Chapter 1. Course Overview

Prof. Jaeseung Choi

Dept. of Computer Science and Engineering

Sogang University

About Attendance

- **We will take attendance starting from the next lecture**
  - Today we will fix the seat map for this
- **After each class, TAs will upload the list of late and absent students in *Cyber Campus***
  - Check the reply of the post in *Announcement* tab
  - If something is wrong, **contact the TA within a day**
- **After two days, TAs will enter this list to SAINT**
  - Once it is entered to SAINT, it's hard to change the result
  - It's your responsibility to **check your status regularly**

Previous Lecture

- **We focused on administrative stuff**
  - General course information
  - Grading components
  - Course policies
  - Prerequisite

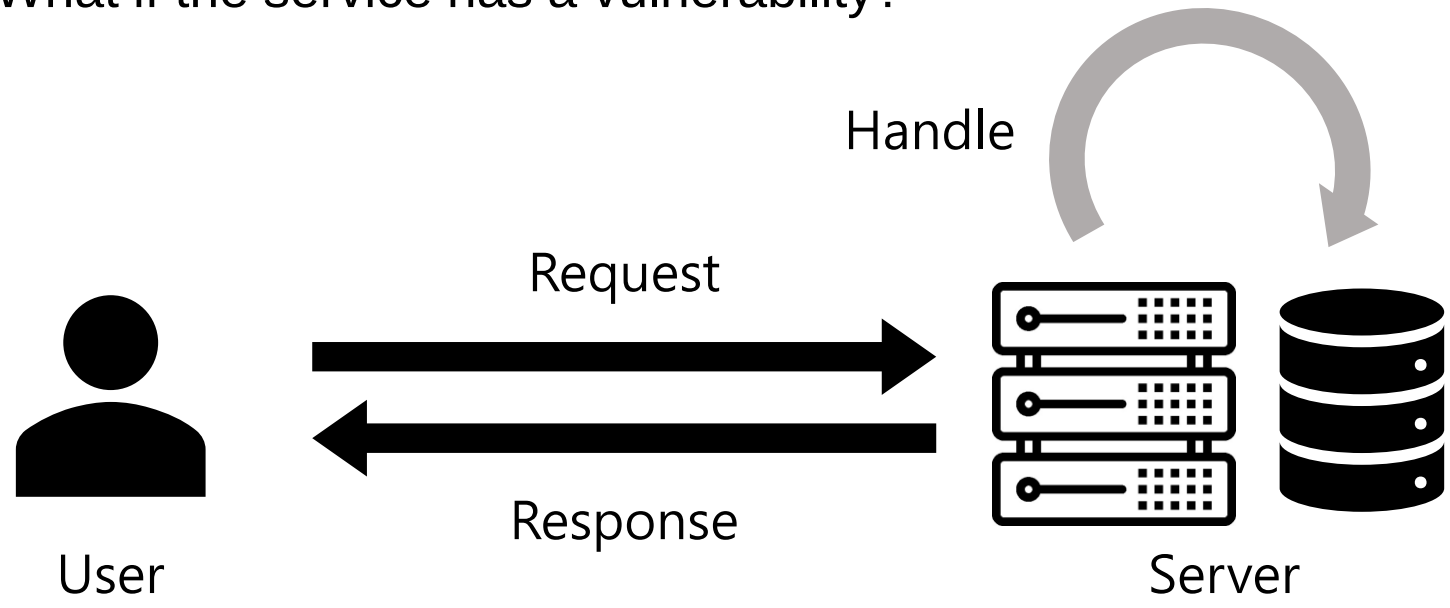
- **If you missed the last class, please download and read the slide carefully!**

Today’s Topic

- **Goal and scope of this course**
  - Software security
- **Basic concepts and terminologies in security**
  - CIA properties
  - Common types of attacks
  - Threat model

