access control

two main activities that must occur in access

1. who are you (Authentication)
2. Do you have the right to do it (Authorization)

- trying to identify subjects, objects
- access control matrix
  - rows: subjects (what possible things a subject can do)
  - columns: objects (who can do what - access control list)
  - cells: define activity we can do (read/write/etc.)

Objectives of Authorization
- keep bad guys out
- let right guys in & keep them in bounds

Audit function: verifies that system is working correctly

Types of AC:
- discretionary access control: owner can grant rights to others
- mandatory: predefined rights based on what you are
- role based: what role you are defines your access
- attribute based: subject & objects have attributes

Requirements
- correct input
- support coarse and fine grain
- separation of duty (super powers shouldn't exist)
- policies (open vs closed)

Unix file access control
- UID/GID security
  - UID: default group
  - if I am this, my effective UID = owner
  - owner + group, world (building interface)