

CSE467: Computer Security

1. Introduction

Seongil Wi

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

- 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 Program analysis!

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

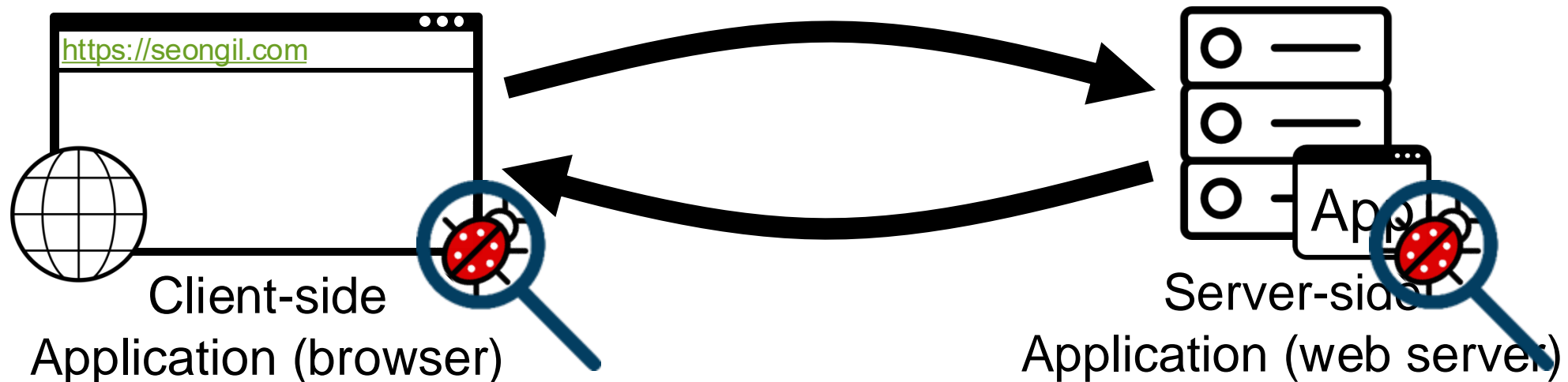
Research Method Program analysis!

Research Target

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

Research Method Program analysis!