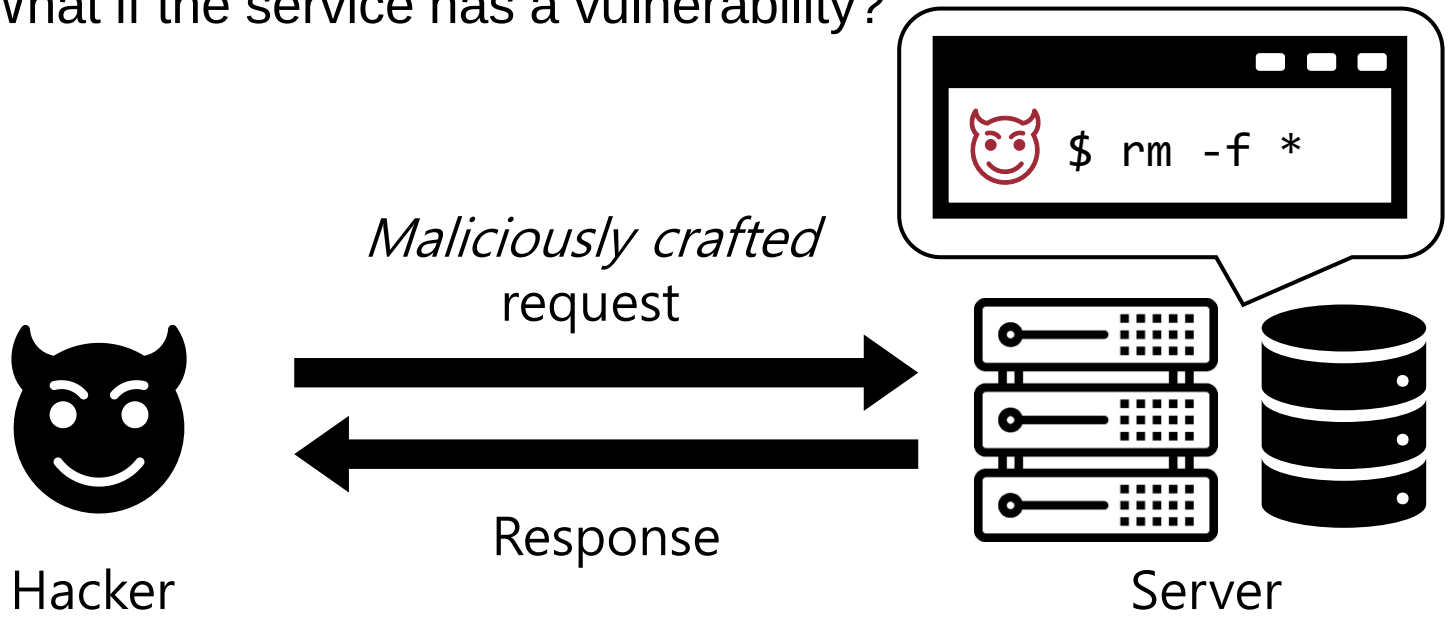
Hacking & Security

- **Various vulnerabilities can occur in computer systems**
  - Hackers can exploit them and pose serious threats
  - We will learn these attacks and the defenses against them
- **Ex) Assume that your computer is running a service**
  - What if the service has a vulnerability?



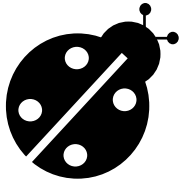
Hacking & Security

- **Various vulnerabilities can occur in computer systems**
  - Hackers can exploit them and pose serious threats
  - We will learn these attacks and the defenses against them
- **Ex) Assume that your computer is running a service**
  - What if the service has a vulnerability?



This Course: Software Security

- **There are many sub-areas in information security**
  - Network security, hardware security, mobile security ...
- **In this course, we focus on *software security***
  - What kind of software **vulnerabilities** exist
  - How hackers can **exploit** those vulnerabilities
  - How to **prevent** hackers from exploiting those vulnerabilities
  - How to **detect** software vulnerabilities automatically (tentative)



Vulnerability

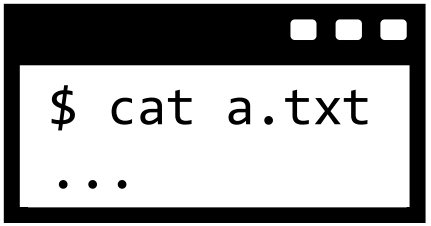
Exploitation

Mitigation

Detection

What Kind of Software?

