Human Factors

**Unusable security = Unused security**
- example: Crypto
- **successes - easy to use**
- **SSL - password encryption important**
- **SSL - money**

**Security**
- *How important is it to secure?*
- *standards affect usability*
- **failures**
- **e-mail - medium difficulty, non-se**
- **WEP (Wired Equivalency Protocol)**

Security can also get in the way!

Example:

- Corporate Network Users
  - Firewall
  - Internet
  - Modem

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 printout to user
5. Operator turns off computer.

- 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

Goals: Introduce a supervisor that limits programs.
CPU can do anything, conduct I/O
On this architecture, memory protection implies I/O protection

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.

So, the OS:
- Loads page of IHA into TLB read-only (address 0)
- Loads addr of IHA into IHA
- Load process TLB entries
- Turns off privilege bit
- Jumps to program
- Nothing else lives on IHA 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

4GB

Interrupt

3GB

1GB ← Kernel code & data

Process code & data