

CSE467: Computer Security

1. Introduction

Seongil Wi

Who am I?

about:Seongil Wi



- Assistant professor
- Security researcher

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

- MBTI: ISFJ



My Research



- UNIST CSE / WebSec Lab. (Web Security Lab)
 - 🏠 Homepage: <https://websec-lab.github.io/>
- 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 Input generation!

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

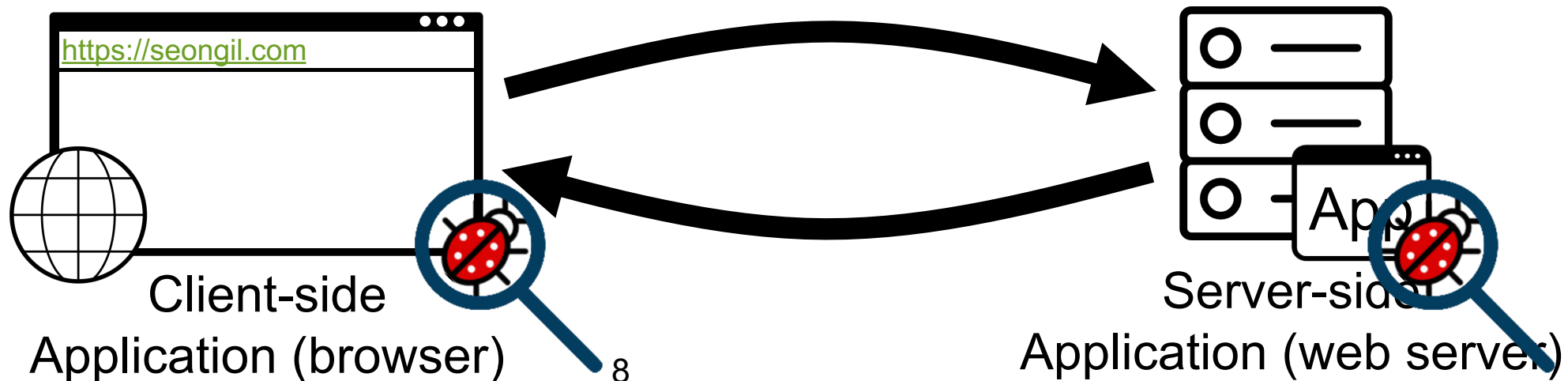
Research Method Input generation!

Research Target

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

Research Method Input generation!