- **Software exists everywhere, in various forms**
- **We mainly focus on Linux applications**
  - Good environment to learn and practice important concepts
- **We will briefly cover OS security and web security, too**
  - OS is a special type of software
  - Dynamic webs and web apps can be thought as software, too



Linux application

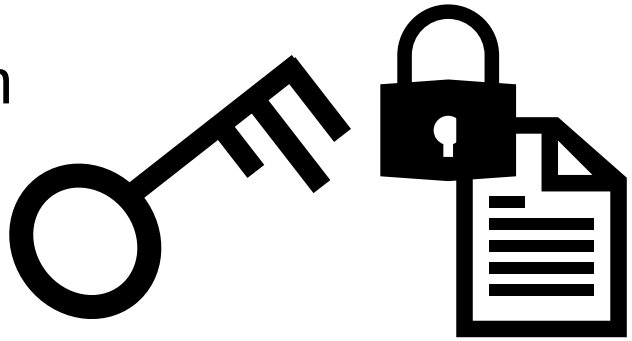
Operating system

Web application

What about Cryptography, etc.?

- **Cryptography is a strong and important tool for security**
  - But it's a *misconception* to equate *security* with *cryptography*
  - There is a separate course for cryptography (CSE4188), so we will not discuss it in this course
- **There are many other fields in security as well, such as *network security*, *hardware security*, etc.**
  - But these topics require lots of field-specific knowledges
  - Ex) You must know *network* well before learning *network security*

Encryption & Decryption

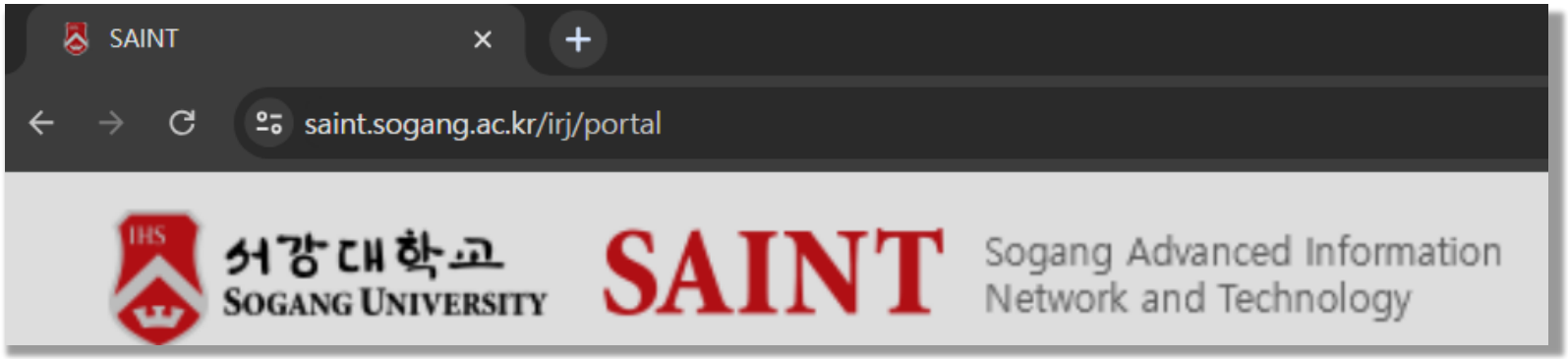


Today's Topic

- **Goal and scope of this course**
  - Software security
- **Basic concepts and terminologies in security**
  - CIA properties
  - Common types of attacks
  - Threat model

