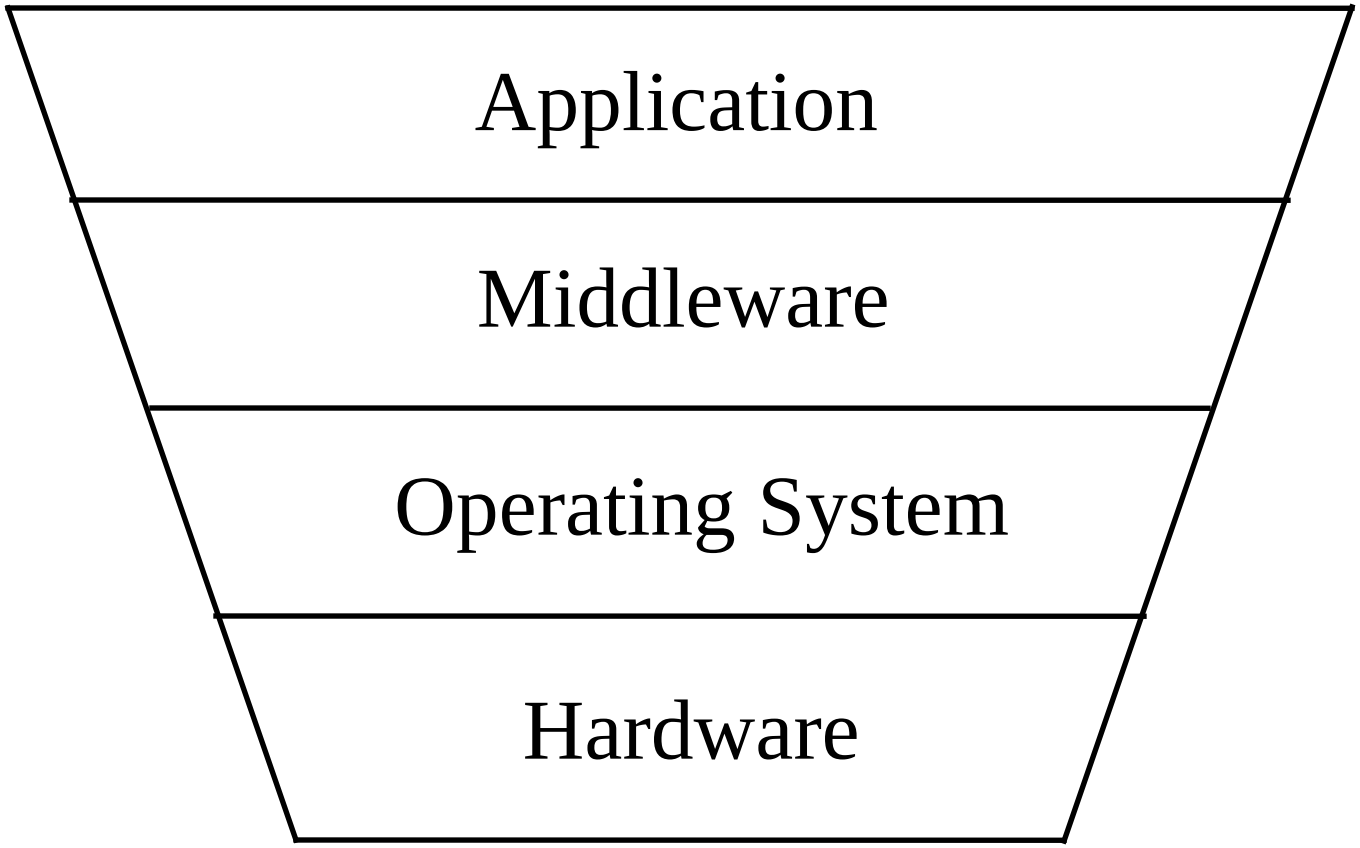
Access Control

Access Control

Access control is the selective restriction of access to an information, computational, or physical resource.

- In principle its all about security
- Also
  - Disruption
  - Privacy
  - Authenticity
  - Order

Pervasive - Everywhere



Access Control is Pervasive

1. Application
   - Complex, custom security policy.
   - Eg: Amazon account: wish list, reviews,
2. Middleware
   - Database, system libraries, 3rd party software
   - Eg: Credit card authorization center
3. Operating System
   - File ACLs, Android permissions system
4. Hardware
   - Memory management, hardware device access.

