CSE551: Advanced Computer Security

1. Introduction

Seongil Wi

Department of Computer Science and Engineering

Who am I?

about:Seongil Wi

- Assistant professor
- Security researcher

- Office: E106, 301-8
- Office Hour: Tuesday, 2~3pm (by appointment)
  - 🏠 Homepage: https://seongil-wi.github.io/
  - ✉ Email: seongil.wi@unist.ac.kr

My Research

- UNIST CSE / WebSec Lab. (Web Security Lab)
  - 🏠 Homepage: https://websec-lab.github.io/

Web Security Lab

- Research keywords:
  - **Web and Software Security**
  - Client/Server-side Security
  - Web Vulnerability Discovery

My research is all about building systems that automatically **analyze** and **find** security bugs in web components

My research is all about building systems that automatically **analyze** and **find** security bugs in web components

Research Method Program analysis, Measurement

My research is all about building systems that automatically **analyze** and **find** security bugs in web components

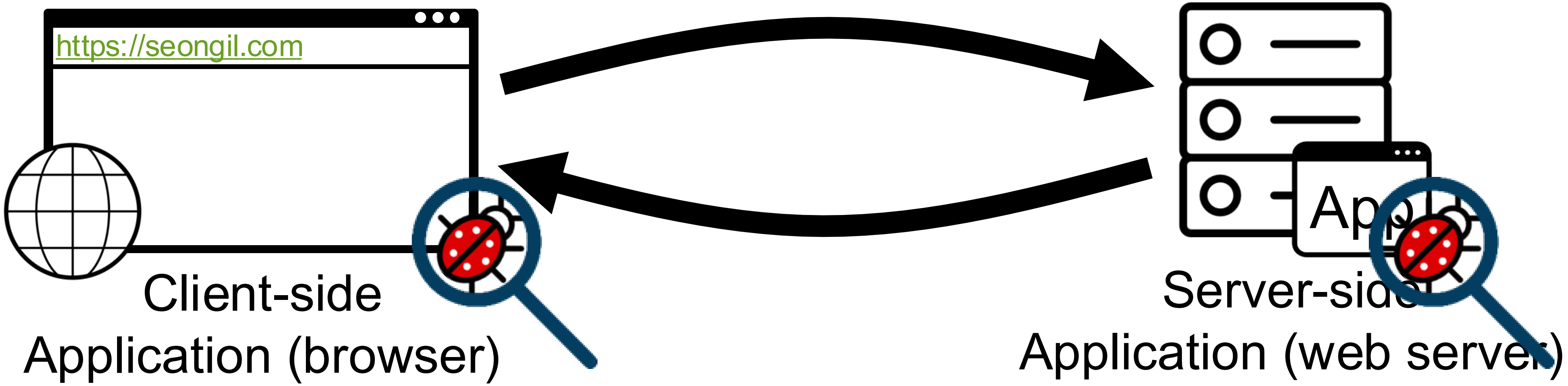
Research Method Program analysis, Measurement

Research Target

My research is all about building systems that automatically **analyze** and **find** security bugs in web components

Research Method Program analysis, Measurement

Research Target Web applications and platforms



https://seongil.com

App

Client-side Application (browser)

Server-side Application (web server)

WebSec Lab (Web Security Lab)

- Finding **security bugs** in web components (applications, browsers, …)
- Finding and measuring **emerging web threats**
- Analyzing online **criminal activities**
- Using…
  - Dynamic/static analysis
  - Clone detection
  - AI techniques
  - Etc.

