TOPIC: 6.857 - Computer & Network Security

DATE: 2/8/16

FILE UNDER:

PAGE: L02.1

Admin:

Pset #1 posted today; due Mon 2/22

See TAs if you don't have pset group

Recitation this week (Fri 2/12 11am 35-225)

Today:

- ☐ Finish L01 material
- ☐ "Growth of Cryptography" talk (Killian award lecture)

Some principles & maxims:

- think adversarially
- be sceptical & paranoid
- don't aim for peffection
  ("There are no secure systems, only degrees of insecurity..." Shamir)
- tradeoff: cost/security
  ("To halve the risk, double the cost..." Shamir)
- tradeoff: ease-of-use/security
- Attacker has to find only one vulnerability,
  Defender has to protect or monitor them all
- "Assume that your system has been breached"
  (Detection/recovery may be more important than prevention)
- Defense in depth (layered defense) ← Be prepared for loss.
- "Don't underestimate the time & effort an adversary will spend trying to break your system" (Morris Sr.)
- Use "separation of privilege" - require 2 people to perform sensitive action
- Use "least privilege" - don't give someone more permissions than they need
- complete mediation - all requests checked for authorization
- transparency - no security through obscurity
- importance of education & training
- sharing info about vulnerabilities can help
- computer & software are toys - if you play rough with them they will break
- adversaries to worry about: insiders
  NSA
  Chinese