

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
<ul style="list-style-type: none">- old, widely used- No special SW- No special HW- Easy replace/recover	<ul style="list-style-type: none">- weak passwords- passwords must be stored- easy to share pw's- reusing passwords- social engineering- keyloggers + ...- system design

- Password Selection

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

- Anderson's Theoretical PW Strength Form.

- 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 ~~temp~~ passwords safe in case of attack

→ hash passwords!

↳ leads to dictionary Attacks

→ prevent / hinder attacks

↳ increase needed efforts

↳ Hash + Salt → ^{regenerate} 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