Research Target Web applications and platforms

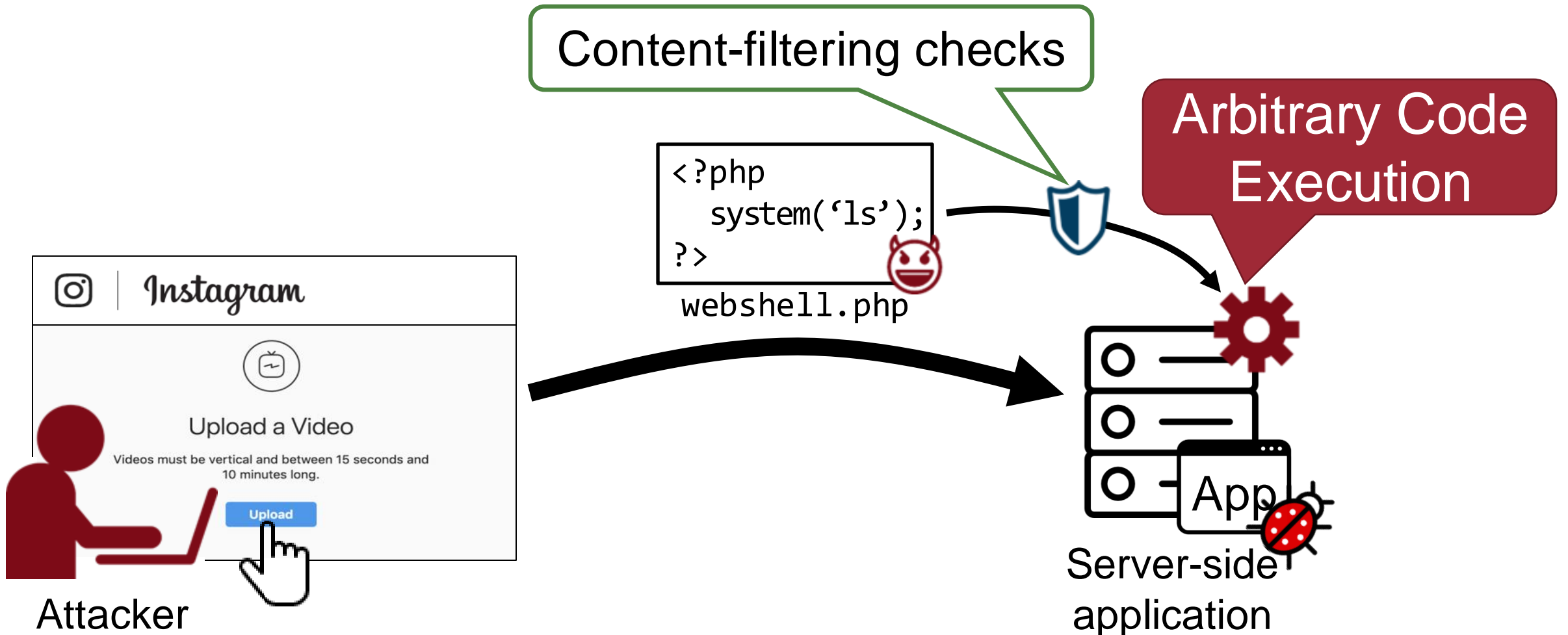


My Research: Finding File Upload Bugs

9

Research Target

Server-side applications (upload system)



My Research: Finding File Upload Bugs

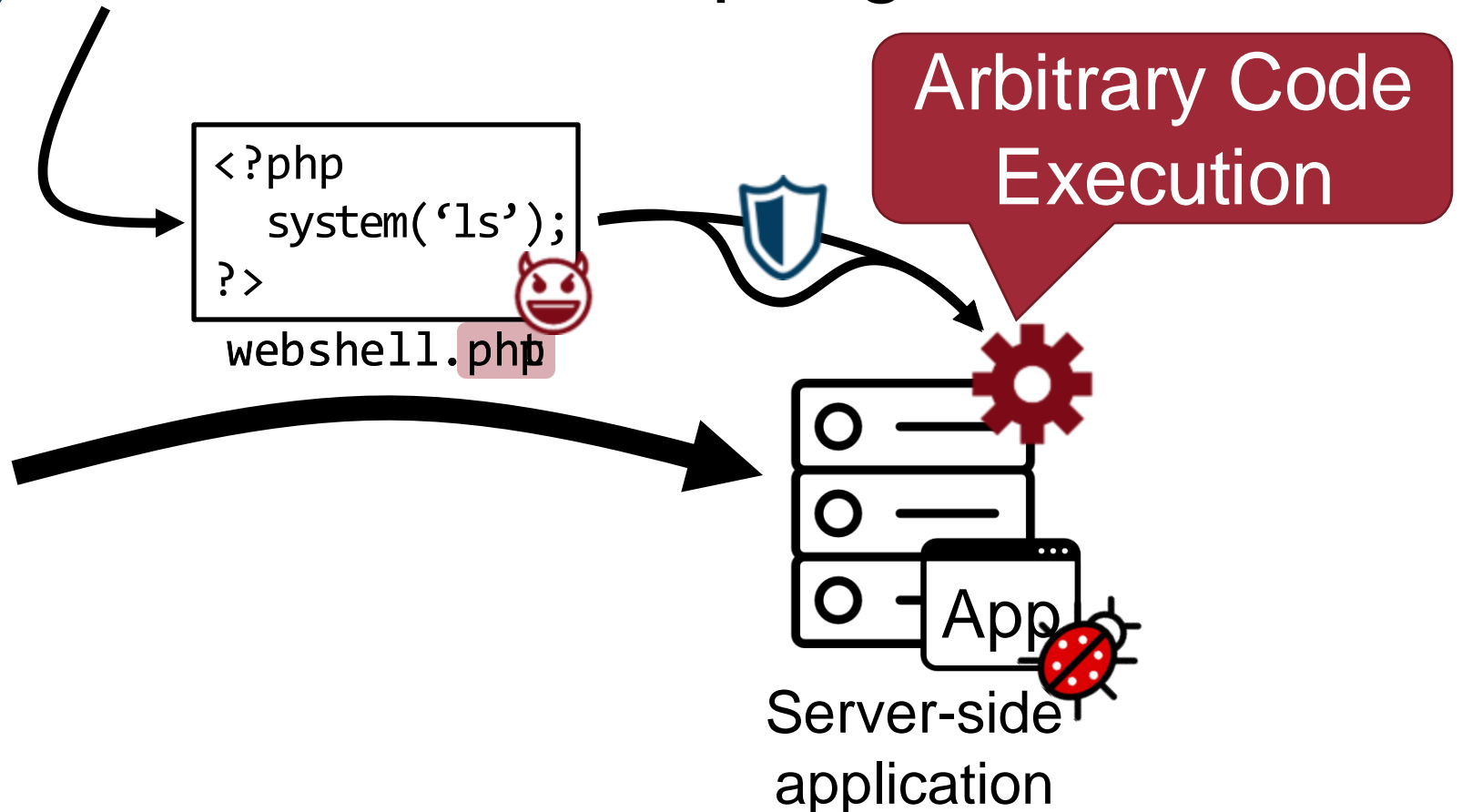
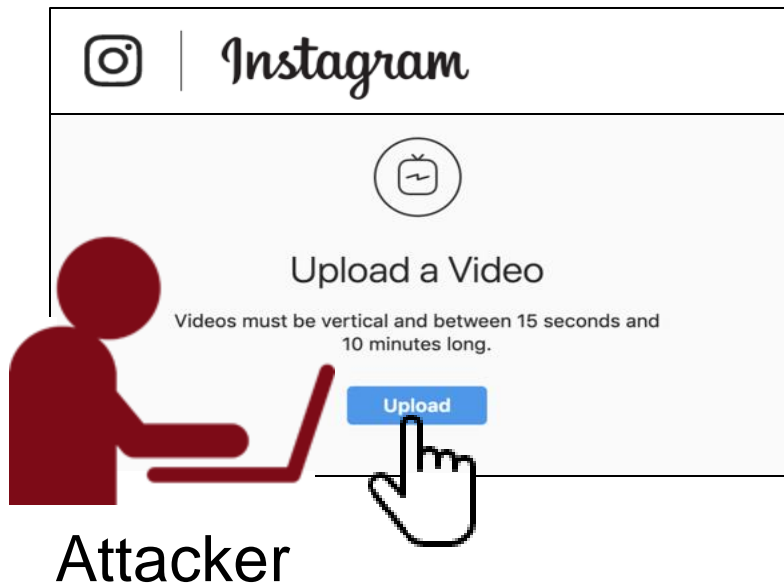
10