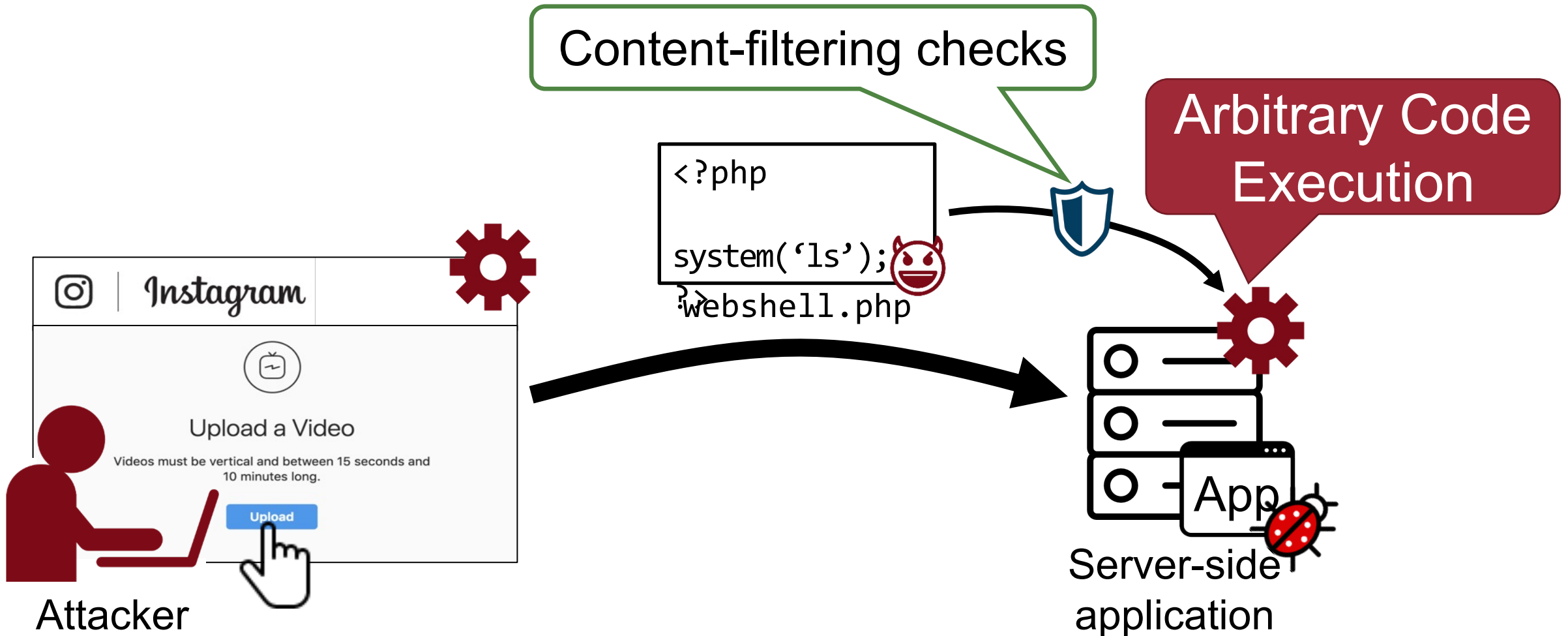
Research Target Web applications and platforms



My Research: Finding File Upload Bugs

9

Research Target Server-side applications (upload system)



