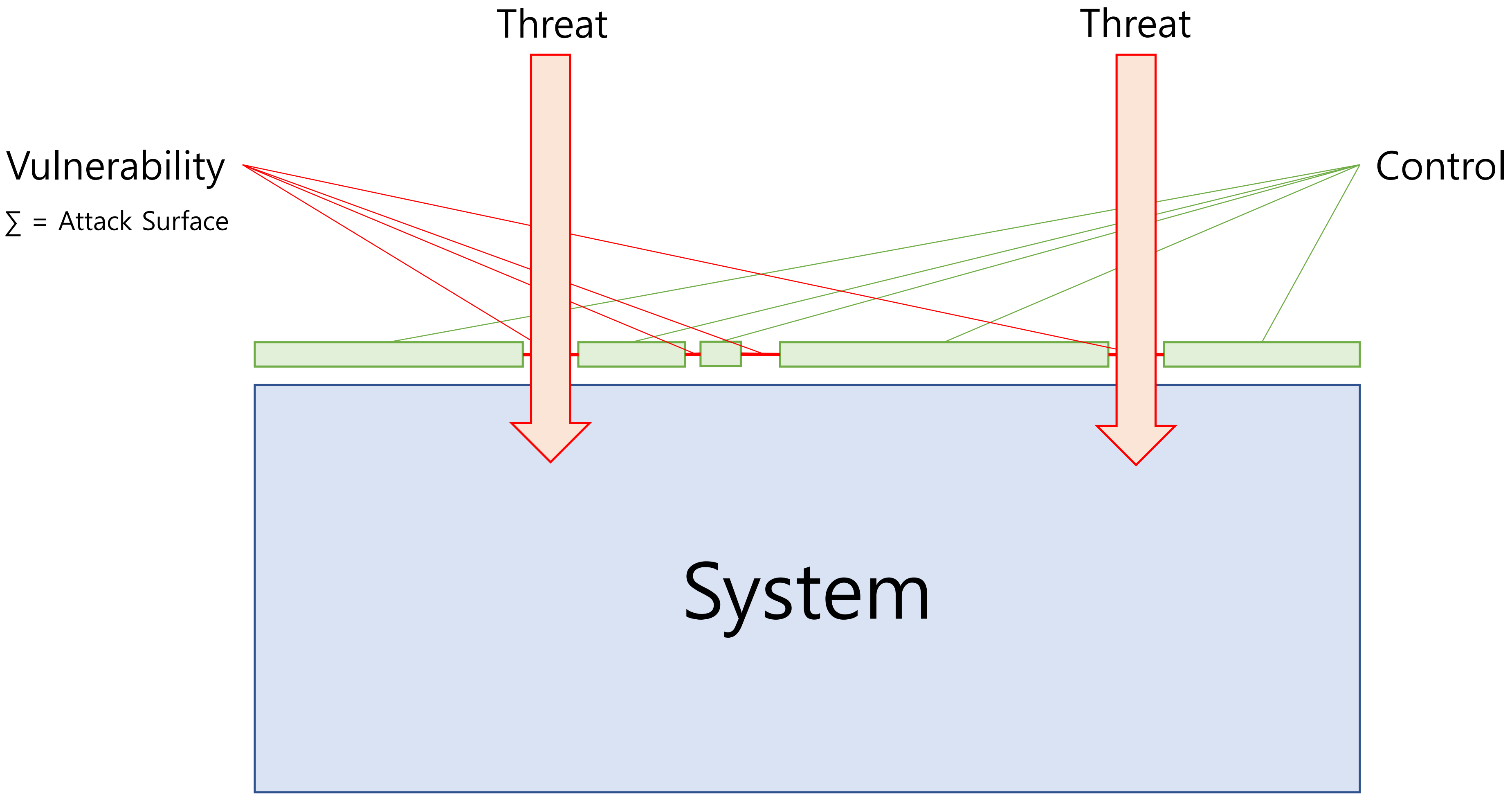
Design and Analyze Secure Networked Systems 1

Prof. Edward Chow @ Colorado Univ.