Research Target

Server-side applications (upload system)

Testing Method

Mutation-based input generation



My Research: Finding File Upload Bugs

11

Research Target

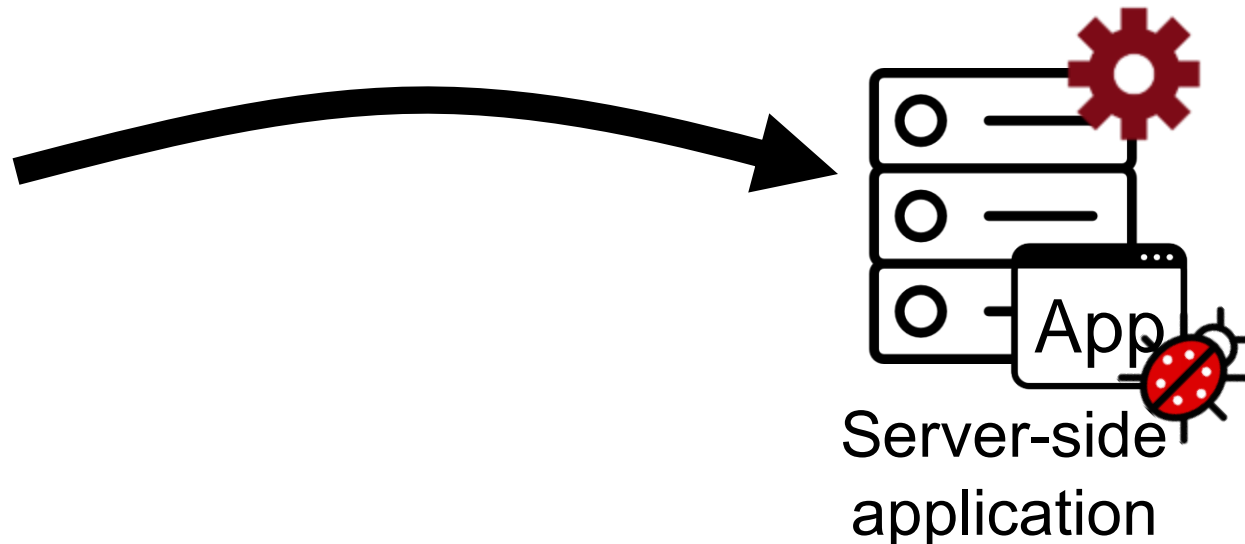
Server-side applications (upload system)