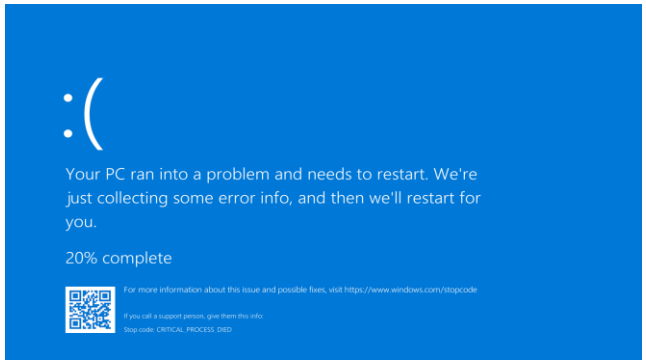
The CIA Properties

- **Key properties that we want to achieve for security**
  - **Confidentiality**: secrets must be kept secret
  - **Integrity**: data should not be tampered
  - **Availability**: the system must be usable
- **Ex) Consider the *SAINT* system of our university**
  - Your grade must be visible/modifiable by authenticated users
  - The system must not go down



Common Types of Attacks

- **Denial-of-service**
  - Shutting down your system or service running on it

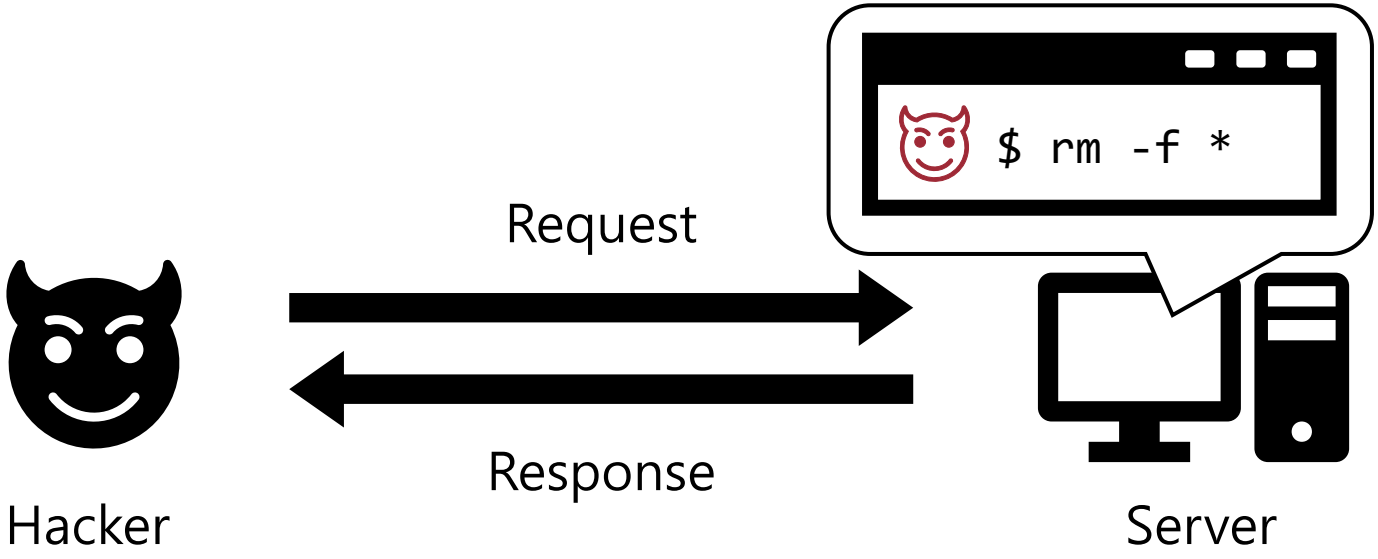


