Announcements

- Reading Chapter 14 (8th ed)
- MT#2 re-grade requests due today
  - Must be submitted in writing to grades.cs.umd.edu
  - Provide paper copy of exam to me

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
- Need to plan for disasters too
  - What if the building burns down?

- 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 date of the file compared to the last backup
      - permits several levels of backup
    - may want multiple levels of incremental (day, week changes)

Backups

- 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.
  - easy answer is to shutdown the machine for backup
  - more typical setup:
    - Compute backup set
    - Backup files
    - Compute new backup set
      - Add any files that were missed

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

Authentication

- How does the computer know who is using it?
  - need to exchange some information to verify the user
  - types of information exchanged:
    - pins
      - numeric passwords
      - too short to be secure in most cases
    - passwords
      - a string of letters and numbers
      - often easy to guess
    - challenge/response pairs
      - user needs to be apply to apply a specific algorithm
      - often involve use of a calculator like device
      - can be combined with passwords
    - unique attributes of the person
      - i.e. signature, thumb print, DNA?
      - sometimes these features can change during life