TOPIC:

DATE: 2/5/14

FILE UNDER:

PAGE: L1.1

6.857 – Network & Computer Security

Prof. Ronald L. Rivest

TA's: Jennifer Jang
Madars Virza
Justin Holmgren
Morgan Lai
–

One handout: course info sheet

http://courses.csail.mit.edu/6.857

Mondays & Wednesdays: Lectures 11:00-12:30 (in 4-270)
Fridays : Recitation 11:00-12:30 (in 4-270)

Outline: Administrivia
Course overview
introduction to security

Administrivia: course info sheet
send email to 6.857-tas@mit.edu
if you are not registered for course
but want to take it & be on
mailing list

Note: Schneier lecture tomorrow (2/6) 5pm
in 32-123
"NSA Surveillance & What to Do About it"

MIT Bitcoin Club mtg 2/11 in 4-370 6:30pm
"What is Bitcoin?"
(see notice on class website; register)

Content:

L1.2

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

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

Security relates to a "security objective" or "security policy":
what is being protected? 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:

- 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

("C I A")

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 & being held accountable for security breach) and so plays a role in prevention.

Who is adversary? (Know your enemy!) L1.5

- 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 & implementation details
passwords
facebook profiles of all personnel

- what resources does adversary have?

Examples:
- large computers
- ability to intercept & modify all communications
- ability to corrupt some participants
  (e.g. payTV subscriber, voter, server, ...)

We typically make generous assumptions about adversary's abilities.

Vocab:

L1.6

"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 fence?)