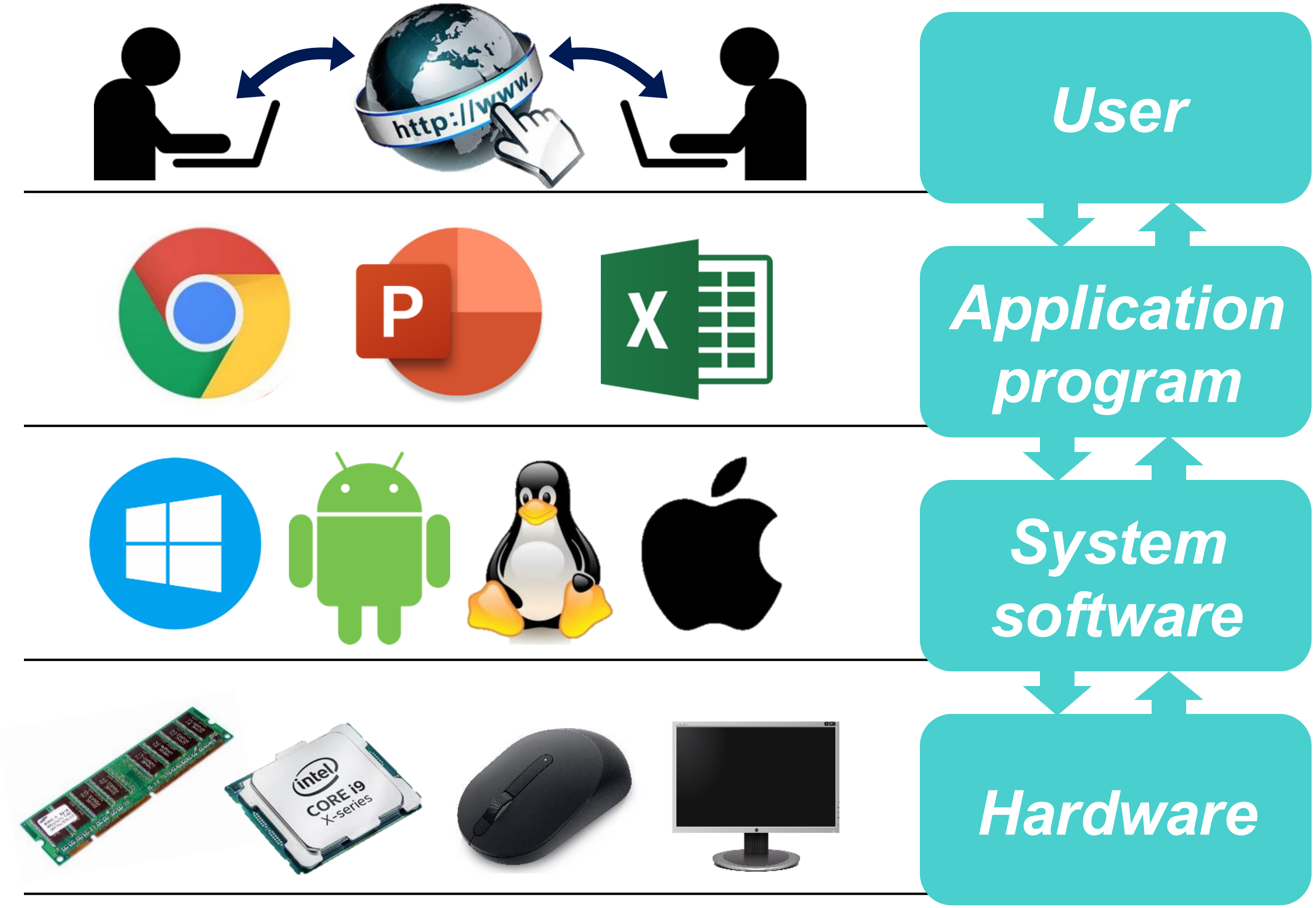
Making ***web ecosystems***
more *secure!*

