TOPIC: 6.857 – Computer & Network Security

DATE: 2/12/18

FILE UNDER:

PAGE: L02.1

Admin:

Pset #1 posted today; due Mon 2/26

Pset groups being created by TAs & emailed today.

Recitations in 54-100

Today:

- ☐ "Growth of Cryptography"

  (Rivest Killian lecture – see slides)

- ☐ Principles of Security (copy pg 2 here, also (pg 8 of L01 notes)) } (didn't get to these...)

TOPIC: 6.857

DATE:

FILE UNDER:

PAGE: L02.2

Some principles & maxims:

- think adversarially
- be sceptical & paranoid
- don't aim for perfection
  ("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