

1/24 Lecture: Security basics: goals, threat models

Beili Wang (with minor edits by Rob Johnson)

*** (Black color is what the professor wrote on the board; Blue color is the notes from the class discussion.)**

General Information about the class:

The course focuses on: single system that multiple users can use but not interfere with each other.

Things on Paper Review:

Is it going to work?

What will be the cost?

What is the result?

How can I get access the system? Break the system?

Objectives in Security:

1. Protecting a resource
2. Private: files, folders, bank accounts, etc.
 - a. From whom?
 - b. From what done to them?
2. From copying (reading), deleting, corrupting.

General Goals:

1. Confidentiality (copying, reading)
2. Integrity (corrupting)
3. Availability (deleting) e.g. virus

Example: Buffer overflow Attack

Integrity – memory corrupting

Availability – gain total control

Confidentiality – can do anything

1. Confidentiality: (protecting the resource)

- Eavesdropper can't read message in transit.
- Thief can't read documents on stolen laptop.
- Other users can't tell that I'm running a large computation.
(ex: mostly in military setting, very expensive to achieve this goal.)
- Observer can't tell that I'm talking to Bob.
(ex: voting machine)

2. Integrity: (Does the system achieve what it should achieve?)

- Only authorized users can modify database.

- No one can modify a program's memory.
- Only authorized users can run programs.
- I only want to accept messages that come from Bob.

4. Availability:

- Attacker can't prevent me from shopping on Amazon.
- Attacker can't consume all of disk.
- Use can't degrade performance to unusable levels.

Q: Why separate address space?

A: More reliable. (Mistakes happen that do not need to shut down the whole system.)
Also, can swap to disk.)

Q: Difference between securities vs. correctness?

1. System may not be fully correct.
2. Correctness:
Mistakes, accident do happen

Ex: Raid 5

Main difference between accidents and security?

Adversary (who has a hammer?)

“Something goes wrong in worst possible way.” (security)

“Adversary has limited power.”

Two Questions:

What do we want to achieve?

Who do we want to achieve it against? (attacker).

Threat models:

Limitation of Attacker:

1. computational power
2. bandwidth (not a problem)
3. storage (not a problem)
4. time
5. money

1. Computational Power

1 Pentium ~ 4GHz = 2^{32} instructions/second

1 Blue Gene ~ 2^{16} CPUs

So total 2^{48} instructions/second

1 year about 2^{25} seconds/year

So about 2^{73} instructions/year

100 years about 2^7 years

So total is about 2^{80} instructions

It is a lot but not infinite amount. The message is time sensitive which limits attacker.
(not important after 100 years)

However: ex: Who kill JFK?

2^{128} keys try 2^{80} instructions, we left 2^{-48} probabilities of recovery key.

Moore's law: computer power doubles, get faster exponentially.

2. Bandwidth:

network flood with packets:

1 attacker, dial up 56kb/second

100,000, dial up 5.6Gb/second

On today's Internet, bandwidth usually not a problem.

An attack that "propagates from one machine to another" is called a worm.

3. Storage is not a problem today.

4. Time:

"Attack at Dawn."

a. Time sensitive: limits attacker.

b. Rekeying, e.g. every 24 hours, limits attacker.

2. Money:

Attacker limited in money.

- Poor attackers: script kiddies

- Resource isn't valuable. (example: Trade secret: \$1 million)

- This also limits defender.

(example: Biometric: fingerprint, Japanese researcher uses gum to break it. (even cheaper)).

1. Access (gain access)

Outsider or Insider

Local vs. Remote attackers

a. Remote attackers

- attackers can communicate with web server, ftp server.

- Cannot log in

b. Local attackers

- assume attacker can log in

2. Related to Access: knowledge

- knows OS version, Applications version

- configuration information

- source code

- vulnerabilities in OS/Apps

3. Doesn't know:

- passwords
- private keys
- random numbers

(example: ssh demon)

Summary:

Defender: Security Goals (What you try to do?)

Attacker: Threat Models

Computation power

Time

Bandwidth

Storage

Money

(What you try to against?)