Announcements

- Reading Chapter 13
- Midterm #2 will be returned on Thursday

Project #4 Intro

- Includes code for VFS layer
  - Need to add fields to user struct to make it work
  - Provides support for PFAT filesystem (read only)
- Supplied bitset implementation

Booting the OS

- How does the OS get loaded and started?
- Process is called booting
  - want to use the OS to load itself
  - but what loads the OS?
- ROM monitor
  - knows how to read from a fixed location on disk and jump into it
- Bootstrap program
  - knows how to load a program from the filesystem and jump into it
- Alternative:
  - put more info into ROM about booting
    - MAC OS has most of the info in ROM
    - hard to change OS without changing ROMs

Booting the OS (cont.)

- put info into ROM about booting
  - MAC OS has most of the info in ROM
  - hard to change OS without changing ROMs
- Network Booting
  - ROM knows how to request a boot packet from the network
    - once the packet is received, execute it
  - useful for systems without local disks
  - used by OS developers to ease edit/compile/boot cycles

Swap Space

- Where is swap space located?
  - Is it a “normal” file in the filesystem?
  - Is is in a special location on disk?
- “normal” file
  - ✔ simple, just looks like a file
  - ✔ easy to change size
    - use normal tools
  - slow since it requires all of the filesystem overhead
- separate disk partition
  - ✔ faster
  - harder to change size (need a new partition)

Backups

- Disks can fail, so need to provide a way to copy them
- Two types of backups
  - full backup (all of the data on disks)
  - incremental (data that has changed since last backup)
    - can mark changed files with a field
    - can use the data of the file compared to the last backup
      - permits several levels of backup
    - may want multiple levels of incremental (day, week changes)
- Does the system need to be shutdown for backups?
  - what if a file is moved during a backup?
    - it could get copied 0, 1, or 2 times.
  - easiest answer is to shutdown the machine from dumps

Security

- security vs. protection
  - protection provides a mechanism to control access to resources
  - security also includes external features such as users
- security requires precluding unauthorized
  - access to data
  - modification of data
  - destruction of data
- several major types of security
  - physical: must protect access to resource it self
    - if you have physical access to a machine, you can break security.
  - users: if a user gives away access (or info) computer security if useless
  - software: OS and system software must provide protection

Who do you trust?

- It's easy to get paranoid
- Do I trust a login prompt?
- Do I trust the OS that I got from the vendor?
- Do I trust the system staff?
  - should I encrypt all my files?
- Networking
  - do you trust the network provider?
  - do you trust the phone company?
- How do you bootstrap security?
  - always need one "out of band" transfer to get going

Computer Threat Model

- must consider acceptable risks
  - value of item to be protected
  - $2,000 of computer time to steal 50 cents of data
    - this is a sufficient deter someone
    - **but** computers keep getting faster
- Basic Ideas:
  - confine access to only the highest level needed
    - run programs as root only if needed
    - don't give system access to all users