


# Course overview

**Hyoungshick Kim**

Department of Software

College of Software

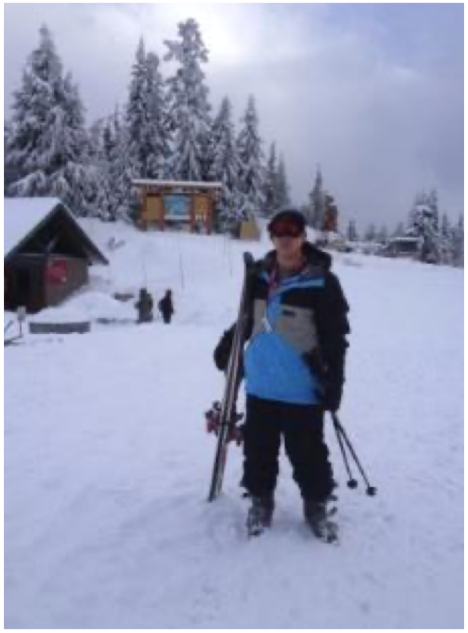
Sungkyunkwan University

# Instructor – Hyoungshick Kim

**Associate Professor** in Department of Software,
Sungkyunkwan University

- Education
  - ✓ Ph.D. in Computer Science, University of Cambridge
- Experiences
  - ✓ Professor, Sungkyunkwan University, Korea (2013 – present)
  - ✓ Distinguished Visiting Scientist, CSIRO Data61, Australia, (2019-2020)
  - ✓ Postdoctoral Fellow, University of British Columbia, Canada (2012-2013)
  - ✓ Senior Engineer, Samsung Electronics (2004-2008)
- Research interests:
  - ✓ Security engineering, Usable security, Software security
- Office hours: Wednesdays 13-14 (*hyoungshick* via Skype)
- Email: hyoung@skku.edu

  Please include **[Security]** in the subject of your e-mail
- Homepage: http://seclab.skku.edu/



- **Lab members:**
- **Academic staff: 2**
- **PhD students: 7**
- **MS students: 7**

# TA – Teaching Assistants

**Jusop Choi**

**Office: 26315**

**Eunsoo Kim**

**Office: 26315**

# Course orientation

1. Intended audience
2. Aims
3. Textbook
4. Class schedule
5. Good security venue

# Intended audience

- Undergraduate students who
  - want to know how a secure system is developed
  - want to get background in information security
  - might be interested in studying information security

# Aims

- To give you a through understanding of information security technologies
  - Security policy (what should be protected)
  - Engineering (how we can obtain assurance that the protection provided is adequate)
  - Protection mechanisms (cryptography, software security, …)
  - Attacks (malicious code, protocol failure …)
- To help you doing a research about information security

# Textbook

- Computer Security and the Internet: Tools and Jewels by Paul C. Van Oorschot: https://people.scs.carleton.ca/~paulv/toolsjewels.html
- Security Engineering (3rd ed.) by Ross Anderson: http://www.cl.cam.ac.uk/~rja14/book.html
- Handbook of Applied Cryptography by Alfred J. Menezes, Paul C. Van Oorschot, Scott A. Vanstone: http://www.cacr.math.uwaterloo.ca/hac/
- Lecture Notes on Cryptography by Shafi Goldwasser and Mihir Bellare https://cseweb.ucsd.edu/~mihir/papers/gb.pdf
- Papers

# Class schedule 1st

| Week | Topic |
|---|---|
| 1 | Course overview & Introduction to computer security |
| 2 | Cryptography I |
| 3 | Cryptography II (HW #1: Breaking the Vigenere cipher) |
| 4 | Cryptography III |
| 5 | Cryptography IV |
| 6 | No lecture (Chuseok Holiday) |
| 7 | Security protocols I |
| 8 | Security protocols II (HW #2: Secure file delivery) |

# Class schedule 2nd

| Week | Topic |
|---|---|
| **9** | Mid term |
| **10** | Software security I (HW #3: Threat modeling) |
| **11** | Software security II |
| **12** | Software security III (HW #4: Buffer overflow exploit) |
| **13** | Web security |
| **14** | Blockchain (HW #5: Paper review report) |
| **15** | Final term |

