CSE467: Computer Security

7-1. Introduction to Software Security

Seongil Wi

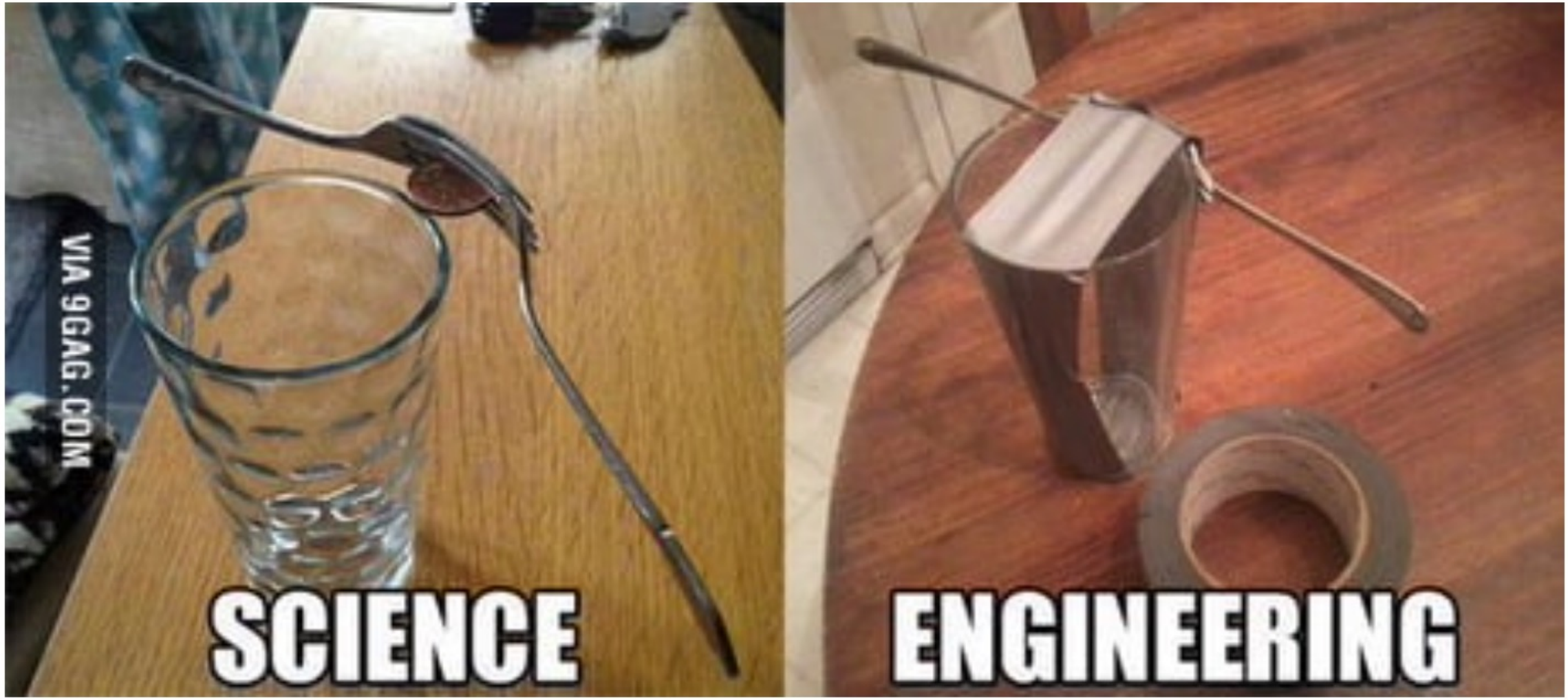
Department of Computer Science and Engineering

Secure Software?

- Can we say a program is secure if it considers the CIA properties?

Where there is engineering, there is a ***security problem***

Engineering Failure



Why?

