Lecture 0 – Introduction

[COSE451] Software Security

Instructor: Seunghoon Woo

Spring 2024

Course Information

- **Instructor**: Seunghoon Woo (우승훈)
  - **Assistant Professor,** Dept. of Computer Science and Engineering
  - **Expertise:** Software Security / Supply Chain Security / Vulnerability Detection
    - ❖ Please refer to https://ssp.korea.ac.kr/
  - **Email**: seunghoonwoo@korea.ac.kr
    - ❖ Feel free to contact me; any questions are welcome ☺
  - **Office**: 206B, Woojung Hall of Informatics
    - ❖ Meeting: appointment by an e-mail
  - **TA**: Heedong Yang (양희동)

Textbook

- **Owing to the nature of software security, which changes rapidly every year, the class does not rely on a single textbook**
  - ① "Software Security: Principles, Policies, and Protection", Mathias Payer, 2021 (https://nebelwelt.net/SS3P/)
  - ② "The Cyber Security Body of Knowledge" Version 1.0, Joseph Hallett et al, 2019 (https://www.cybok.org/media/downloads/CyBOK-version-1.0.pdf)
  - ③ "Computer security: principles and practice“, William Stallings and Lawrie Brown, 5th edition, 2023
  - ④ Research papers and articles

Class Schedule

- **Woojung Hall of Informatics, Room 205, Mon/Wed 15:00 – 16:15**
  - Lecture contents and orders can be flexibly tuned

WEEK	CONTENTS
1	Introduction
2	Software Security Principles
3	User Authentication
4	Access Controls
5	Memory Safety
6	Practical Exercises
7	Secure Software Lifecycle
8	**Midterm Exam**

WEEK	CONTENTS
9	Attack Vectors
10	Open-Source Software Security
11	Supply Chain Security
12	Malicious Software
13	Defense Strategies
14	Advanced Topics in Software Security
15	Class Review
16	**Final Exam**

Learning Objectives

- **Why do we study "Software Security"?**

Learning Objectives

- **Why do we study "Software Security"?**
  - As software has become pervasive in our daily lives, the importance of security has increased
  - Among various computer science domains (e.g., network, hardware), flaws existing in software immediately translate into significant threats
    - ❖ Log4j, WannaCry, SolarWinds, etc.
  - Software security is one of the most powerful means to effectively respond to security threats!

Learning Objectives

- **Why do we study "Software Security"?**

<https://securityboulevard.com/2021/12/log4j-the-meme-0/>

<https://monetd.github.io/security/Log4j%28Log4jShell%29-%EC%B7%A8%EC%95%BD%EC%A0%90-%EB%B6%84%EC%84%9D/>

<https://www.reddit.com/r/ProgrammerHumor/comments/rgvbco/yet_another_log4j_meme/>

Class Overview

- **Class contents**
  - Theoretical lectures
    - ❖ Software security knowledge, including attack methods and defense mechanisms
  - Practical exercises (basic software security)
    - ❖ Planning to invite experts
  - Advanced topics
    - ❖ Introduction of research on software security

Class Overview

- **Prerequisite courses**
  - Operating systems and Information Security are recommended before taking this course (but not mandatory)
  - Fundamental knowledge of C/C++
  - When it comes to topics related to Operating Systems (or Information Security), I plan to explain basic concepts as well

Grading

- **Midterm exam 35% & Final exam 35%**
  - Missing any of the two exams without permission / Cheating => F
- **Assignment 20%**
  - One small project related to addressing real-world software vulnerabilities
  - (Temporal) Capture The Flag (CTF) format assignments
  - Failing to submit / Late work / Cheating will result in a penalty to your score
- **Attendance 10%**
  - Self attendance check: please use Blackboard to attend the class
  - Absent more than 1/3 of all classes => F
  - Additional points are awarded for active participation in class

Next Lecture

- **Software Security Principles**
  - Basic terms
  - Basic concepts
  - Security principles