# System Security

Dr. Yeonjoon Lee

# Instructor and AI

- **Instructor: Professor Yeonjoon Lee**
  - Office: 제 3 공학관, 504호
  - Email: yeonjoonlee@hanyang.ac.kr
  - Office hour: Right after class or by appointment
- Class meeting time and location:
  - 수업: Tuesday 15:00 PM – 17:00 PM (제 1공학관, 305 강의실)
  - 실습: Friday 09:00 AM – 11:00 AM (제 3공학관, 318 호 컴퓨터보안실습실)
- **TA:**
  - 이석원 (sevenshards00@gmail.com)
  - Office hour: Wednesday 15:00 PM – 17:00 PM or by appointment
- Slides: https://github.com/luc2yj/HY-CSE4044

# If you have any questions…

- Job searching in Korea / USA..
- Graduate School, Research opportunity..
- What do you expect from the class?
  - Credits only?
  - Know something about security
  - Some hands-on experiences
    - To which extent?
- More about me:
  - Website: yeonjoonlee.com
  - Research topics: IoT Security, System Security, Mobile Security, NLP & Machine Learning based Security, Cyber-crime, etc.

# Course Objectives

- Introduction to system security
  - Give you a general survey of security and privacy technologies
  - Help you understand the basic concepts, ideas
  - Prepare you for taking more advanced security courses

- Try to offer some “experience” of security technologies
  - Get some hands-on experience on threats and defense
  - Capture the trend of some security threats
  - Learn how to do security-related research

# Prerequisites

- You will be able to fully enjoy the fun of the course if you have the following skills:
  - Programming
  - Operating system

# Textbook

- *Computer Security: Principles and Practice (3rd or 4th Edition)*, by William Stallings and Lawrie Brown
  - There is online version for 3rd Edition
- *Computer & Internet Security: A Hands-on Approach,* by Wenliang Du
- Additional materials on slides
- Articles from the web (your reading project)

# Grading

- Class attendance (10%)
- Weekly lab assignments (25%)
- Reading projects (25%)
  - Project proposal (20%)
  - Project report (80%)
  - Presentation (TBD)
- Final (40%)

# Policies for Class Attendance

- Points that are subtracted from the total points for the semester associated for non-attendance will commence ONLY after 2 unexplained absences.
- Besides these two classes, you can ask for medical leave if you can provide proper evidence (see the course website).
- Otherwise, you will lose 3 points whenever you miss one class.

# Policies for Class Participation

- You are expected to actively engage in class
- Lectures are intended to be interactive, involving discussion
- Ask questions, participate in discussion, don’t look at your laptop

# Reading projects

- Review and analyze existing security technologies
  - One or Two students (with different expectations)
  - Bonus could be given to the project involving implementation and evaluation

- Suggested topics will be discussed in future lectures, but you are encouraged to come up with your own topics

# Ethics and Cheating

- **Ethics**

  DO NOT TRY HACKING EXPERIMENTS ON PUBLIC NETWORKS!!!

- **Cheating Policy**

  학교 규정에 따라 처리

# Tentative Arrangement

- Introduction
- Set-UID Programs
- Environment Variables and Attacks
- Shellshock Attack
- Buffer Overflow Attack
- Return-to-libc Attack and ROP
- Format String Vulnerability
- Race Condition Vulnerability
- Dirty COW
- Reverse Shell
- Meltdown Attack
- Spectre Attack
- Other Interesting Topics of Security (TBD..)

# Tentative Arrangement (cont'd)

- Lab starts from Week 1 (Environment Setup).

- Reading Project
  - Proposal: 2020/4/7
  - Final report: Will finalize the date later (2020/6/12)
  - Final presentations: TBD (To be discussed..)

# Reading Project Topic Examples

- Android Security
  - Malware Detection
  - Vulnerabilities Detection
- IoT Security
  - Study on platforms (e.g., smartthings)
  - Smart Things
  - IIoT
- Cloud Security

# Reading Project Topic Examples

- Threats on Autonomous Vehicles
- Cybercrime (e.g., Dark web, Crowdturfing)
- Adversarial Machine Learning
- Privacy-Preserving Machine Learning
- Forensics approaches for IoT systems
- Smart Speakers

# If you want to build something..

- Let me know!

- NLP related things
- GUI automation
- Reverse Engineering
- Static or Dynamic analysis

# Questions?

# Proposal

- Proposal Deadline: 4/7 11:59pm
- Proposal Format
  - Single column
  - Single spacing
  - Font type: 바탕체
  - Font size: 10
  - Layout: 좌/우/위/아래 모두 20mm
  - Page limit: 2 pages
- Final Report Deadline: 6/12 11:59pm.
- Final Report template will be uploaded next week.