http://www.cs.sunysb.edu/~r+tjohnso/
teaching/cse509-sp07

**Reviews**: r+tjohnso + 509r @ cs.sunysb.edu  
**All else**: r+tjohnso @ cs.sunysb.edu

Thursday's reading is now fixed

**Rule**: Least shared mechanism
- code
  - downside
    - less auditing of code
    - expertise required
  - upside
    - less trust
    - limit damage
- data

**Rule**: Psychological Acceptability
Unused security is unused security

![Diagram showing network architecture with firewall (FW) and Internet connection.}]
Early security research: Isolate

Current security research: Controlled sharing

No sharing

What does this achieve?
- confidentiality
- integrity
- availability

Assumptions
- operator is infallible
- operator is not malicious
- no network
- computer has no state
- enough paper
- electricity
- room is sealed
- denial of service
If Ring == 0: can execute any instruction
Else: can only execute “normal” instructions

TLB - maps pages

<table>
<thead>
<tr>
<th>virt</th>
<th>phys</th>
<th>perm</th>
</tr>
</thead>
<tbody>
<tr>
<td>1234</td>
<td>0012</td>
<td>R</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

New instructions
load TLB should not be available to untrusted programs
clear TLB
drop Priv “normal” instruction
Syscall “normal” instruction
  · Ring := 0
  · Jumps to IHA
write IHA privileged
On system boot
  * CPU is in Ring0
  * loads and executes OS

On OS Kernel boot
  * sets IHA

To run program, OS Kernel
  * load program into some physical pages
  * places entries in TLB
  * drop Priv
  * jump to program

**Goals**

- memory insulation
  * confidentiality
  * integrity
  * availability?

- device isolation
  * built on memory protection

- CPU insulation
  * confidentiality + integrity (save/restore full CPU state)
  * availability (Timer)

Have we achieved "full" isolation? **No.**

- timing leaks
- memory usage leaks

Non-interference
Very inefficient
Sharing
- OS “sendmsg” command
  - destination
  - data
- OS will prepend unforgeable src address to your message
- another syscall command: recvmsg

Homework Grading System

Student App

submit homework

student app gets grades

get class average

Professor App

get my grades

get class average

Student trusts Professor
Student and Professor trust OS