My Research: Finding File Upload Bugs

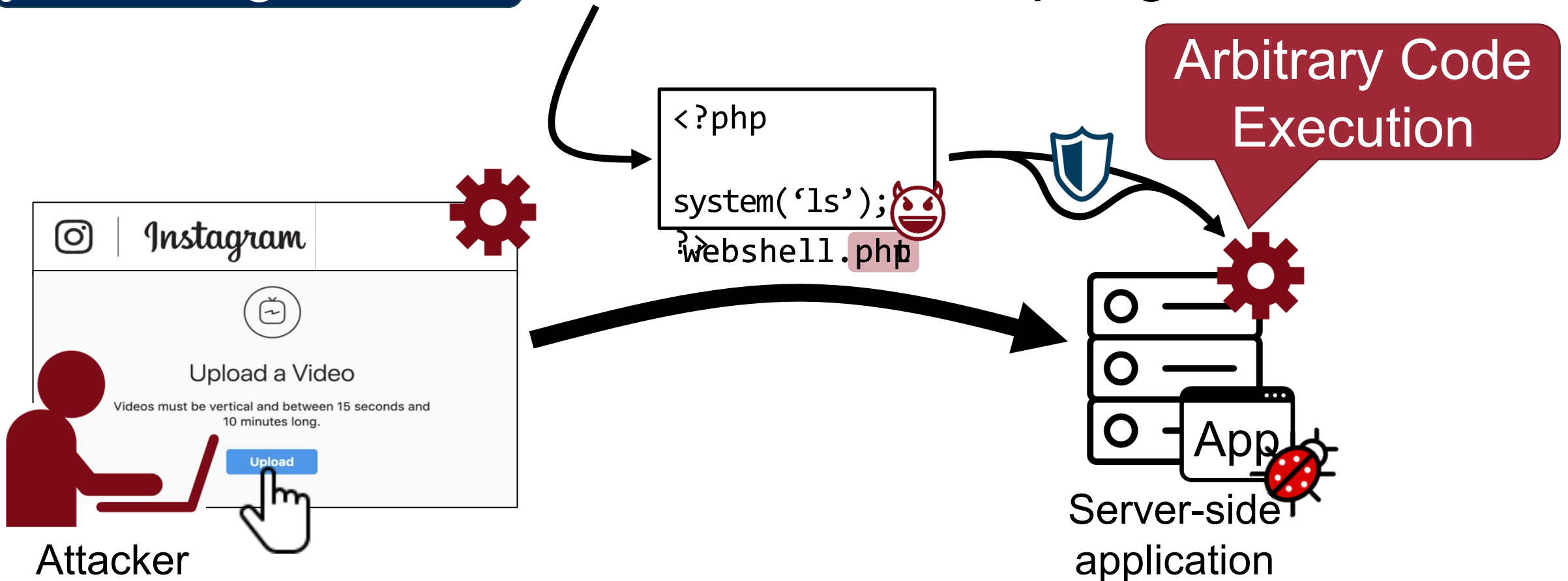
10

Research Target

Server-side applications (upload system)

Testing Method

Mutation-based input generation



My Research: Finding File Upload Bugs

11

Research Target

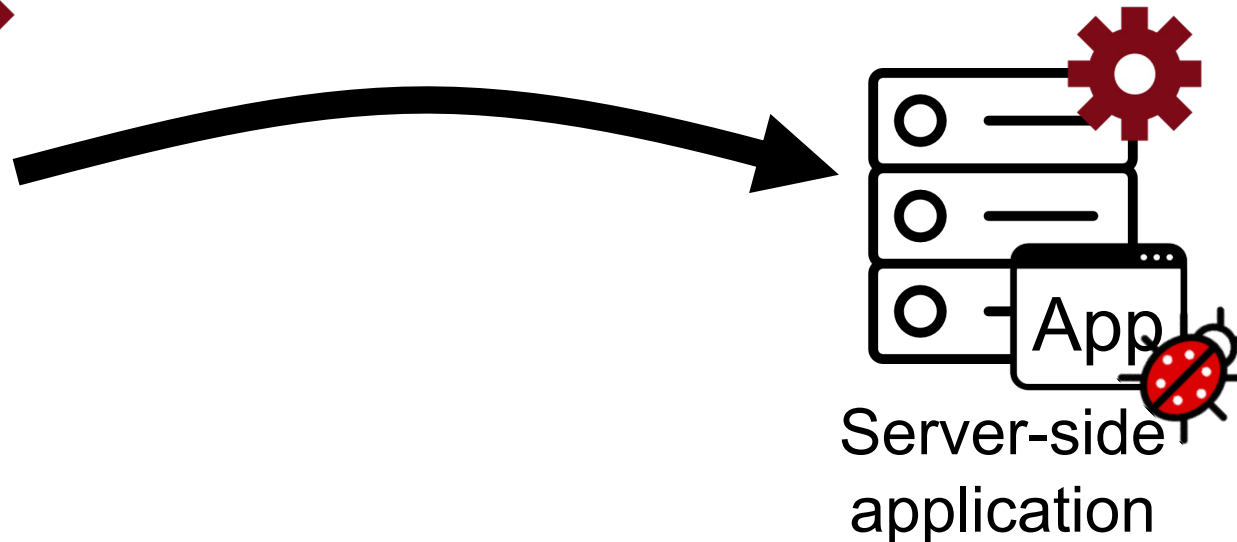
Server-side applications (upload system)

Testing Method

Mutation-based input generation

Result

- Found **30 file upload bugs** in 23 applications
- 13 bugs have been patched (Rewarded \$4,000)
(550만원)
- Published in *NDSS'20*



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

*Feel free to contact me,
if you are interested in
web security 😊*

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

This Course

Course Information



- **Course Website:**
 - <https://websec-lab.github.io/courses/2023f-cse467/>
- **Syllabus:** See the course website
- **TA:**
 - Dongyeon Yu (유동연, dy3199@unist.ac.kr)
- **Textbook:**
 - Lecture slides will be provided
 - See more in the course website