# Evaluation

- Research paper review (5%)
- Programming assignments (20%)
- Mid term (30%)
- Final term (30%)
- Attendance (5%)
- Online Discussion (10%)

# Evaluation - Assignments

- 1 paper reading report (for top security research papers) in English (5%)
  - ✓ Best reports will be selected for presentation (with extra credit)
- 4 programming assignments (20%)

# Assignments - Reading report

- Your reading report (at least 2 pages) should be organized as follows:
  - Title
  - Your name, student ID
  - Summary: summary should include
    - Motivation of the paper
    - Which problem the paper is trying to solve
    - Key ideas to solve the problem
    - How authors evaluate their solution
  - Strength of the paper
  - Weakness of the paper
  - Future work: not mentioned by the author

# How to choose your paper

- You can choose a paper from the top-tier conferences (2017~2020)
  - General: IEEE S&P (Oakland), USENIX Security, ACM CCS, NDSS
  - (2nd General: ESORICS, Euro S&P, ACSAC, AsiaCCS)
  - Hardware: CHES
  - Usable Security: CHI, SOUPS
  - Security Economics: WEIS
  - Privacy: PETS
  - Financial Security: FC
  - Malware/Intrusion Detection: RAID, DIMVA
  - Cryptography: Crypto, Eurocrypt, Asiacrypt
  - Etc. (e.g., USENIX WOOT: offensive research)

**You are encouraged to discuss with me for choosing your paper.**

# Prerequisite

- Some familiarity with C programming language

# Plagiarism

- Discussion of course material and collaboration with other students is encouraged but each student must write/type and submit his/her own solution.
- Your codes (or documents) should never contain sections which are identical to the submission of another student, past or present.
  - Submissions will be analyzed using a static analysis tool when applicable.
- Violation of these policies can result in automatic failure of the course.

# Example of Plagiarism

[Data Structure]과제2 점수 Inbox x

[redacted]

May 16

to hyoung

Korean › Filipino Translate message Turn off for: Korean

안녕하세요 교수님 저는 자료구조개론 수업을 듣는 [redacted]이라고 합니다. 제 과제 점수에 Plagiarism이라 채점이 되어 있습니다. 제가 2016311427학번의 사람과 비슷하다는 걸로 인식이 되어 있는것 같습니다. 하지만 제가 이 분을 알지도 못하고 저는 제 아는 사람과 인터넷 검색을 통해서 코드를 작성했습니다. 그런데 저 학번의 분도 같은 지인 분께 물어보거나 저와 비슷한 도움 사이트를 이용하는 것 같아 이런 일이 발생한 것 같습니다. 하지만 저 분의 코드를 절대로 베낀 것을 아닙니다. 그래서 표절에 대해서 재판단해주실 수 있는지 부탁드립니다.

**Hyoungshick Kim** <hyoung@skku.edu>

May 16

to [redacted]

안녕하세요, [redacted] 학생.

다른 학생의 논문을 베낀 것뿐만 아니라 인터넷에서 다른 사람 코드를 가져오는 것도 표절입니다. 표절의 정의를 잘못 알고 있는 것 같습니다.
이건 학생으로서 절대로 하지 말아야 하는 행동이며, 제가 수업 시작할 때 이미 이를 공지한 바 있습니다.

인터넷에서 가져온 부분에 대해서 citation을 했었나요?
도움 사이트라는 것이 무엇인지 모르겠지만, 표절이라는 판정은 틀리지 않은 것 같습니다.

김형식 드림

**Please do not copy a code from the internet.**

# Late Submission Policy

- Assignments submitted after the due date/time are considered late.
- You can hand in projects late. But there's a cost associated. Each 24 hours (or part thereof) late will cost you 20%.
  - Thus, if you hand something in that would have been worth 7 on time, but it's 36 hours late, that means that you only get 7*0.8*0.8=4.48.

# Questions?


Sungkyunkwan
Campus
Social
Graduate
Professors
English
Confucian
campus
Zone
Sciences
University
Global
Education
Seoul
Natural
Suwon
Korean
School
university
established
edit
also
Humanities
Science
schools
Administration
ASLE-Korea
Academic
Advanced
constructed
Building
Engineering
located
Joseon
Anniversary
Institute
now
two
Hall
Course
lecturers