This Course

Advanced Computer Security

Computer Security

The protection of **computer systems** from unauthorized access



User

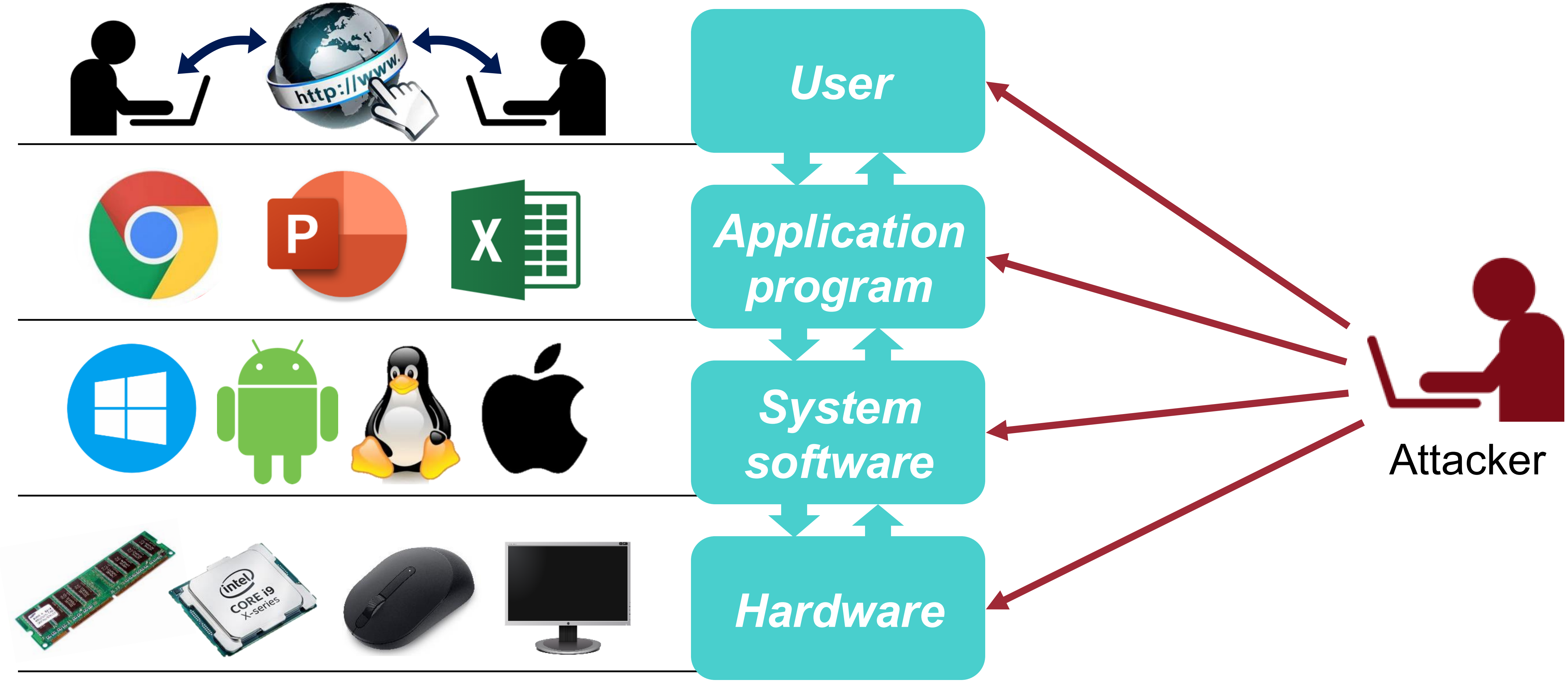
Application program

System software

Hardware

Course Objectives: Principles

The protection of **computer systems** from unauthorized access



User

