU
- System bus: communication medium between CPU, memory, and peripherals
# Architectural Features Motivated by OS Services

<table>
<thead>
<tr>
<th>OS Service</th>
<th>Hardware Support</th>
</tr>
</thead>
<tbody>
<tr>
<td>Protection</td>
<td>Kernel/User mode</td>
</tr>
<tr>
<td></td>
<td>Protected Instructions</td>
</tr>
<tr>
<td></td>
<td>Base and Limit Registers</td>
</tr>
<tr>
<td></td>
<td>Interrupt Vectors</td>
</tr>
<tr>
<td>Interrupts</td>
<td>Trap instructions and trap vectors</td>
</tr>
<tr>
<td>System calls</td>
<td>Interrupts or Memory-Mapping</td>
</tr>
<tr>
<td>I/O</td>
<td>Timer</td>
</tr>
<tr>
<td>Scheduling, error recovery, billing</td>
<td>Atomic instructions</td>
</tr>
<tr>
<td>Synchronization</td>
<td>Translation look-aside buffers</td>
</tr>
<tr>
<td>Virtual memory</td>
<td></td>
</tr>
</tbody>
</table>
Protection

Kernel mode vs. User mode: To protect the system from aberrant users and processes, some instructions are restricted to use only by the OS. Users may not:

- address I/O directly
- use instructions that manipulate the state of memory (page table pointers, TLB load, etc.)
- set the mode bits that determine user or kernel mode
- disable and enable interrupts
- halt the machine

but in kernel mode, the OS can do all these things.
Protection (cont)

The hardware must support at least kernel and user mode.

- A status bit in a protected processor register indicates the mode.
- Protected instructions can only be executed in kernel mode.
- Multics: support for a hierarchy of kernel modes (components of the kernel were protected from each other).
Crossing Protection Boundaries

OS Kernel

Trap Handler → System Service Routine

Trap to Kernel Mode

Kernel Mode

User Mode

System Call

User Programs

Process

User Programs
Crossing Protection Boundaries (cont)

**System call:** OS procedure that executes privileged instructions (e.g., I/O)

- Causes a trap, which vectors (jumps) to the trap handler in the OS kernel.
- The trap handler uses an ID parameter from the system call to jump to the appropriate handler (I/O, Terminal, etc.).
- The handler saves caller’s state (PC, mode bit) so it can restore control to the user process.
- The architecture must permit the OS to verify the caller’s parameters.
- The architecture must also provide a way to return to user mode when finished.
Memory Protection

- Architecture must provide support so that the OS can:
  - protect user programs from each other, and
  - protect the OS from user programs.

- The simplest technique is to use base and limit registers.

- Base and limit registers are loaded by the OS before starting a program.

- The CPU checks each user reference (instruction and data addresses), ensuring that it falls between the base and limit register values.
Memory Protection (cont)

Memory

- Program A
- Program B
- Program C

Base Register
Limit Register
Traps

- **Traps**: special conditions detected by the architecture
  - Examples: page fault, write to a read-only page, overflow, systems call

- On detecting a trap, the hardware:
  - Saves the state of the process (PC, stack, etc.)
  - Transfers control to appropriate trap handler (OS routine)
    * The CPU indexes the memory-mapped trap vector with the trap number,
    * Jumps to the address given in the vector, and
    * Starts to execute at that address.
    * On completion, the OS resumes execution of the process.
Traps

Trap Vector:

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>0:</td>
<td>0x00080000</td>
</tr>
<tr>
<td>1:</td>
<td>0x00100000</td>
</tr>
<tr>
<td>2:</td>
<td>0x00100480</td>
</tr>
<tr>
<td>3:</td>
<td>0x00123010</td>
</tr>
<tr>
<td>...</td>
<td>...</td>
</tr>
</tbody>
</table>

- Modern OS use Virtual Memory traps for many functions: debugging, distributed VM, garbage collection, copy-on-write, etc.

- Traps are a performance optimization. A less efficient solution is to insert extra instructions into the code everywhere a special condition could arise.
I/O Control

- Each I/O device has a little processor inside it that enables it to run autonomously.
- CPU issues commands to I/O devices, and continues
- When the I/O device completes the command, it issues an interrupt
- CPU stops whatever it was doing and the OS processes the I/O device’s interrupt
Memory-Mapped I/O

- Enables direct access to I/O controller (vs. being required to move the I/O code and data into memory)
- PCs reserve a part of the memory and put the device manager in that memory (e.g., all the bits for a video frame for a video controller).
- Access to the device then becomes almost as fast and convenient as writing the data directly into memory.
- Before memory-mapped I/O: the instruction set provided specific operations for I/O. Why do we not do this very often now?
Interrupt based asynchronous I/O

- Device controller has its own small processor which executes asynchronously with the main CPU.

- Device puts an interrupt signal on the bus when it is finished.

- CPU takes an interrupt.

1. Save critical CPU state (hardware state),
2. Disable interrupts,
3. Save state that interrupt handler will modify (software state)
4. Invoke interrupt handler using the in-memory Interrupt Vector
5. Restore software state
6. Enable interrupts
7. Restore hardware state, and continue execution of interrupted process
Direct Memory Access (DMA)

- Purpose: Large I/O operations
- Processor first configures the device for the transfer
- Processor then grants (or shares) control of the system bus to the device
- Device generates interrupt on completion of the transfer
- Useful for ???
Direct Memory Access (DMA)

Useful for ???

- Video I/O
- Audio I/O
- Disk operations
Timer & Atomic Instructions

Timer

- Time of Day
- Accounting and billing
- CPU protected from being hogged using timer interrupts that occur at say every 100 microsecond.
- At each timer interrupt, the CPU chooses a new process to execute.
- At every change in process, the operating system performs a context switch
Synchronization

- Interrupts interfere with executing processes.
- OS must be able to synchronize cooperating, concurrent processes.

⇒ Architecture must provide a guarantee that short sequences of instructions (e.g., read-modify-write) execute atomically. Two solutions:

1. Architecture mechanism to disable interrupts before sequence, execute sequence, enable interrupts again.

2. A special instruction that executes atomically (e.g., test&set).
Virtual Memory

- Virtual memory allows users to run programs without loading the entire program in memory at once.

- Instead, pieces of the program are loaded as they are needed.

- The OS must keep track of which pieces are in which parts of physical memory and which pieces are on disk.

- In order for pieces of the program to be located and loaded without causing a major disruption to the program, the hardware provides a translation look-aside buffer to speed the lookup.
Summary

Keep your architecture book on hand.

OS provides an interface to the architecture, but also requires some additional functionality from the architecture.

⇒ The OS and hardware combine to provide many useful and important features.
Next Time

Wednesday:

- Read chapter 3
- Lab 0 due