Access Control Matrix/table

A table that defines permissions.

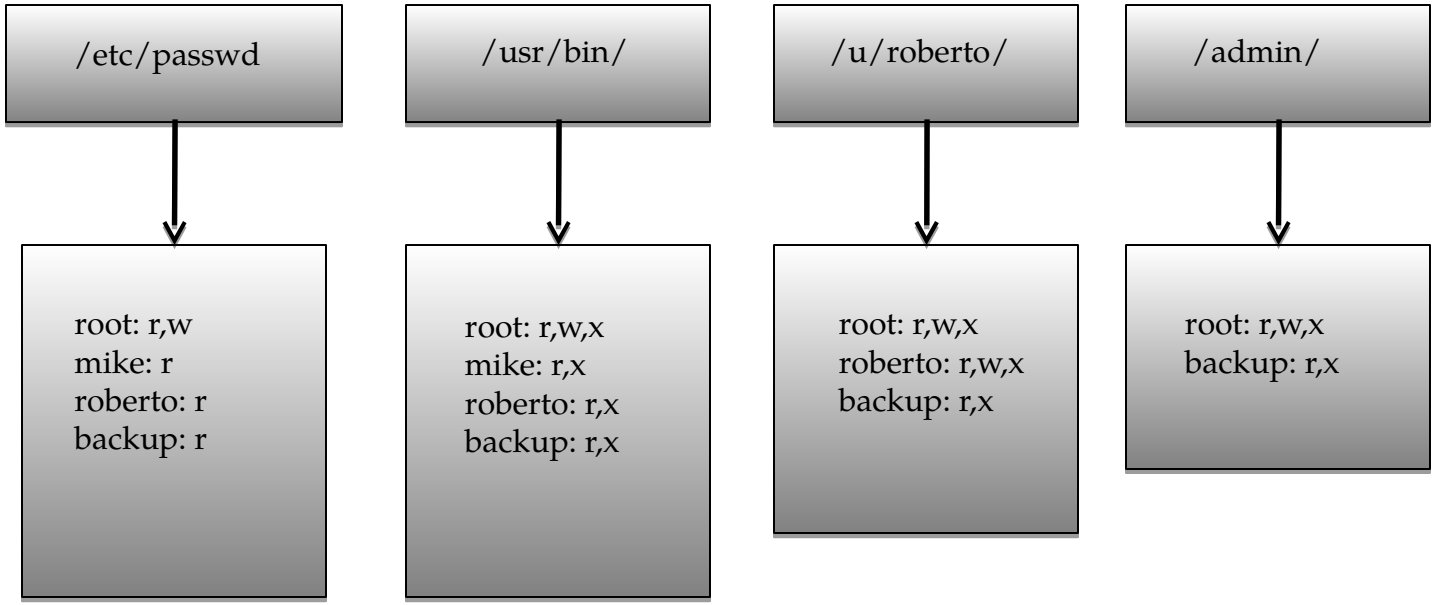
- Each row associated with a **subject, (**user, group, or system) that can perform actions.
- Each column associated with an **object, (**file, directory, document, device, resource, etc) for which we want to define access rights.
- Each cell filled with the access rights for subject and object.
- Access rights include reading, writing, copying, executing, deleting, and annotating.
- An empty cell means no access rights granted.

Access Control Matrix

	/etc/passwd	/usr/bin/	/u/roberto/	/admin/
root	read, write	read, write, exec	read, write, exec	read, write, exec
mike	read	read, exec		
roberto	read	read, exec	read, write, exec	
backup	read	read, exec	read, exec	read, exec
. . .	. . .	. . .	. . .	. . .