Testing Method

Mutation-based input generation

Result

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



- 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

Computer Security

Computer Security



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



User



*Application
program*



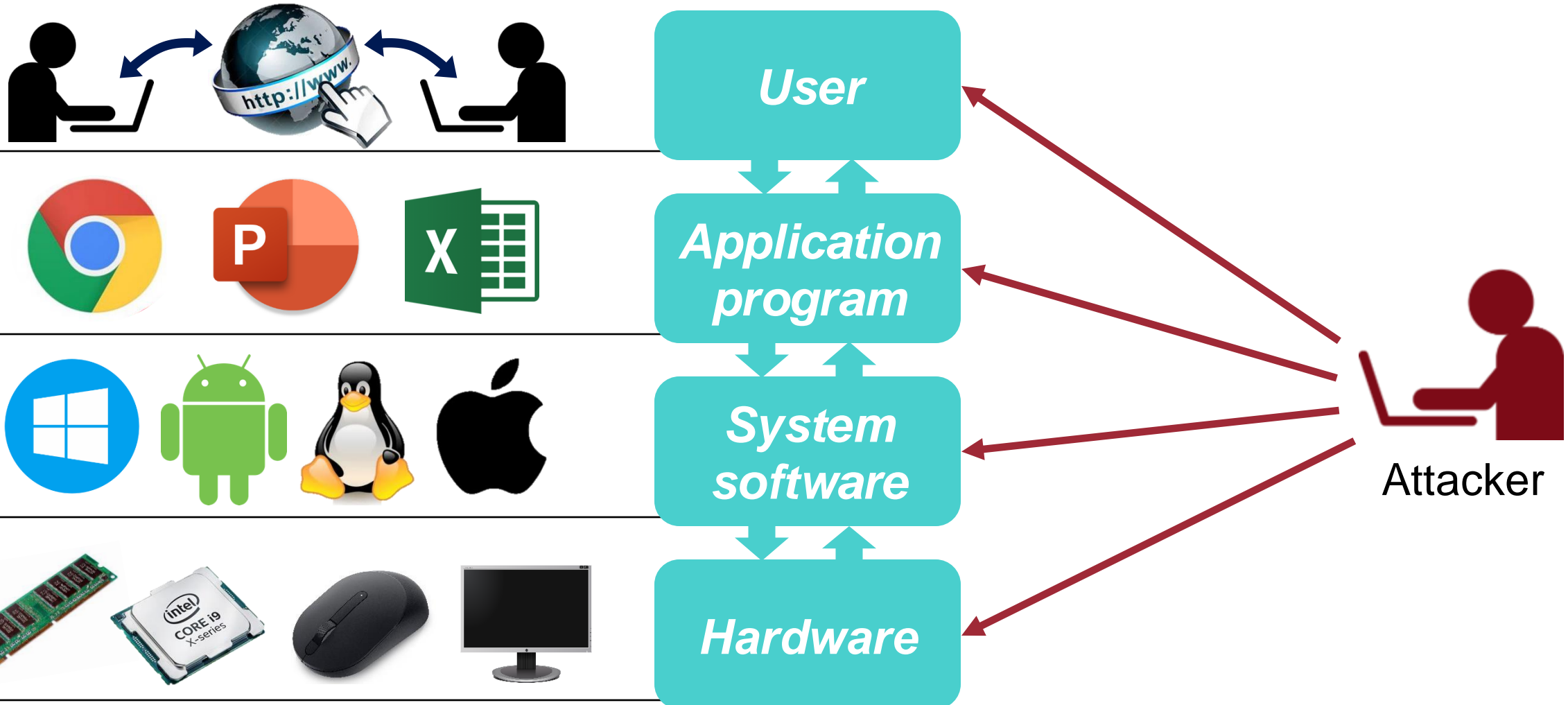
*System
software*



Hardware

Course Objectives: Principles

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



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?



