CS370 Notes
Week 4

User Authentication
- binding a "subject" (external entity) to an internal / system entity (AKA "principal")
- 2 steps:
  - → subject presents a claim / identifier
  - → subject must present corroborating evidence to prove you are you.

Complementation Information
- all the info we submit during signup or registration
- processed to complementation information by computer

Password Based Authentication

PROS	CONS
- old, widely used	- weak passwords
- No special SW	- Passwords must be stored
- No special HW	- easy to share pw's
- Easy replace/recover	- reusing passwords
	- Social Engineering
	- keyloggers + NW
	- system Design

- Password Selection
  - ↳ people choose bad passwords
  - ↳ Research points towards
    - → use generated pronounable words (random phonemes)
    - → use longer pw's (no restrict.)
    - → use Passphrases "my first name..."

- Anderson's theoretical PW Strength formula
  - → P = probability of success
  - → G = guesses in 1 unit time
  - → T = number of time Units
  - → N = number of possible pw's
    - ↳ $P = (TG/N)$
  - → Assumes random passwords

- Password Storage
  - → How do we check ~~files~~ passwords with known ones, but keep all the ~~comput~~ passwords safe in case of attack
  - → hash passwords!
    - ↳ leads to dictionary Attacks
  - → Prevent / hinder attacks
    - ↳ increase needed efforts
      - ↳→ Hash + Salt → regreate dictionary
    - ↳ root only can access PW's
    - ↳ Block access if possible
  - → IT constantly runs cracker.
    - ↳ lock out accounts that are weak
  - → stop bad password selection
    - ↳ Bloom filter: tell if $p_i \in P$
      - ↳→ May provide false positives
- Password (Manglers / Managers)
  - ↳ single point of failure