Application program

System software

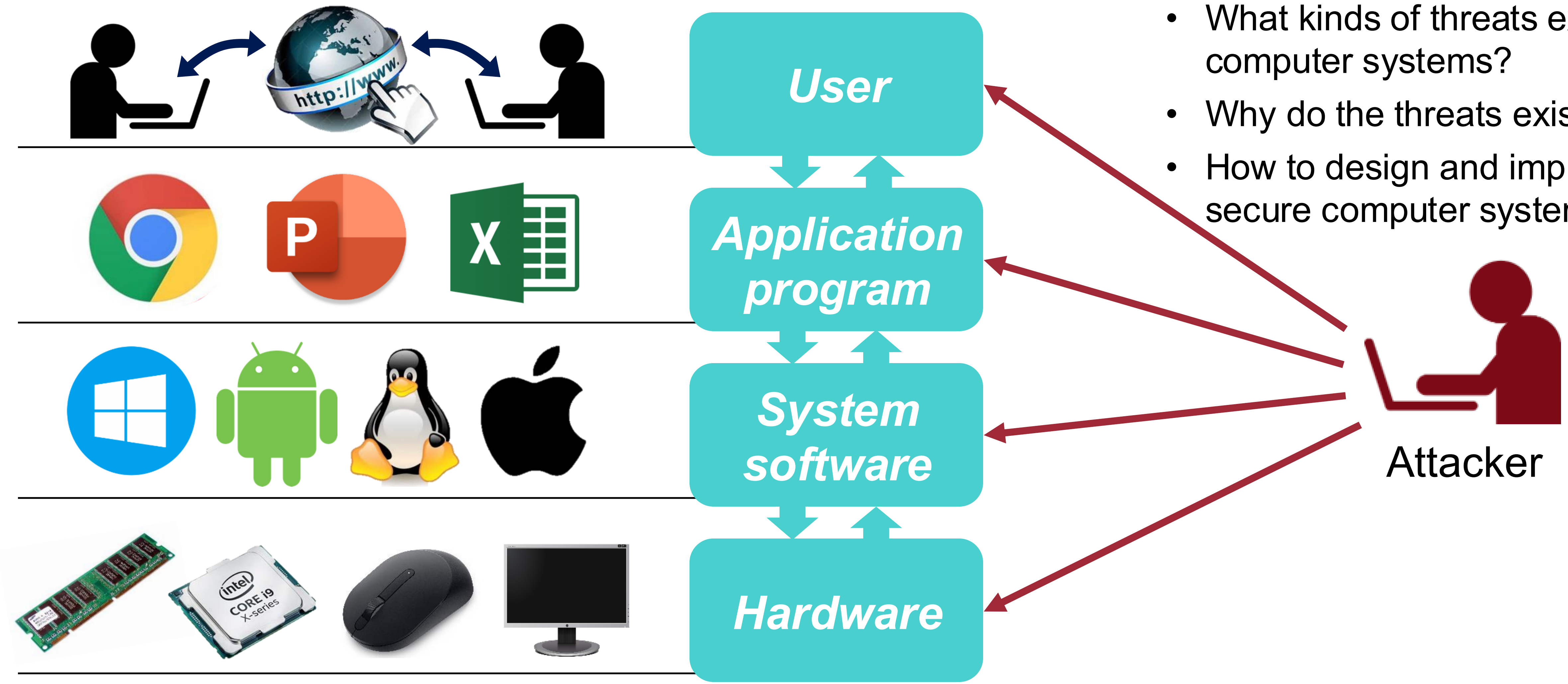
Hardware

Attacker

Course Objectives: Principles

The protection of **computer systems** from unauthorized access

- What kinds of threats exist in computer systems?
- Why do the threats exist?
- How to design and implement secure computer systems?