Humans always make ***mistakes***

Software Security is About Software Bugs

- Find software bugs
- Exploit software bugs
- Patch software bugs

Software Bug

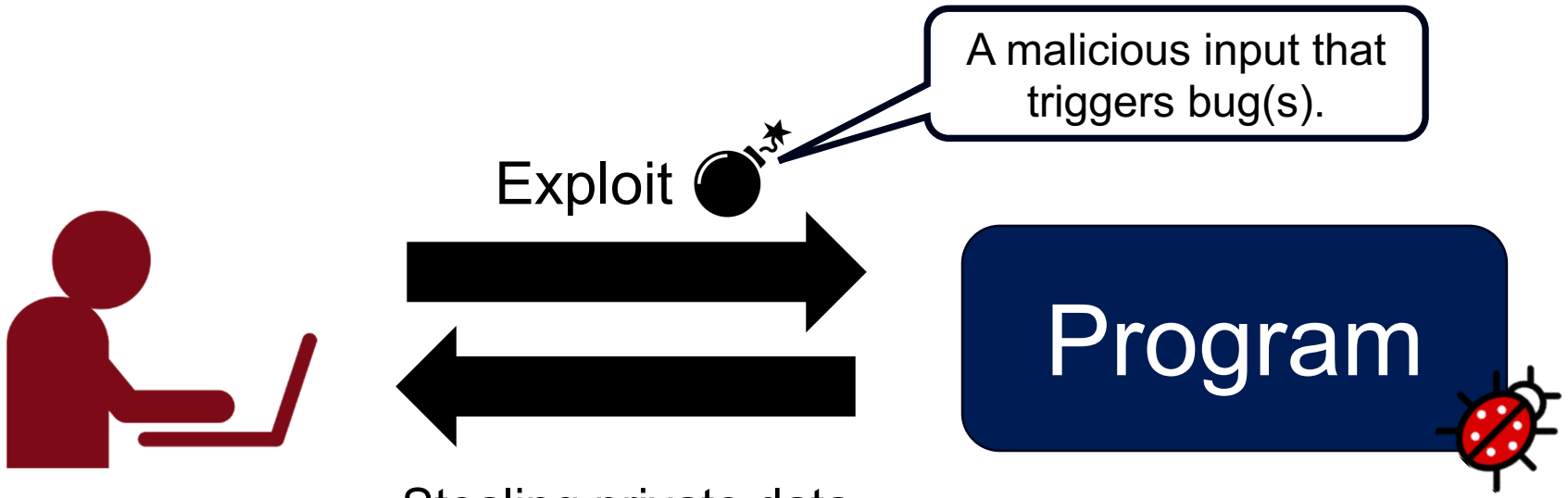
- Software bug is an *error/fault/mistake* in the code that produces **an unexpected result**

Software Bugs is the Key

- ***Root cause*** of many security problems including malware, hacking incidents, phishing, privacy leakage, etc.

Not Every Bug is Security Critical

- Some bugs are merely about aesthetics. Some bugs allow an attacker to compromise the whole system.



- Stealing private data
- Executing arbitrary commands
- ...

Think Like Adversaries

Threat Modeling

- **Threat modeling** is the process of systematically identifying threats to a system, such as vulnerabilities or lack of defense mechanisms

Attack Scenario

- (Assumption) This course is too difficult to follow. However, you really want to get an ‘A’ in this course in order to graduate

Of course you should never attack anyone in reality!

Potential Threats

What do you have to do? Where would be the solutions?

- Steal the solutions
- Hire security experts to solve exams on behalf of you
- Modify my score after grading is done (get administrative privilege from the UNIST academic system)
- Perform denial of service attack on UNIST portal
- etc

Depending on how much effort you are willing to put ...

