6.857 Computer and Network Security
Lecture 1

"Security" relates to "computing or communicating in the presence of adversaries."

Typically involves an "information system": PC, network of computers, cell phone, email, ATM, car, smart grid, RFID, wireless link, medical device, …
Everything is digital now!

Security relates to a "security objective" or "security policy": what is being prevented? What activities or events should be prevented/detected?

Security policy usually stated in terms of:
- Principals (actors or participants, perhaps in terms of their roles)
- Giving permissible (or impermissible) actions or operations
- On (classes of) objects

Examples:
- "Each registered voter may vote at most once."
- "Only an administrator may modify this file."
- "The recipient of an email shall be able to authenticate its sender."

Security policies (goals) often fall into one of three classic categories ("CIA"):
- 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

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

Examples:
- smart card for voter
- password for sysadmin
- digital signature on email
- locked cabinet for server

Security mechanisms are typically one of two forms:

1. Prevention: keep security policy from being violated
   Examples: fence, password, encryption, memory bounds check, …

2. Detection: detect when policy is violated
   Examples: motion sensor, tamper-evident seal, stored fingerprint ("hash") of executables, intrusion detection on network, virus scanner,…

Detection mechanism often comes with recovery mechanism (remove intruder, remove virus, load files from backup, …)

Detection may involve deterrence (adversary risks being identified and being held accountable for security breach) and so plays a role in prevention.

Who is adversary? (Know your enemy!)

- May be insider/outsider, vendor, …

Examples:

- Voter may wish to sell her vote.
- Election official may be corrupt.
- Vendor may install "backdoor" in system.
- Eavesdropper may manipulate communications.

What does adversary know?

Examples:

- System design and implementation details
- Passwords
- Facebook profiles of all personnel

What resources does adversary have?

Examples:

- Large computers
- Ability to intercept and modify all communications
- Ability to corrupt some participants (e.g. payTV subscriber, voter, server…)

We typically make generous assumptions about adversary's abilities.

Vocab:

"vulnerability" = weakness that might be exploited by an adversary (e.g. poor password, buffer overflow possibility)

"threat" = potential violation of security policy (e.g. by exploiting a vulnerability)

"risk" = likelihood that threat will materialize

"risk management" = balancing one risk against another, or other factors, such as cost, ease-of-use, understandability, availability, …

No mechanism is perfect – we build fences, not impenetrable walls (how high is a fence?)

6.857 Network and Computer Security

Spring 2014