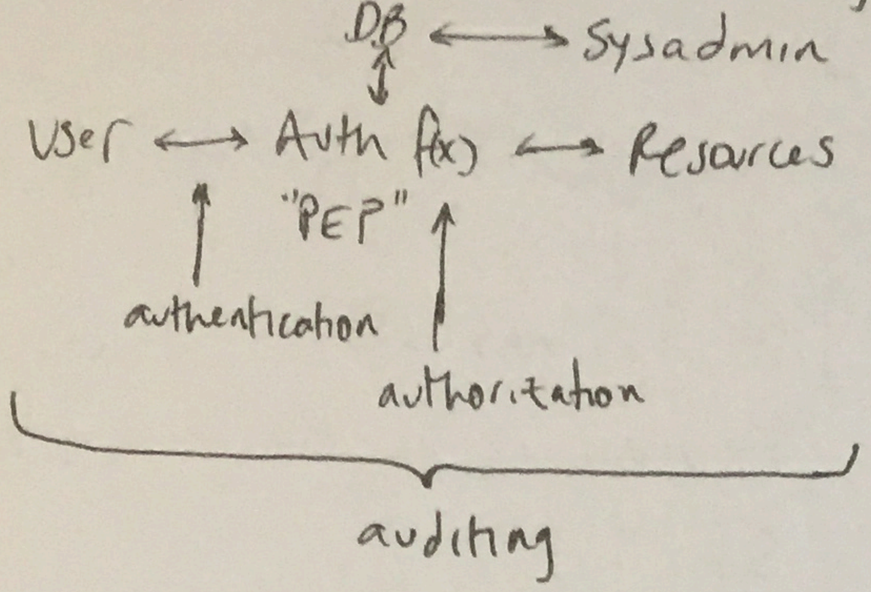
CS370 Notes
week 5

Access Control

- critical to computer security



- 3 "A"'s
  - → authentication: bind external entity to system entity
  - → Authorization: grant permissions to access a resource
  - → Auditing: '3rd party' / independent review of system actions

Access Control Policy Models

- Discretionary Access Control (DAC)
  - ↳ based on requestor identity, access rules
  - ↳ user can adjust policy,
- Mandatory Access Control (MAC)
  - ↳ testing labels associated with process and resource against rules
  - ↳ users cannot change
  - ↳ Labels such as TOP SECRET...
- Role Based Access Control (RBAC)
  - ↳ based on role or group.
- Attribute Based Access Control
  - ↳ based on attributes and context of access

Access Control Requirements

- functions' inputs are trustworthy
- Granularity of access (dir... bytes...)
  - ↳ tradeoff: precision / overhead
- Default closed (or open...)
- Policy conflict and combination resolution
- Admin Policy - who changes

Access Control Principles

- Least Control
- Separation of duty (more than one entity to complete critical tasks)
- Dual Control: changes to AC requires 2 entities.

Access Control Elements

- subject: system entity that can access objects
- object: file (UNIX), or other.
- Access Right: permissions

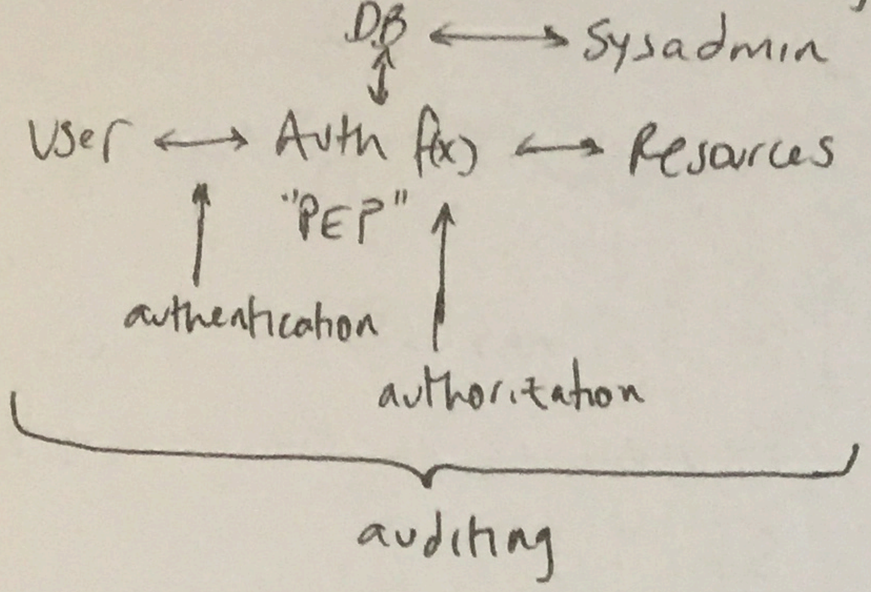
Access Control Matrix (ACM)

- basic abstraction. way of visvalizing completeness of AC.
- Not used for implementation

CS370 Notes
week 5

Access Control

- critical to computer security



- 3 "A"'s
  - → authentication: bind external entity to system entity
  - → Authorization: grant permissions to access a resource
  - → Auditing: '3rd party' / independent review of system actions

Access Control Policy Models

- Discretionary Access Control (DAC)
  - ↳ based on requestor identity, access rules
  - ↳ user can adjust policy,
- Mandatory Access Control (MAC)
  - ↳ testing labels associated with process and resource against rules
  - ↳ users cannot change
  - ↳ Labels such as TOP SECRET...
- Role Based Access Control (RBAC)
  - ↳ based on role or group.
- Attribute Based Access Control
  - ↳ based on attributes and context of access

Access Control Requirements

- functions' inputs are trustworthy
- Granularity of access (dir... bytes...)
  - ↳ tradeoff: precision / overhead
- Default closed (or open...)
- Policy conflict and combination resolution
- Admin Policy - who changes

Access Control Principles

- Least Control
- Separation of duty (more than one entity to complete critical tasks)
- Dual Control: changes to AC requires 2 entities.

Access Control Elements

- subject: system entity that can access objects
- object: file (UNIX), or other.
- Access Right: permissions

Access Control Matrix (ACM)

- basic abstraction. way of visvalizing completeness of AC.
- Not used for implementation