Note by waegaein@github.com

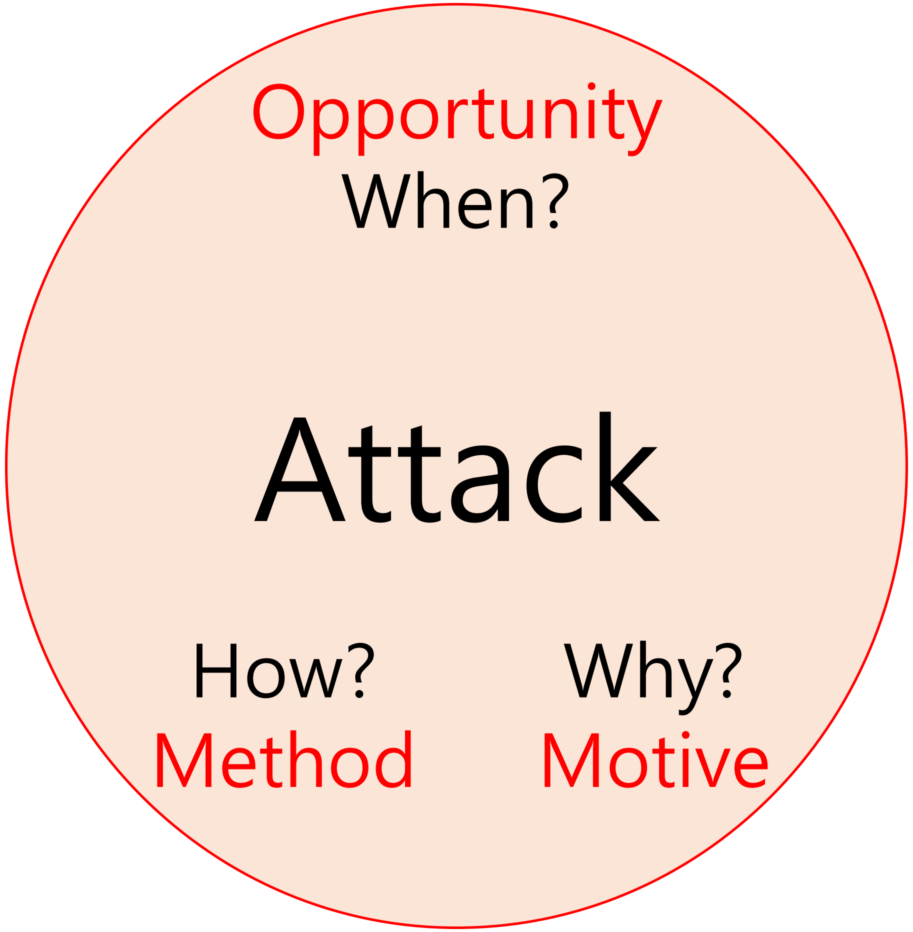
Glossary

- Vulnerability
  - A weakness in the security system that might be exploited to cause loss or harm.
  - e.g. HW / SW / Policy / Procedure
- Attack Surface
  - Sum of the vulnerabilities in a given system that are accessible to a hacker.
- Threat
  - A set pf circumstances that has the potential to cause loss or harm.
  - e.g. Interception / Interruption / Modification / Fabrication
- Control
  - Removes or reduces a vulnerability. Control of vulnerabilities blocks threat.


Threat
Threat
Vulnerability
∑ = Attack Surface
Control
System

Glossary

- Method
  - The skill, knowledge, tools and other things with which to be able to pull off the attack.
- Opportunity
  - The time and access to accomplish attack.
- Motive
  - A reason to want to perform this attack against this system.



Opportunity

When?

Attack

How?

Method

Why?

Motive

Security Analysis

- Denying any of M.O.M. prevents attacks.
- Why difficult?
  - Knowledge/Specification/Source available of Internet.
  - Access to computer systems available through Internet.
  - Motives are financial, to show prowess, or random.
- Case: First Bank ATM Heist in Taiwan
  - **Method:** Hackers remotely accessed server and dispatched false patch to ATMs.
  - **Opportunity:** Hackers were able to enter IT equipment room in London branch.
  - **Motive:** $2.2M financial gain.

Glossary

- Confidentiality
  - The concealment of information or resources.
  - **Attack:** Intercept the message in transit or hack into data storage.
  - **Defense:** Encrypt data both in storage and in transit.
- Integrity
  - The trustworthiness of data and resources.
  - **Attack:** Intercept and alter the message in transit or hack into server and modify data.
  - **Defense:** Create digest and digitally sign it.
- Availability
  - The ability to use the information or resources as desired.
  - **Attack:** Send large volume of dubious requests to servers.
  - **Defense:** Duplicate servers on different locations or trace back and push back attackers.

Confidentiality
Is it secret?

Integrity
Is it original?

Availability
Is it on sale?