Attacker

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

Course Information



- **Course Website:**
 - <https://websec-lab.github.io/courses/2025s-cse467/>
- **Syllabus:** See the course website
- **TA:**
 - Jaeho Bae (배재호, bjho@unist.ac.kr)
 - Zeewung Shin (신지웅, zeeshin@unist.ac.kr)
- **Textbook:**
 - Lecture slides will be provided
 - See more in the course website

Course Logistics



- **Homework:** 45%
 - 1~2 Programming assignment
 - 2 Capture-the-flag (CTF) event (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 20

Any solution you submit (hw, exam, etc.) must be your **own** work

If you violate this rule,
you will immediately get an **F**

Important Notice (1): Academic Integrity 21



- 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): 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 (출퇴), 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

Important Notice (2): 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 (출퇴), 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!

Important Notice (3): 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 > TA > instructor
 - Except for
 - Too detailed ones (TA is not a debugger!)
 - Directly related to the solutions
- **Actively discuss with your classmates**

Important Notice (4): Blackboard Participation

- We will use Blackboard discussions for Q&A
- We will check **your participation** in the discussion
- If you answer other students' questions, and if the answer is valid one, you will receive bonus point!



Computer Security

Q&A

Discussion

Student Activity

Discussion Topic

  Unfollow

Leave any questions related to the course here.

- You may also answer your peers' questions. The person who submits a valid answer first will **receive bonus points** (Tip: Click the "follow" button for this Q&A discussion. Blackboard mobile app will give push notifications whenever a new question is posted).

Homework



- **#1: Hacking practice**
 - Software security, Web security, ...
- **#2: Programming assignments**
 - Cryptography, Network security, ...
- Late penalty of 10% per day (up to 3 days)
- Detailed instructions will be announced later



Q. Is it okay to send an 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.

Special Activity: Hack Class101!

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

Motivation



[클래스101] 정보 보안 컨설팅 문의 드립니다.

[Class101] Inquiry about Security Consulting



Injung Chung <hero@101.inc>

02-18 (화) , 오후 6:18

Seongil Wi / 위성일 (CSE) ✎

Hack Class101 (Collaboration with Calss101)



- Find unknown security issues on Class101 websites!
- Instruction: <https://bounty.class101.net/>
 - Foreigners should use a translator
- Activity period: 03/03 ~ 06/18
- **DO NOT** try anything illegal!

Hacking Ethics

- Hacking: seek to compromise computer systems or networks by exploiting vulnerabilities
 - E.g., stealing confidential data, DDoS
- White hat hackers: hired to find vulnerabilities
 - Give contributions to the society
 - **DO NOT** disclose the bug publicly before the fix is released
 - **DO NOT** see/change the other user's information

징 계 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 예정이오니 이러한 사례가 발생되지 않도록 각별히 유념하기 바랍니다.

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

검인

2017. 03. 10

학생처장

2017. 3. 2.

UNIST GUKJENew

Hack Class101: Email Submission Form



- **TO:** seongil.wi@unist.ac.kr
- **CC:** infra@101.inc, bjho@unist.ac.kr
- **Title:** [Hack Class101,ID,Name] Title of the vulnerability
- **Content:**
 - Bug description
 - Attack step with exploit (It should be reproducible!)
 - Provide a screenshot
 - Describe the security impacts that may occur as a result of the attack

If you do not use this form,
you will not receive bonus points/rewards

Hack Class101: Evaluation Criteria



- The evaluation criteria are as follows:
 - Clarity (of the report)
 - Severity (of the reported vulnerability)
 - Relevance (to this course)
- Depending on the content of your report, you will **receive extra points**
- Additionally, if Class101 provides a **reward**, you will be the one to receive it 😊

Hacking real-world websites is not possible due to ethical issues. Note that this is a very unique and valuable chance to *train your hacking skills on a real-world website!*

This activity is conducted for the security of Class101 and your training.
Prof. Wi will not receive any commission.

Question?

Today, everyone will be acknowledged for attendance!