Blue Screen of Death

503 Error

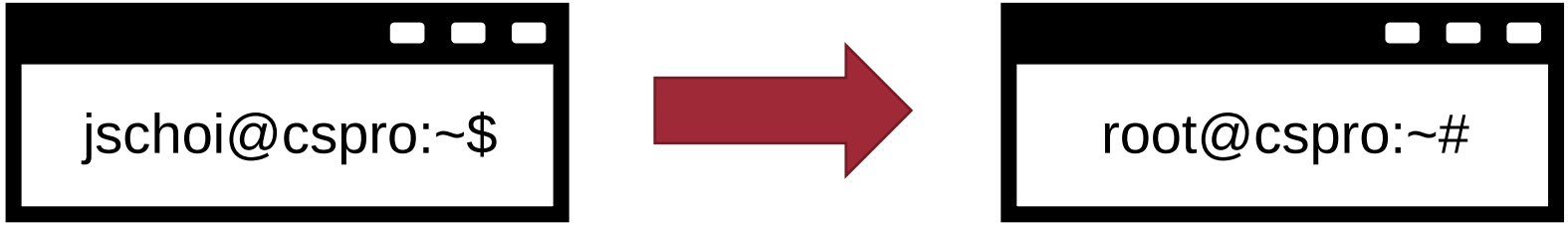
Common Types of Attacks

- **Denial-of-service**
  - Shutting down your system or service running on it
- **Code execution**
  - Running arbitrary, unintended code in your system



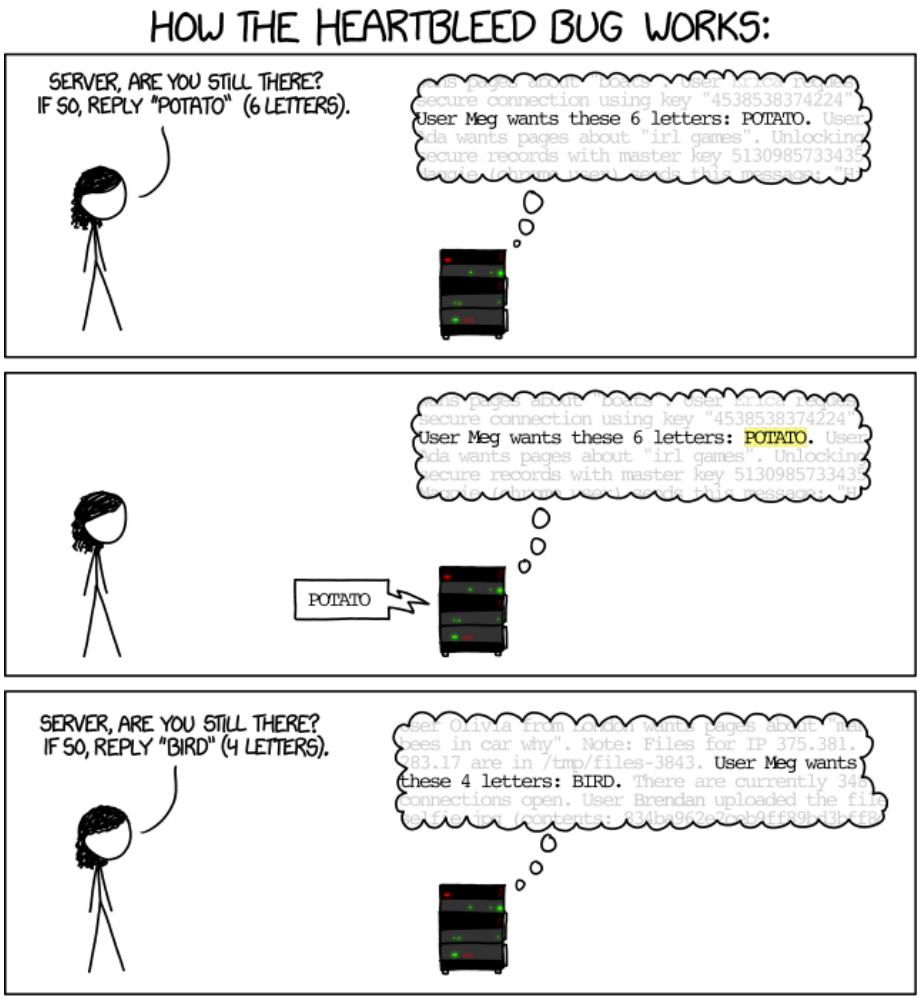
Common Types of Attacks

- **Denial-of-service**
  - Shutting down your system or service running on it
- **Code execution**
  - Running arbitrary, unintended code in your system
- **Privilege escalation**
  - Gaining unintended privileges