User

Application program

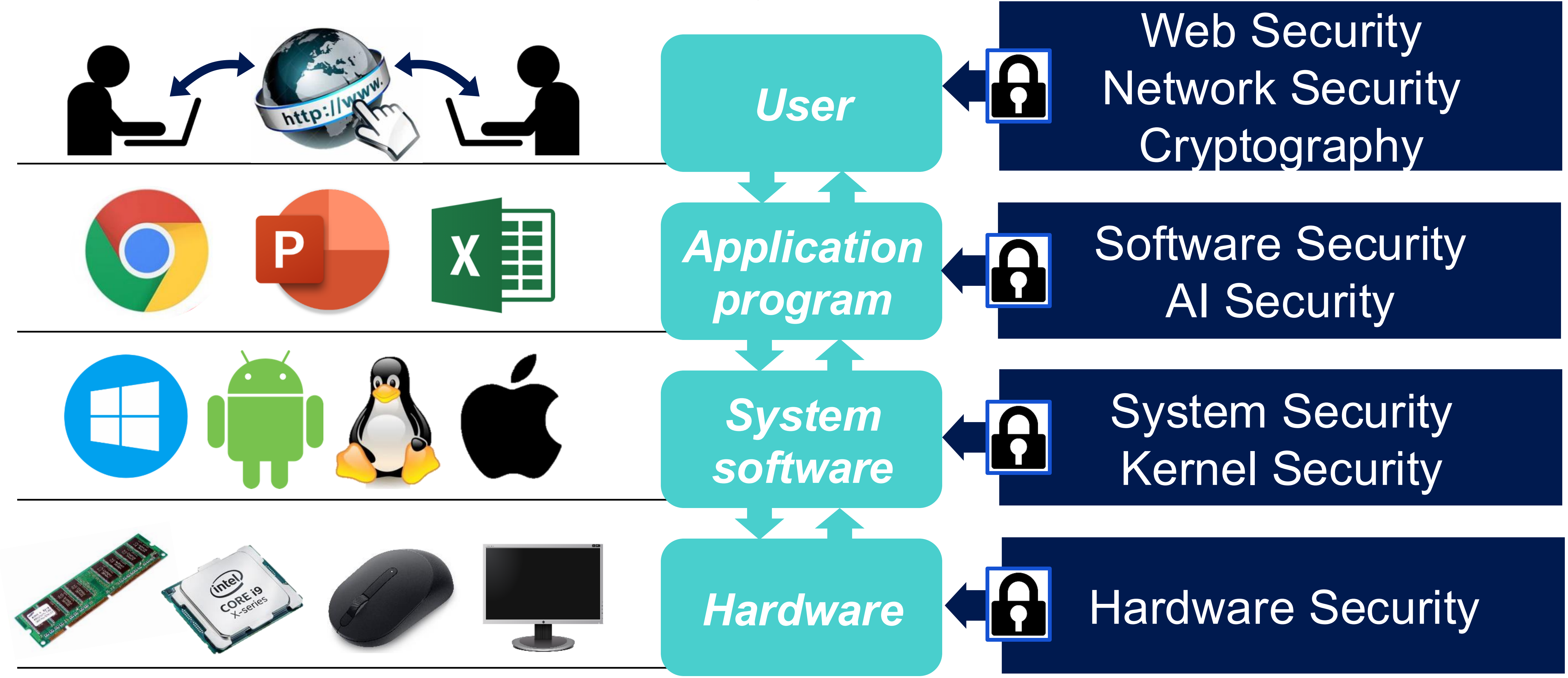
System software

Hardware

Attacker

Course Objectives: Principles

The protection of **computer systems** from unauthorized access



User

Application program

System software

Hardware

Web Security
Network Security
Cryptography

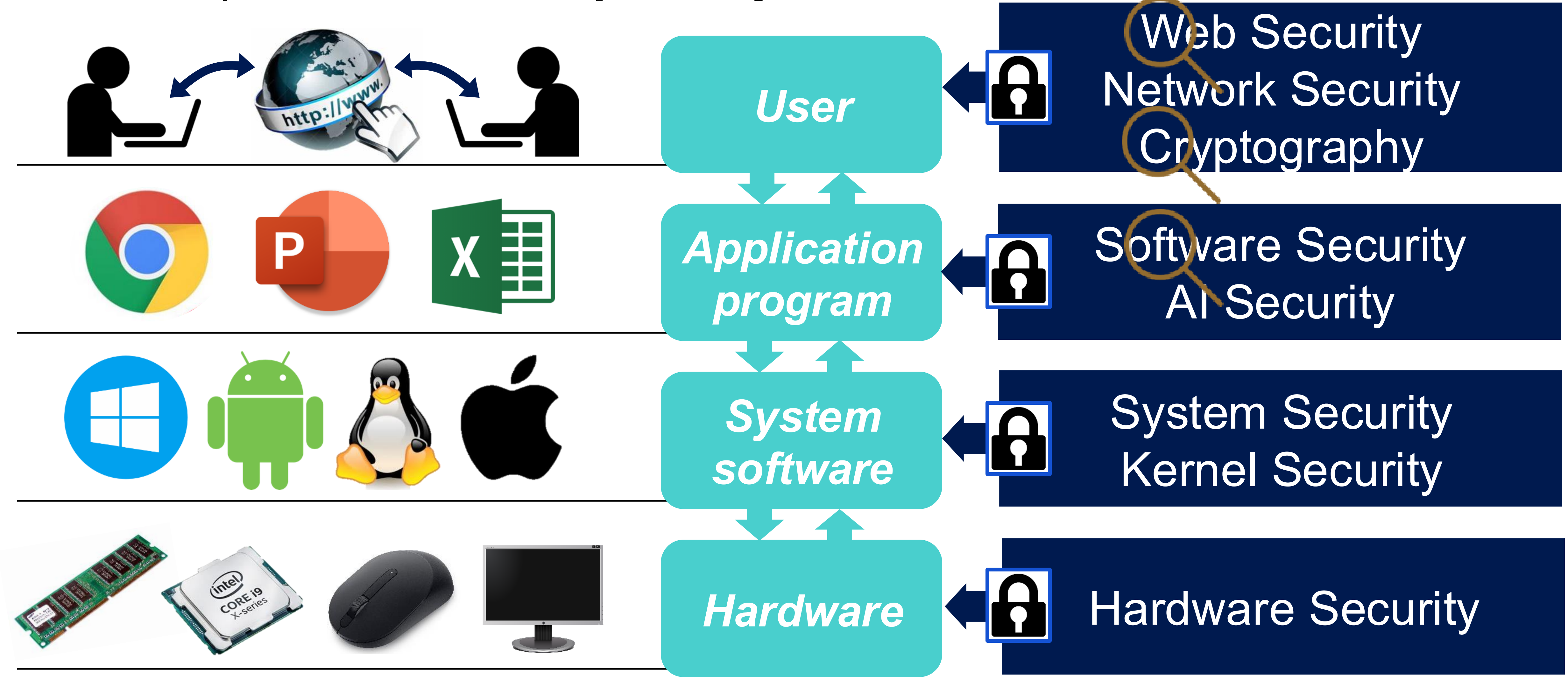
Software Security
AI Security

System Security
Kernel Security

Hardware Security

This Course

The protection of **computer systems** from unauthorized access



User

Application program

System software

Hardware

Web Security
Network Security
Cryptography

Software Security
AI Security

System Security
Kernel Security

Hardware Security

Course Information

- **Course Website:**
  - https://websec-lab.github.io/courses/2025f-cse551/
- **Syllabus:** See the course website
- **Textbook:**
  - Lecture slides will be provided
  - See more in the course website

Course Logistics

- **Homework:** 15%
  - Paper summary: three papers

- **Project:** 40%
  - Proposal submission
  - Checkpoint (progress) submission
  - Final presentation
- **Final exam:** 40% (No midterm exam! 😃)

- **Participation:** 5%
  - Active participation including questions, discussions, and activities (online or offline)

Homework: Paper Summary

- Paper #1: A paper related to software security
- Paper #2: A paper related to web security
- Paper #3: A paper related to web security

- Late penalty of 10% per day (up to 3 days)

- Detailed instructions will be announced later

Project

- 1~2 persons for one team
- The topics must be related to the computer security
  - I recommend linking this to your research!

- Submit your proposal by **9/16**

Proposal Submission Guidelines

- You should upload a single PDF file on BlackBored.
- The name of the PDF file should have the following format: `[your ID-last name.pdf]`
  - If your name is Gil-dong Hong, and your ID is 20231234, then you should submit a file named “20231234-Hong.pdf”
  - If your team consists of two people, each member must submit a PDF file

- **Your proposal must follow the following format:**
  - Template: Double-Column ACM format (Sigconf style) – provided on BlackBored