Grading



- **Homework:** 45%
 - 1~2 Programming assignment
 - 2 Capture-the-flag (CTF) event (basic hacking practice)
- **Quizzes:** 10% (2~3 quizzes)
- **Final exam:** 35% (No midterm exam! 😊)
- **Participation:** 10%
 - Active participation including questions, discussions, and activities (online or offline)

Important Notice (1): Academic Integrity 16



- DO NOT share the course contents (e.g., assignments or exams) with others
 - E.g., Github public repository, chegg.com, etc
- DO NOT discuss the details of solutions with others
- DO NOT plagiarize
 - Submit your own work
- Any integrity violation: at **LEAST F**

UNIST CSE Policy on Cheating and Plagiarism

Note: The term **solution** means program code, mathematical derivation, experimental setup, etc., for any type of deliverable, homework assignment, or projects in class.

The purpose of this document is to make our expectations in CSE as clear as possible in regard to the Honor Code at UNIST. The basic principle under which we operate is that each of you is expected to **submit your own work in your courses**. In particular, attempting to take credit for someone else's work by turning it in as your own constitutes plagiarism, which is a serious violation of fundamental academic standards. However, you are also encouraged to work as a team and collaborate with each other, and it is usually appropriate to ask others—the TA, the instructor, or other students—for direction and debugging help or to talk generally about

Important Notice (2): Class



- **Language:** English (default)
- **Attendance:** always (default), absence (if necessary)
 - No quantified attendance score
 - But, you must attend at least 3/4 of all classes
 - I expect you to be here, as you expected to be here!
- **Questions & discussion (either in Korean or in English):** highly encouraged
 - (Out-of-class) If you have questions: blackboard > TA > instructor
 - Except for
 - Too detailed ones (TA is not a debugger!)
 - Directly related to the solutions
- **Actively discuss with your classmates**