Access Control Lists (ACLs)

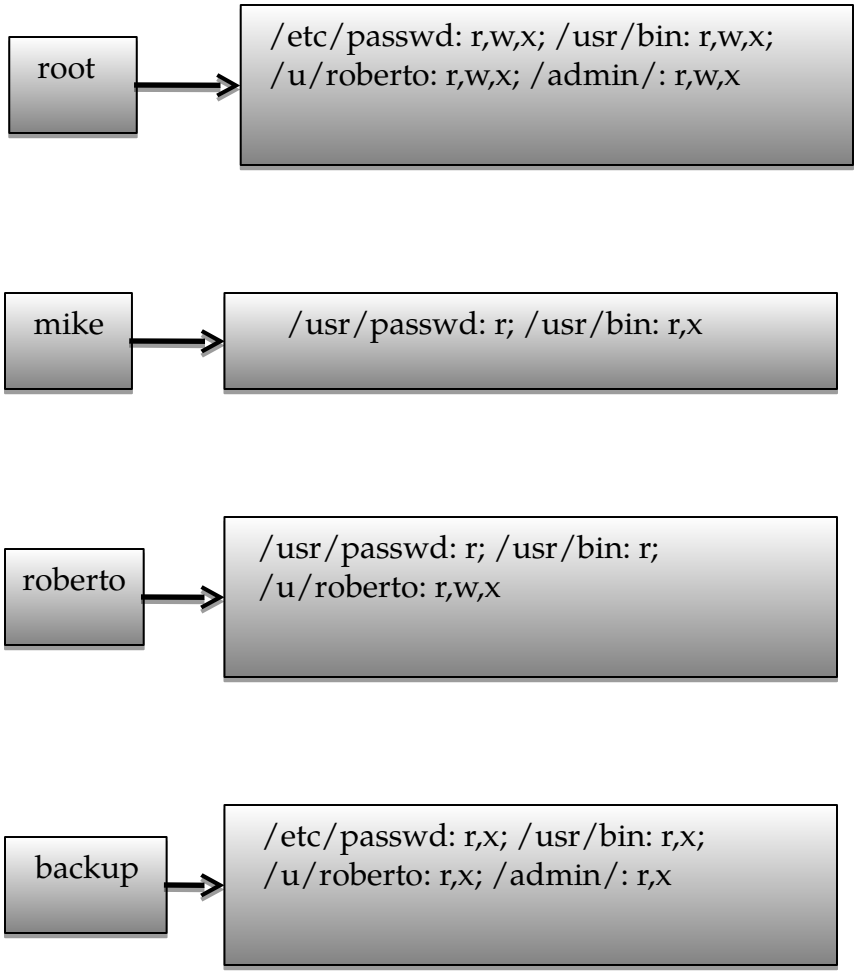
An **ACL** defines, for each object, o, a list, L (o's access control list) enumerating subjects s having access rights for o and, for each s, the access rights s has for o.



Capabilities

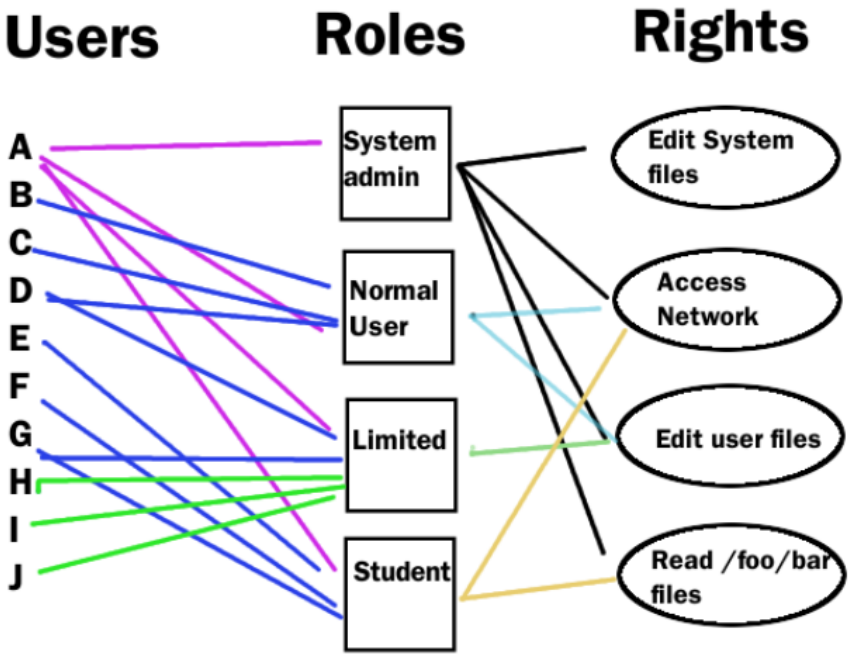
Capabilities

- Subject centerd approach (ACL object centered)
- defines, for each s, the list of o's s has non empty rights, together with the rights for each o



Role-based Access Control

Define **roles** and then specify access control rights for these roles, rather than for subjects directly.