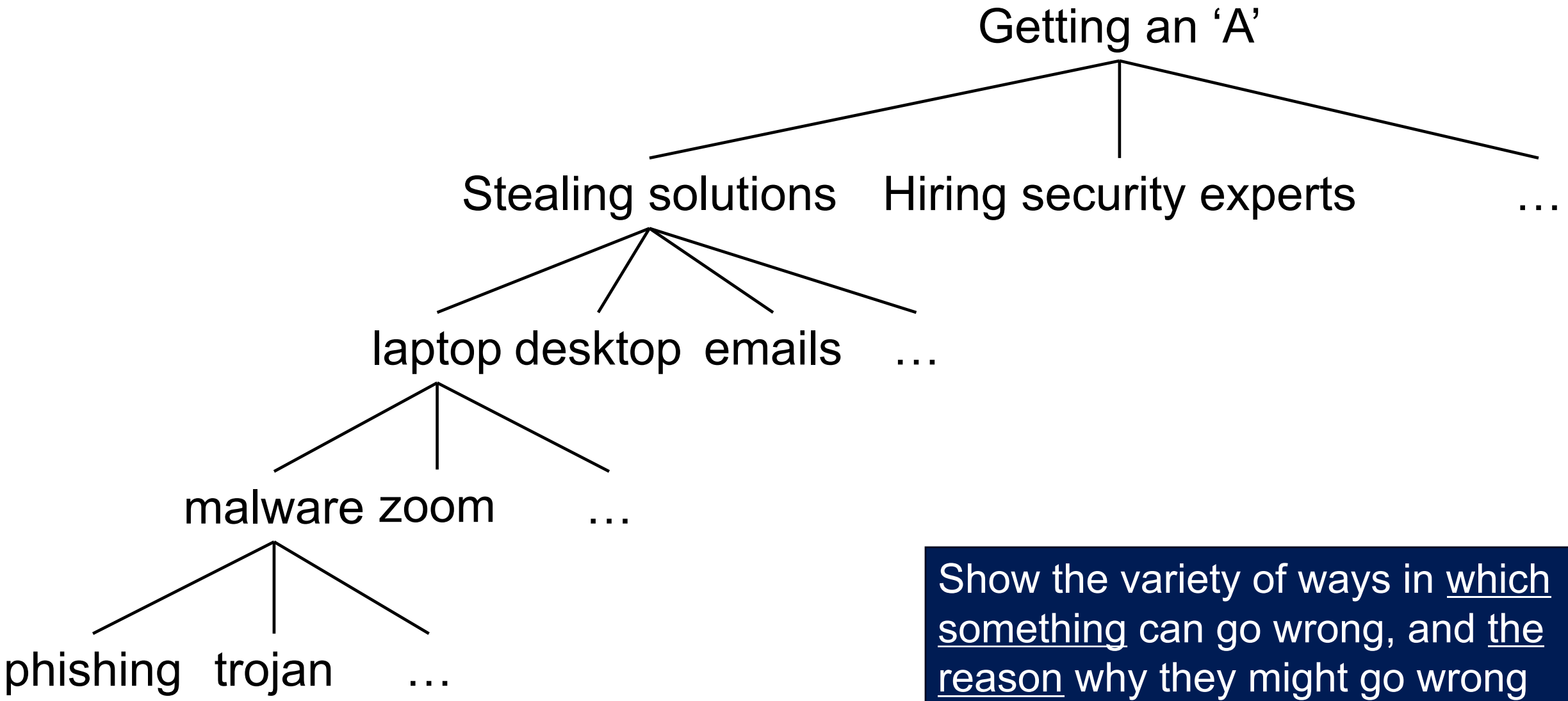
Enumerate Attack Points

- To “steal the solutions”…what do you have to do? Where would be the solutions?
  - Prof. Wi’s laptop
  - Prof. Wi’s desktop
  - Prof. Wi’s GitHub account.
  - The trash bin in Prof. Wi’s office
  - TA’s emails
  - TA’s office
  - Blackboard
  - etc.

Oftentimes, those attack points are called the ***Attack Surface***

Think Like Adversaries

Attack Tree



Show the variety of ways in which something can go wrong, and the reason why they might go wrong

Overview of the Lecture

- Understand general ***principles (NOT*** about learning hacking skills***)***

- ***Reverse Engineering*** (5-6 lecture):
  - Learn how attackers find and exploit bugs
  - Learn how current defense techniques work

- ***Secure Coding*** (1 lecture):
  - Learn how to engineer secure software systems

Question?