Computer Security

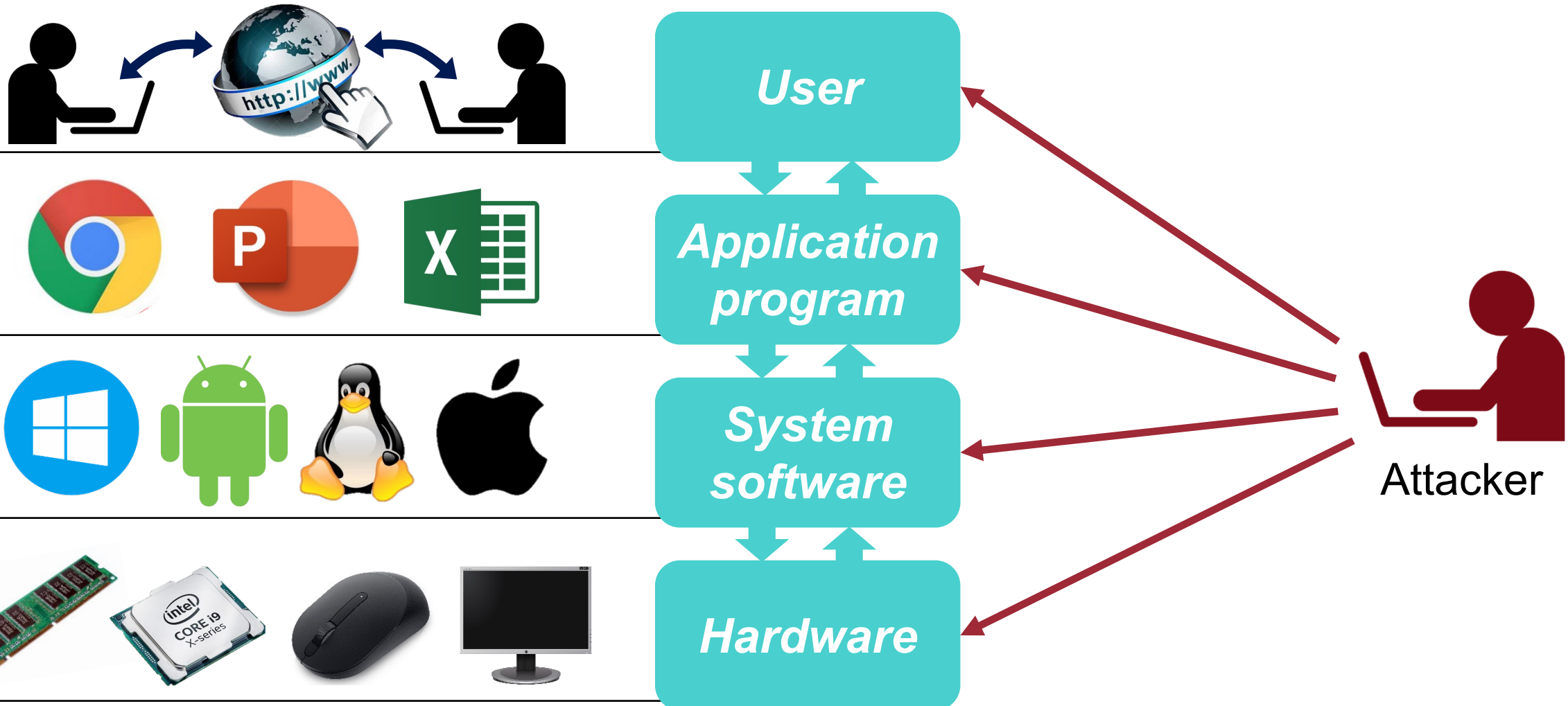
18



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

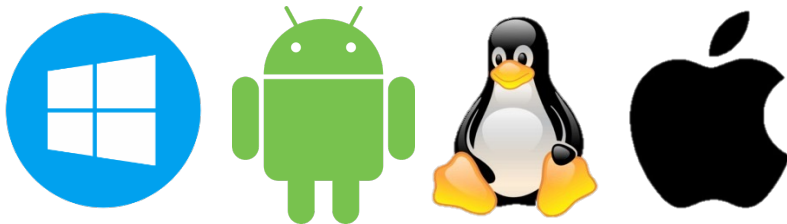
Course Objectives: Principles

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



Course Objectives: Principles

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



User

Application program

System software

Hardware

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



Course Objectives: Principles

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



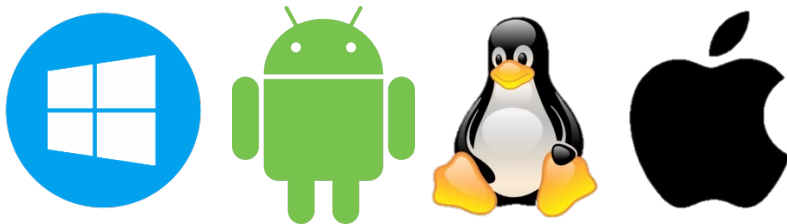
User

Web Security
Network Security
Cryptography



Application program

Software Security
AI Security



System software

System Security
Kernel Security



Hardware

Hardware Security

Homework



- **#1: Hacking practice**
 - Software security, Web security, ...
- **#2: Programming assignments**
 - Cryptography, Network security, ...
- Late penalty of 10% per day
- Detailed instructions will be announced later



Q. Is it okay to send a email at midnight?

– Of course! No one cares.

Q. I am not familiar with hacking and computer security.

– Your main goal is to learn the basics of the computer security.

Q. Is it ok to use ChatGPT for the programming assignment?

– Your sub-goal: Learn how to use AI ethically & constructively

Q. What happens if I submit AI-generated code?

– If unlucky, detected by our clone checker. You will get F. If lucky, you get a high score. But will be naturally selected soon.