Discretionary and Mandatory

Discretionary Access Control (DAC)

- Users set ACLs on objects OR
- Sys admins set capabilities for each user.

Mandatory Access Control (MAC)

- Administrator configures access control matrix.
- Access cannot be altered while system is running.

Some Models: Bell - LaPadulla

Security levels arranged in linear ordering

Top Secret: highest
Secret
Confidential
Unclassified: lowest

Levels consist of security clearance L(s)

Objects have security classification L(o)

LaPadulla Model

Developed in 1970s
Formal model for access control
Subjects and objects are assigned a security class
Form a hierarchy and are referred to as security levels
A subject has a security **clearance**
An object has a security **classification**
Security classes control the manner by which a subject may access an object

BL example

Security level	***Subject***	***Object***
Top Secret	Tamara	Personnel Files
Secret	Samuel	E-Mail Files
Confidential	Claire	Activity Logs
Unclassified	James	Telephone Lists

- Tamara can read all files
- Claire cannot read Personnel or E-Mail Files
- James can only read Telephone Lists

Some Models – Biba Integrity M

Various models dealing with integrity
Strict integrity policy:

Simple integrity: *modify only if* $I(S) \geq I(O)$
Integrity confinement: *read only if* $I(S) \leq I(O)$
Invocation property: *invoke/comm only if* $I(S_1) \geq I(S_2)$

UNIX Access Control Model

UID
- integer user ID
- UID=0 is ***root***

GID
- integer group ID
- Users can belong to multiple groups

Objects have both a user + group owner.

UNIX File Permissions

Three sets of permissions:

- User owner
- Group owner
- Other (everyone else)

Three permissions per group

- read
- write
- execute

UID 0 can access regardless of permissions.

Files: directories, devices (disks, printers)

UNIX File Permissions

Best-match policy

- OS applies permission set that most closely matches.
- You can be denied access by best match even if you match another set.

Directories

- read = listing of directory
- execute = traversal of directory
- write = add or remove files from directory

Look deeper

Implementations in win
Implementations in unix

Hardware Protection

Confidentiality
- Processes cannot read memory space of kernel or of other processes without permission.

Integrity
- Processes cannot write to memory space of kernel or of other processes without permission.

