Outline: ☐ Administrivia
☐ Course content overview

Administrivia:

- review course information sheet
- signup online (re-register) & also sign clipboard

Content:

- Computing or communicating in presence of adversaries
- "Protecting" some resource, communication, or activity...
- Typically involves an "information system":
  PC, network of computers, cell phones, Pay TV
  E-mail, cars, ATM machines, RFID's, iPODs, ...
- Security policy:
  - gives desired security objectives or properties
    "Each registered voter may vote at most once."
    "Only an administrator may modify this file."
    "The recipient of an email message shall be able to authenticate its sender."
  - usually stated in terms of
    - principals (actors or participants)
    - (perhaps in terms of their roles) [voter]
    - permissible actions or operations
    - on (classes of) objects

- Security mechanism (or security control) is component, technique, or method for (attempting to) achieve or enforce security policy.

  Ex: smart card for voter
  password for sysadmin
  digital signature for message sender
  locked cabinet for PC

- Mechanisms (aka "countermeasures") are typically of one of two forms:
  - prevention: keep security policy from being violated
    Ex: fence, password, encryption, memory bounds check
  - detection: identify when policy is violated
    Ex: motion sensor, tamper-evident seal, stored fingerprint ("hash") of all executables, intrusion-detection on network, virus scanner, ...
  - detection mechanisms usually come with recovery mechanism (remove intruder, remove virus, load files from backup)
  - detection may involve deterrence (give adversary risk of being held accountable for security breach), and so is part of prevention (!).

2/4/09

6.857 [redacted]
Rivest L1.3

- Security policies (goals) often fall into one of three categories: (classic)
  - confidentiality: information should not be disclosed to unauthorized parties
  - integrity: information should not be modified in an unauthorized manner
  - availability: system or resource shall be available for use as intended

  ("CIA")
- Who is adversary?
  - may be insider/outsider, vendor, ...

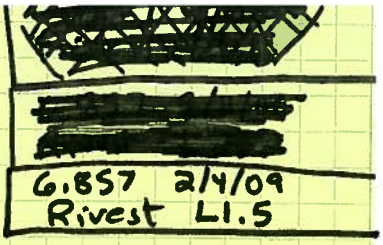
    Ex: voter may wish to sell her vote
    Election official may be corrupt
    vendor may sell systems with backdoors
    eavesdropper may tamper with databases...
  - what does adversary know?

    Ex: system design & implementation details
    passwords
    personnel...
  - what resources does adversary have?
    - large computers
    - ability to intercept & modify all communications
    - ability to corrupt some participants (e.g. pay TV subscriber, or voter)
    - typically make generous assumptions about adversary's abilities

6.857 [redacted]
Rivest L1.4

- Terminology:
  - vulnerability = weakness that might be exploited by some adversary
    (Ex: poor password, buffer overflow possibility)
  - threat = potential violation of security policy
    (e.g. by exploiting some vulnerability)
  - risk = likelihood that threat will materialize
  - risk management = balancing risk against other factors:
    cost, ease-of-use, understandability, availability, ...
    ⇒ no security mechanism is perfect.
    we are building ~~walls~~ fences, not impenetrable walls...
    ("how high is fence")

- Security mechanisms may involve:
  - identification of principals ("user name")
  - authentication of principals (password, biometric)
  - authorization: checking permission list 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: all parties self-interested)



6.857 2/4/09
Rivest L1.5

Some principles:

- Be sceptical & paranoid:
- don't aim for perfection (There is no secure system, only degrees of insecurity...)
- tradeoff cost/security (to halve the risk, double the cost...)
- separation of privilege: require 2 people to perform task...
- ease of use is important...
- KISS...
- defense in depth / layered defense
- no security through obscurity
- crypto is very useful
- user education & awareness important
- personnel policies important...
- physical protection is foundation...
- complete mediation...
- principle of least privilege