Past Class:-
Trajectory of Computer Security Research
- is moving towards Finer grained and more dynamic control sharing
  Mash ups (Google Map and Craigslist)

This Class
- Hardware and OS basics

How to enforce security in system:
Allow restricted the access to RAM
- Segment Registers gives a higher range
- TLB - Translation Look Aside Buffer

<table>
<thead>
<tr>
<th>Virtual</th>
<th>Physical</th>
</tr>
</thead>
<tbody>
<tr>
<td>20 bytes</td>
<td>maps to</td>
</tr>
<tr>
<td>12</td>
<td>6</td>
</tr>
<tr>
<td>13</td>
<td>5</td>
</tr>
<tr>
<td>14</td>
<td>6</td>
</tr>
</tbody>
</table>

e.g.
If someone application for (13,107), it would get mapped to (5,107). But if it asks for (27,45), page fault occurs. So essentially, no mapping in TLB result in PF.

Computer Boot up steps:-
- OS has access to all the memory via physical address. In X86 setup, CPU is in real
mode and bypasses the TLB
- OS adds entries for itself in TLB
- System switches to protection mode
- New entries for applications are created in TLB

TLB manipulation is privileged only to OS

Privilege Register
- We add a register in HW that contains a bit to indicate the state of TCB
  - Priv 1 means TLB/Interrupt instruction access is allowed
  - Priv 0 means TLB/Interrupt instruction access is denied
- Application cannot change the Priv
- Migration of Priv from 0 to 1 is forbidden

Running an Application (say A)
1. Clear old entries from TLB
2. Add application A’s entries to TLB
3. Set Clock to interrupt in 100ms
4. Set Priv to 0
5. Jump to App A

Imp Points
- Interrupt restores Priv 1
- OS Stub entries remain in TLB for reloading OS when we get an interrupt. These stub entries are read only

Goals of Security
- Availability:- Clock ensures that no process takes the CPU infinitely
- Integrity:- Read only OS pages
- Confidentiality:- The TLB never contains the OS pages that are confidential.

Alternative TLB design

<table>
<thead>
<tr>
<th>PID</th>
<th>OPS</th>
<th>VIR</th>
<th>PHY</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>X</td>
<td>12</td>
<td>0</td>
</tr>
<tr>
<td>1</td>
<td>RW</td>
<td>13</td>
<td>1</td>
</tr>
<tr>
<td>1</td>
<td>RW</td>
<td>12</td>
<td>2</td>
</tr>
</tbody>
</table>

- What if we replace the Priv Bit by PID
- Better Design
  - No need to load / unload app code
  - If PID is 0, OS works. Else, App mode