

Human Factors

Unusable Security = Unused Security

example: Crypto

successes - easy to use

SSH - password encryption important

SSL - money

Security

• How important is it to secure

• standards affect usability

failures

e-mail - medium difficulty, ^{mostly} non-se

WEP (Wired Equivalency Protocol)

Security can also get in the way!

Example:

Corporate Network users



Firewalls direct web traffic, but if System Admin blocks

most internet pages, users become frustrated & find another route.

Trend in Computer Security - Greater sharing

- Everyone gets separate computers (no network)



Multiprogramming environment (UNIX)



RPC/IPC (users share files with each other)



Mobile Code problems with these ideas.

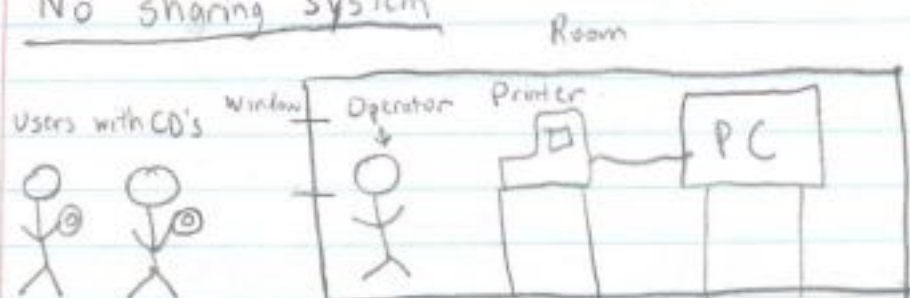


???

Researching new ideas

Nowadays, current world relies on Multiprogramming & RPC/IPC

No sharing system



Running System

- ① User gives disk to operator
 - ② Operator inserts disk & turns on computer
 - ③ Computer runs for one hour
 - ④ Operator gives any print out to user
 - ⑤ Operator turns off computer.
- ↻
back to step 1

- Disks handed to operator could be dangerous
- Confidential because no input/output is shared

- ### Goals
- Confidentiality ✓
 - Integrity ✓
 - Availability ✓

Trust (Integrity)