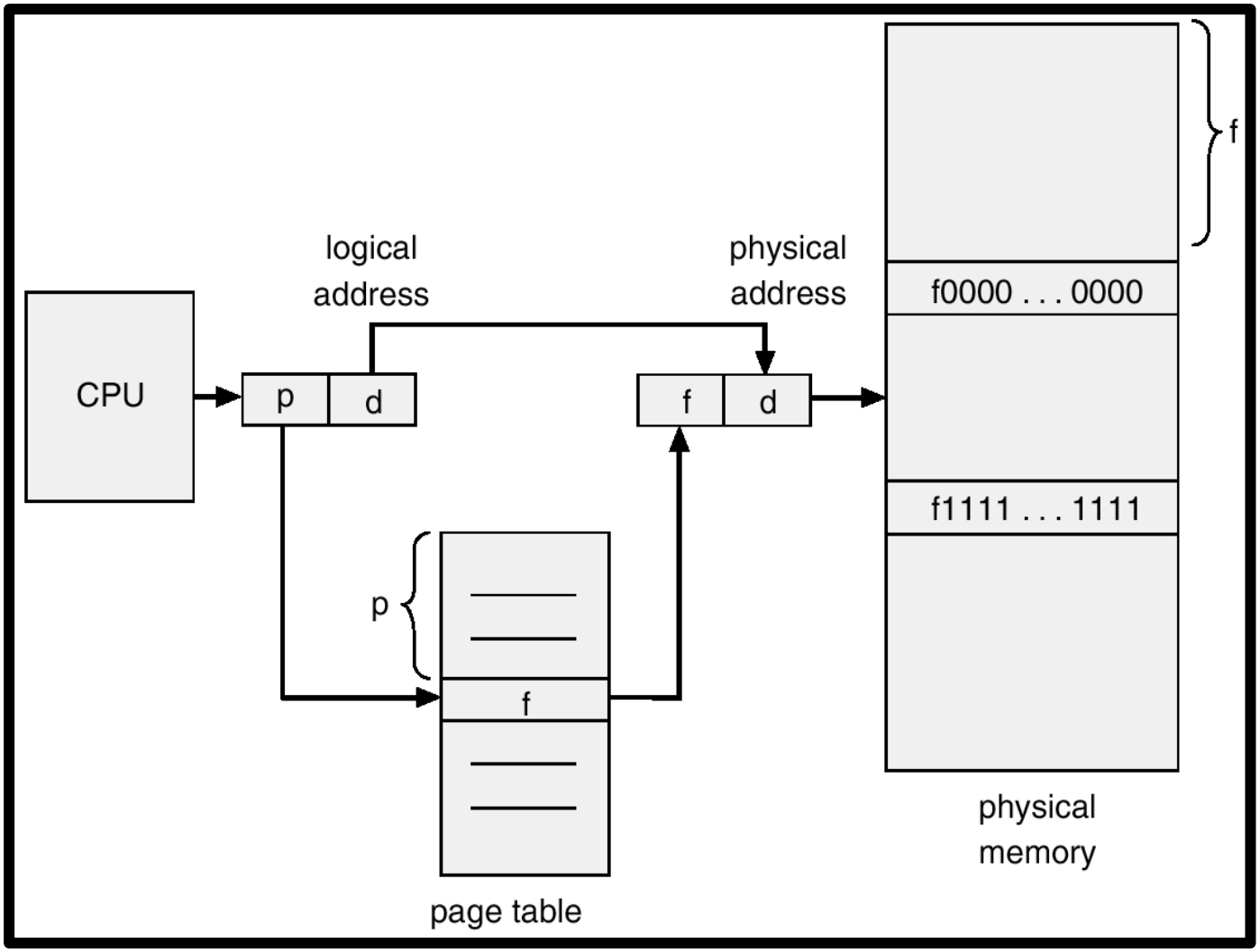
Availability
- One process cannot deny access to CPU or other resources to kernel or other processes.

Hardware Mechanisms: VM

Each process has its own address space.

- Prevents processes from accessing memory of kernel or other processes.
  - Attempted violations produce page fault exceptions.
- Implemented using a page table.
- Page table entries contain access control info.
  - Read
  - Write
  - Execute
  - Supervisor

VM Address Translation



Hardware Mechanisms: Rings

Protection Rings.

- Lower number rings have more rights.
- Intel CPUs have 4 rings
  - Ring 0 is supervisor mode.
  - Ring 3 is user mode.
  - Most OSes do not use other rings.
- Multics used 64 protection rings.
  - Different parts of OS ran in different rings.
  - Procedures of same program could have different access rights.

Hardware: Privileged Instructions

Only can be used in supervisor mode.

Setting address space
- MOV CR3

Enable/disable interrupts
- CLI, STI

Reading/writing to hardware
- IN, OUT

Switch from user to supervisor mode on interrupt.

Hardware: System Timer

Processes can voluntarily give up control to OS via system calls to request OS services.

Timer interrupt

- Programmable Interval Timer chip.
- Happens every 1-100 OS, depending on OS.
- Transfers control from process to OS.
- Ensures no process can deny availability of machine to kernel or other processes.

Some Research work

Lots of work going on in access control

- Models and mechanisms
- Architectural based controls
- Smart Devices
- AC policy management
- Relationship with security pillars
- Etc etc

Some Research work

Check Google scholar

- Scholar.google.com
- Search for one paper in one area of your choice
- Read it by sat 19th – be ready to brief the class in 4 minutes.
- Make a 4 slide presentation

Some Research work

We shall

- Get deeper into each area
- Write a technical report in groups