CS370 Notes

week 1

What is Computer Security

- an art & a science of protecting or securing computer systems.
- art: some parts of security are an art (mindset, cyphers)
- Science: CS...
- Needed because of adversaties.

Security Notions

- Confidentiality: preventing unauthorized access to data.
- Privacy: preventing unauthorized access to data that concerns People.
  - ↳ also about what the user consents to share.
- Integrity: prevent unauthorized modifications to data, i.e. writes.
  - ↳ authentication: "From Addr" = Origin
  - ↳ System: Unauthorized mods to sys
- Availability: ensuring timely access to the target
- Authenticity: property of being genuine
- Accountability: the actions of an entity should be able to be traced to the source

Security Strategy

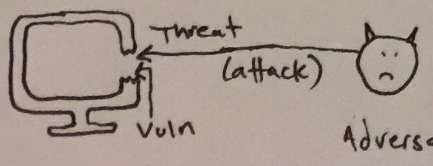
- Specification / Policy
- Implement Policy / How?
- Correctness / Assurance / Working?
- Incentives (correct on 1-3)

Cyber Security Principles [10]

- Economy of Mechanism
- Fall safe (or to safe state)
- Complete Mediation (every access is checked)
- Open design (closed source ≠ source of sec)
- Separation of Privilege (2 or more keys)
- Least Privilege (min (priv))
- Least Common Mechanism (No/Lim Shared)
- Psychological Usability (UI)
- Work Factor
- Failure Recording

Security Mechanisms

- Prevention (encryption)
- Detection
- Response
- Recovery



Attack Surface

- reachable
- exploitable
- vulnerability