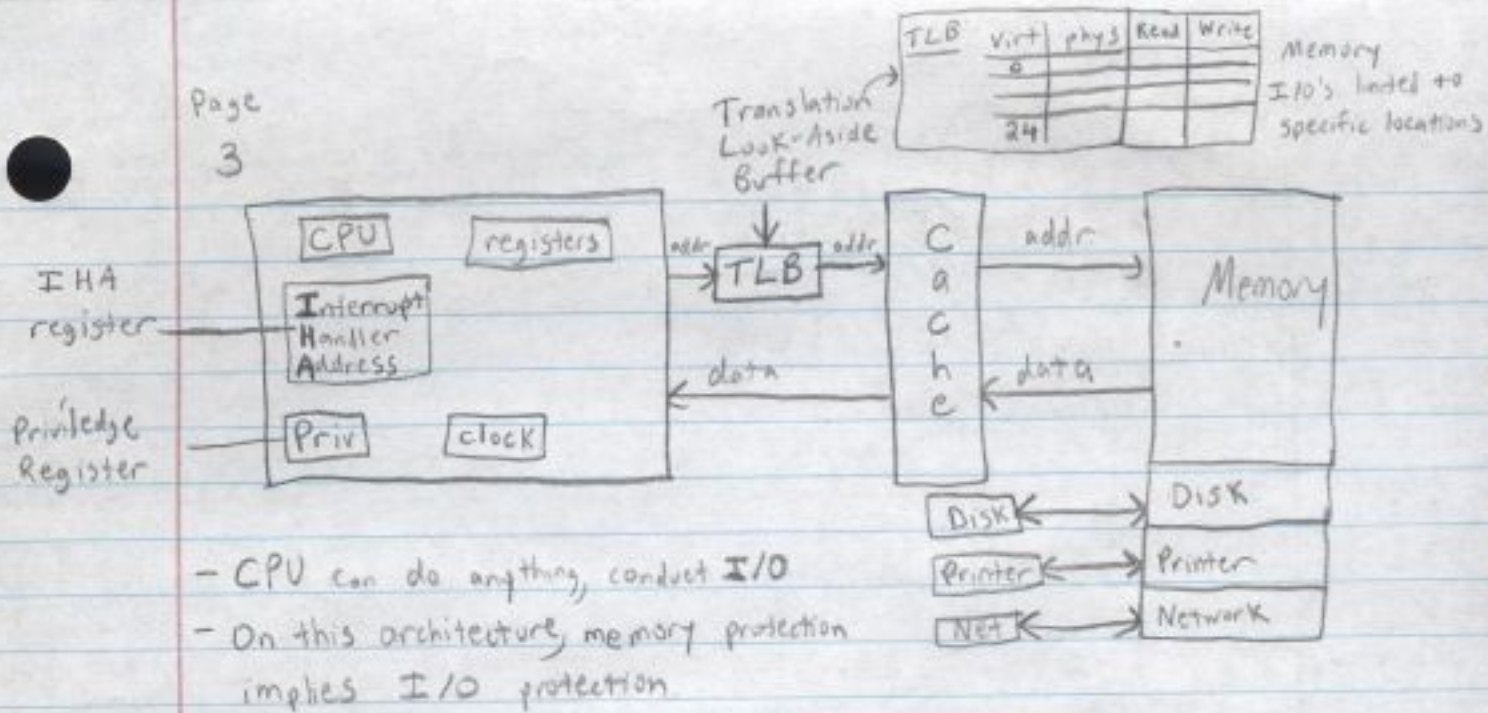
- Operator must be honest & diligent
- Power off is total reset
- Room is sealed
- Stolen disks / user authentication
- Queueing policy (for availability)
- Availability of operator

Disadvantage

Very wasteful/inefficient
ex: 10 minute program in one hour timeslot

Virtual Machines

Goal: Introduce a supervisor that limits programs.



Instructions

- Load/store architecture Reg ↔ Mem
- Register to register computation
- Flush cache
- Load/store IHA
- Loading/storing for TLB, TLB does no good for security since program can alter it.

Thus, add Privilege Register. with values 0=yes 1=no

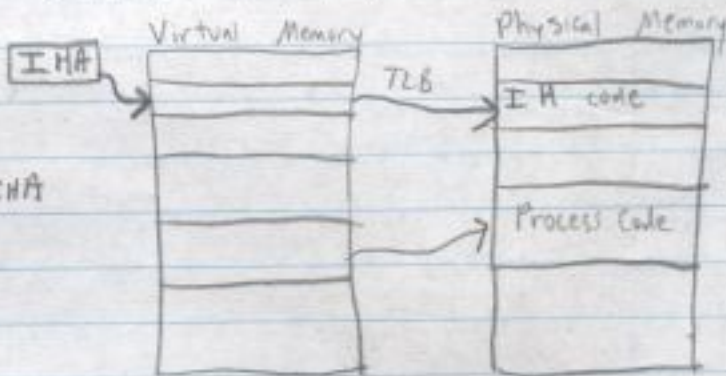
- Priv bit goes to 'yes' on an interrupt

OS process uses IHA, so protection needed.

	Yes	No
Load TLB	✓	X
Read TLB	✓	X (for virtual machine)
Load IHA	✓	X
Read IHA	✓	X

So, the OS:

- Loads page of IH into TLB read-only (address 0)
- Loads addr of IH into IHA
- Load process TLB entries
- Turns off privilege bit
- Jumps to program
- Nothing else lives on IH page
- Clear registers
- Clear memory pages of process



Availability not listed. Scheduler needed (clock) to prevent one program from running too long.

Linux Setup

Process Virtual Memory

