

Admin:

Pset #1 posted later today  
(with assigned groups. Be sure you have signed up to be on our student email list, so you are assigned a group!)

Today:

- Project idea
  - Finish LOL material
  - Growth of cryptography talk (Killian award talk)
- “honeyword generator”  
how to generate good  
“decoy passwords”  
see ~~Juels~~ Juels/Rivest  
ACM CCS '13  
paper on Honeywords

## Some principles:

L1.8

- be sceptical & 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 & crypto keys