사이버보안개론

Introduction to Cybersecurity

유준수 (Joon Soo Yoo, Ph.D.)

Fall 2026

Defense & Advanced Security Lab (DAS Lab)
Department of Advanced Defense Technology and Industry
Jeonbuk National University

사이버보안개론

Cybersecurity Fundamentals and Offensive Security

1. How This Course Works

이 수업은 크게 두 가지 방식으로 진행한다.

Online Lecture

메인 교재를 중심으로 사이버보안의 전반적인 개념과 기본 원리를 학습한다.

- Security Principles
- Cryptography
- Access Control
- Operating System Security
- Network Security
- Software Security

Offline Class

실제 취약점과 공격 사례를 살펴보고, 공격자의 관점에서 시스템을 분석한다.

- Vulnerability Analysis
- CVE
- Offensive Security
- IoT / Embedded Systems
- Security Research

2. Main Textbook

Main Textbook

Computer Security: Principles and Practice

William Stallings and Lawrie Brown

3rd Edition

이 책을 본 수업의 **기본 교재** 로 사용한다.

온라인 강의에서는 교재를 중심으로 사이버보안의 핵심 개념과 원리를 학습하며, 중간고사와 기말고사 역시 이러한 기본 내용을 중심으로 평가한다.

Course Principle

먼저 **Security Fundamentals**를 충분히 이해한 뒤, 오프라인 수업에서 실제 공격과 취약점 분석으로 확장한다.

3. Offline Class: First Stage

학기 초반에는 **실제 취약점 분석 사례**를 중심으로 공부한다.

학생들은 보안 기업의 기술 블로그, CVE 분석 자료, 실제 공격 사례 등을 읽고 다른 학생들에게 쉽게 설명한다.

주로 다음 내용을 살펴본다.

- 어떤 시스템을 분석했는가?
- 공격자는 어디에서 시작했는가?
- 어떤 취약점을 발견했는가?
- 취약점을 어떻게 발견했는가?
- 실제 공격은 어떻게 이루어지는가?
- 어떻게 방어할 수 있는가?

목표는 실제 보안 분석이 **어떤 방식으로 이루어지는지 이해하는 것**이다.

4. Offline Class: From Practice to Research

학기 중반부터는 실제 공격 사례에서 한 단계 더 나아가 **보안 연구 논문과 Advanced Topics**를 살펴본다.

Practical Security Problem

⇓

Why is this difficult?

⇓

How can we analyze it more effectively?

⇓

Security Research

예를 들어 다음과 같은 주제를 살펴볼 수 있다.

- Firmware Analysis
- Vulnerability Discovery
- Fuzzing
- Embedded / IoT Security
- Systems Security

5. Offline Class: Final Stage

학기 후반에는 가능하면 **직접 분석하고 구현하는 단계**까지 진행한다.

예를 들면,

- 기존 취약점이나 공격을 직접 재현해보기
- 보안 도구를 사용하여 시스템을 분석해보기
- 기존 공격을 다른 환경에 적용해보기
- 간단한 공격 또는 방어 아이디어를 구현해보기
- 흥미로운 결과가 있다면 연구 주제로 발전시키기

Important

모든 학생이 새로운 취약점이나 논문을 완성해야 하는 것은 아니다.

중요한 것은 **직접 분석하고 구현하면서 새로운 질문을 발견하는 것**이다.

6. From Practice to Research

오프라인 수업의 흐름은 단순한 공격 실습에서 끝나지 않는다.

Learn an Attack

⇓

Understand the Vulnerability

⇓

Reproduce or Analyze It

⇓

Ask New Questions

⇓

Research Idea

Research Direction

좋은 결과가 나온 경우에는 수업 프로젝트를 이후의 **학부 연구, 연구실 프로젝트, 논문**으로 발전시킬 수 있다.

7. Embedded and IoT Security

오프라인 수업에서는 실제 시스템의 보안을 이해하기 위해 **IoT와 Embedded System Security** 사례도 다룬다.

- Hardware Interfaces
- UART / JTAG / SWD
- Firmware Extraction
- Firmware Reverse Engineering
- Network and Protocol Analysis
- Vulnerability Discovery

이러한 기술 자체를 모두 전문적으로 다루는 것이 목적이라기보다,

Goal

실제 시스템에서 **Attack Surface를 찾고 취약점을 분석하는 기본적인 사고방식과 기술** 을 익히는 것이 목적이다.

8. Connection to Robot and Autonomous Systems

Embedded Security와 Offensive Security에서 배운 내용은 향후 로봇과 자율시스템 보안에도 연결될 수 있다.

Hardware / Firmware

⇓

Operating System / Software

⇓

Network / Protocol

⇓

Robot / UAV / Autonomous System

⇓

Cybersecurity

단순히 취약점을 찾는 것을 넘어, **공격이 실제 시스템에 어떤 영향을 주는지**까지 생각해보는 것을 목표로 한다.

9. Beyond the Classroom

이번 수업에서 배운 내용은 강의실 안에서 끝나는 것이 아니라 실제 보안 실무와도 연결할 예정이다.

Cybersecurity Fundamentals

⇓

Vulnerability / CVE Analysis

⇓

Security Papers

⇓

Hands-on Analysis

⇓

78ResearchLab Security Training

학기 이후에는 희망 학생을 중심으로 78ResearchLab과 연계한 **실전 보안 교육 및 실습**도 진행할 예정이다.

10. The Overall Learning Path

이번 학기의 전체적인 학습 흐름은 다음과 같다.

Textbook and Online Lectures

Security Fundamentals

⇓

Practical Security Cases

Blogs / CVEs / Vulnerability Analysis

⇓

Advanced Security Research

Papers / Advanced Techniques

⇓

Hands-on Project

Reproduction / Analysis / Implementation

⇓

Research or Industry Training

Let’s Get Started

Computer Security

Principles, Attacks, and Real-World Systems

Thank You

Questions?