  - 2 pages maximum (reference is excluded)
  - Format: Background, Motivation, Proposed Idea, Expected Results, Research Timeline, (+Role and Responsibility, if the team has two members), Reference

FYI: Project Ideas

- Software testing, Bug finding
    - IoT devices, routers and others
- Suggest system/hardware-level defenses
- Extract secret keys from applications
- Finding fishing websites using novel approaches
- Cross-site communication
- Finding browser bugs
- …

Attendance

Attendance is, of course, mandatory and enforce UNIST attendance rules

- **I will not include your attendance score in the grade**
  - **However,** I will drive the course in a way that rewards those who consistently participate with higher scores!

- **Also, missing more than 8 times will get an 'F'**
  - Your responsibility to check attendance online!
  - If you attend and leave immediately (출튀), there will be a grading penalty
  - Show me evidence in case of an unavoidable absence, e.g., military training, illness, funeral
  - There is no excuse for absences due to your decision, e.g., interviews, competition participation

Attendance

Attendance is, of course, mandatory and enforce UNIST attendance rules

- **I will not include your attendance score in the grade**
  - **However,** I will drive the course in a way that rewards those who consistently participate with higher scores!
- **Also, missing more than 8 times will get an 'F'**
  - Your responsibility to check attendance online!
  - If you attend and leave immediately (출튀), there will be a grading penalty
  - Show me evidence in case of an unavoidable absence, e.g., military training, illness, funeral

I expect you to be here, as you expected me to be here!

Class

- **Language:** English (default)
- **Attendance:** always (default), absence (if necessary)
  - No quantified attendance score
- **Questions & discussion (either in Korean or in English):** highly encouraged
  - (Out-of-class) If you have questions: blackboard
  - Except for
    - Too detailed ones
    - Directly related to the solutions
- **Actively discuss with your classmates**

Question?

Today, everyone will be acknowledged for attendance!