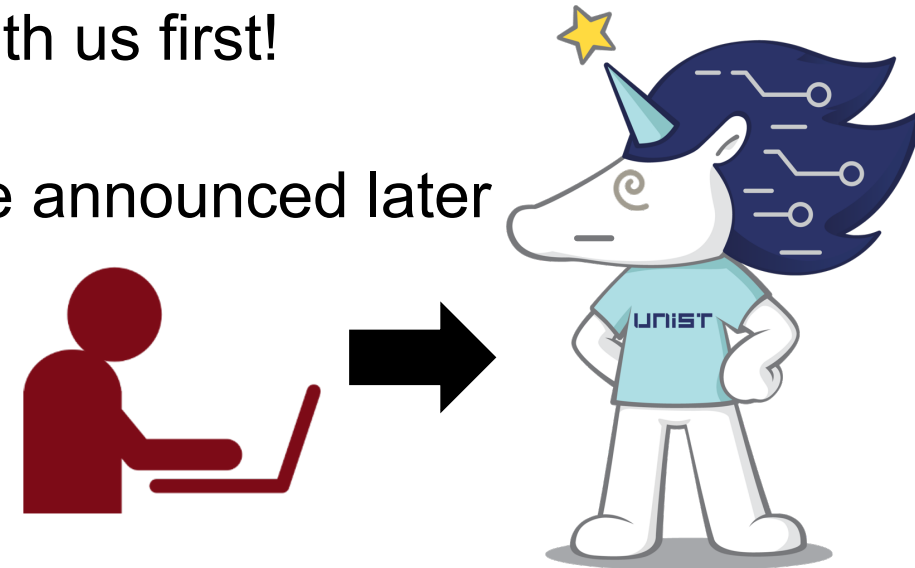
Activities: be a white hacker!

Not mandatory, not homework, but participation is highly recommended to upgrade your score!

Activity (1): SaveUNIST



- If you find unknown security problems on campus, report them to me!
 - Physical (e.g., building) or cyber (e.g., portal, email, etc.)
- Depending on the severity, bonus points will be given
 - E.g., A+ → 1 letter grade up → 10% score up → ... → 1 drink → ...
- **(IMPORTANT!) DO NOT** try anything illegal
 - If you cannot decide by yourself, discuss it with us first!
- Detailed instructions (e.g., period, targets) will be announced later



Hacking Ethics

- Hacking: seek to compromise computer systems or networks by exploiting vulnerabilities
 - E.g., stealing confidential data, DDoS
- White hat hackers: hired for penetration testing to find vulnerabilities
 - Give contributions to the society
 - DO NOT disclose the bug publicly before the fix is released
 - DO NOT exploit
- Be careful! UNIST is a national institute

징 제 공 고

생활관 전산망 해킹 학생에 대하여 아래와 같이 징계 조치가 되었습니다. 이는 우리 학교의 인재상인 “남을 배려할 줄 아는 정직한 인성을 가진 사람”에 위배되는 사건으로 매우 유감스럽게 생각합니다.

재학생들은 학칙 및 학생징계 규정에 의거한 해당 학생의 징계내용을 확인하고, 유사 사례 적발 시 **중징계 할 예정**이오니 이러한 사례가 발생되지 않도록 각별히 유념하기 바랍니다.


성명	징계내용	징계사유	제한사항
○○○ ○○○	유기정학	생활관 웹사이트 해킹	1. 학칙위 기제 2. 장학금 지급 제한 3. 생활관 인사 제한 4. 징계기간 수강 및 학생활동 금지

검 인

2017. 03. 10

학생처장

2017. 3. 2.

UNIST  GUKJENews

Activity (2): HackGPT



- Does ChatGPT become a friend or villain?
- **Report NEW security threats that can be caused by ChatGPT!**
 - Read “Large Language Models like ChatGPT say The Darnedest Things”, **CACM’23**
 - DO NOT report known issues (e.g., generating buggy code): a lot of studies already done
 - Describe a concrete and detailed scenario



- Detailed instructions (e.g., period) will be announced later

Question?