6.857 Computer and Network Security
Lecture 2

Admin:
- Problem Set #1 posted (with assigned groups)

Today:
- Project ideas
  - "honeyword generator"
  - how to generate good "decoy passwords"
  - see Juels/Rivest ACM CCS '13 paper on Honeywords
- Finish Lecture 1 material
- Growth of cryptography talk (Killian award talk)

Some principles:

- Be skeptical and paranoid
- Don't aim for perfection ("there are no secure systems, only degrees of insecurity…")
- Tradeoff cost/security ("to halve the risk, double the cost…" – Adi Shamir)
- Be prepared for loss
- "KISS" ("keep it simple, stupid!")
- Ease of use is important
- Separation of privilege – require 2 people to perform action
- Defense in depth (layered defense)
- Complete mediation (all requests checked for authorization)
- Least privilege (don't give some more permissions than they need)
- Education
- Transparency (no security through obscurity)

Security mechanisms may involve:
- Identification of principals (e.g. "user name")
- Authentication of principals (e.g. password, biometric)
- Authorization: checking to see if principal is authorized for requested action
- Physical protection: locks, enclosures
- Cryptography: math in service of security (hard computational problems)
- Economics: (note model change here: parties are self-interested, e.g. spammer, …)
- Deception: to get adversary to reveal himself or waste his efforts (e.g. honeypot)
- Randomness, unpredictability: e.g. for passwords and crypto keys

6.857 Network and Computer Security

Spring 2014