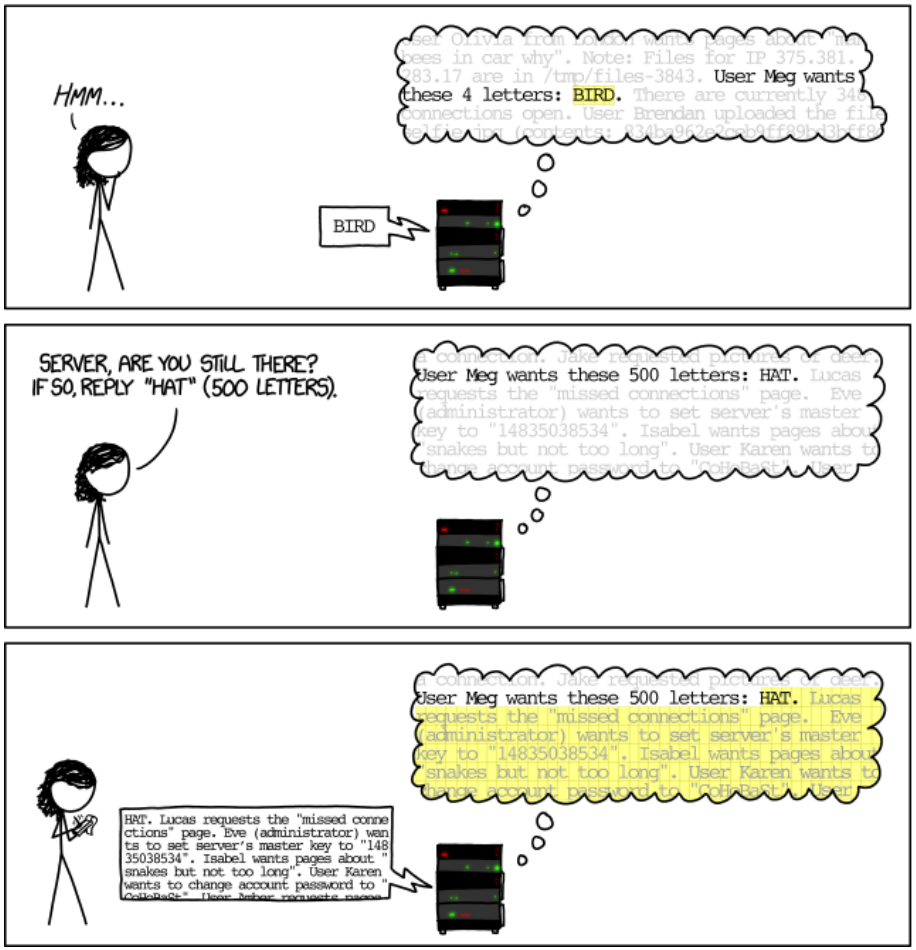
Common Types of Attacks

- **Denial-of-service**
  - Shutting down your system or
- **Code execution**
  - Running arbitrary, unintended
- **Privilege escalation**
  - Gaining unintended privileges
- **Information leakage**
  - Accessing sensitive data
  - Ex) Heartbleed bug



Common Types of Attacks

- **Denial-of-service**
  - Shutting down your system or
- **Code execution**
  - Running arbitrary, unintended
- **Privilege escalation**
  - Gaining unintended privileges
- **Information leakage**
  - Accessing sensitive data
  - Ex) Heartbleed bug



Threat Modeling

- **Broad meaning:** the overall process of identifying system's potential vulnerabilities and threats
- In **narrow meaning,** threat model usually specifies:
  - What is legitimately allowed for arbitrary users (including hacker)
  - What hackers want to achieve by exploiting vulnerabilities
  - Which *attack surfaces* hackers can target
  - Ex) Consider a scenario where one of the students in this class tries to attack CSPRO server: What is the *threat model?*
    - Of course, you must never do this!