Introduction to Information Security

1. Introduction

Kihong Heo

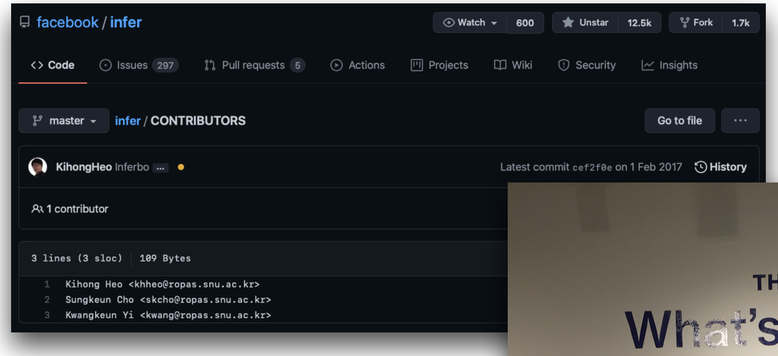
KAIST

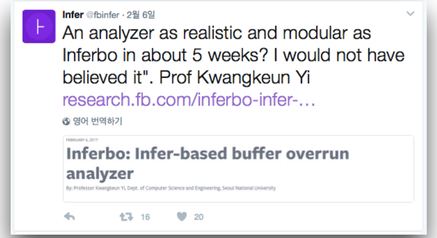
About Me

- Instructor: Kihong Heo (허기홍, kihong.heo@prosys.kaist.ac.kr)
- KAIST CS / GSIS / Programming Systems Lab.
- Homepage: https://kihongheo.kaist.ac.kr / https://prosys.kaist.ac.kr
- Office: N5 2321
- Office Hours: after each class (by appointment)

My Research

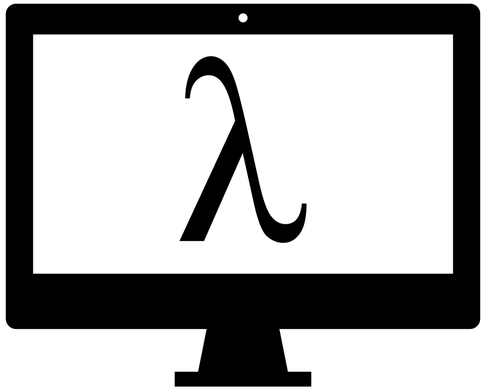
- Goal: solid PL theories $\Longleftrightarrow$ powerful programming systems
- Keywords: programming language, program analysis, SW engineering, SW security
- Good memories:





*https://research.fb.com/blog/2017/02/inferbo-infer-based-buffer-overrun-analyzer/

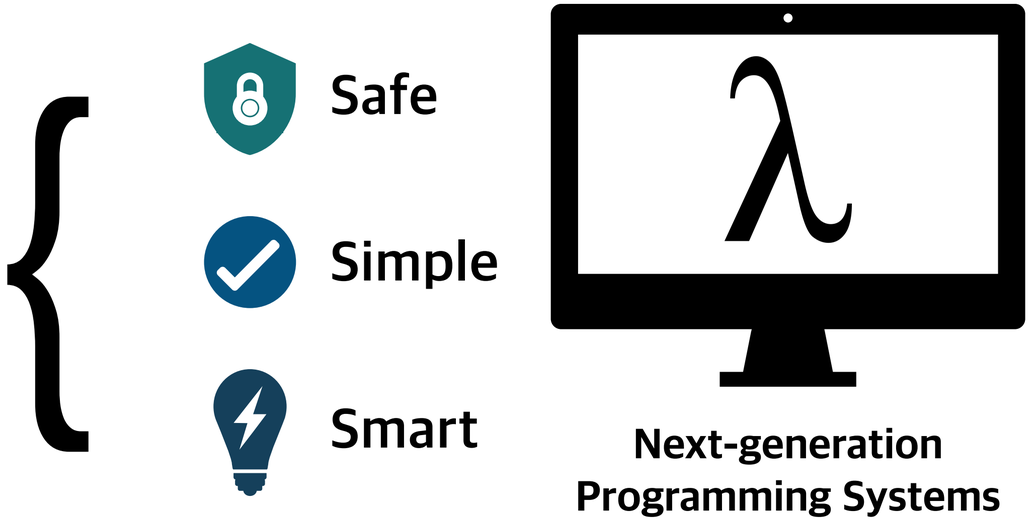
My Research



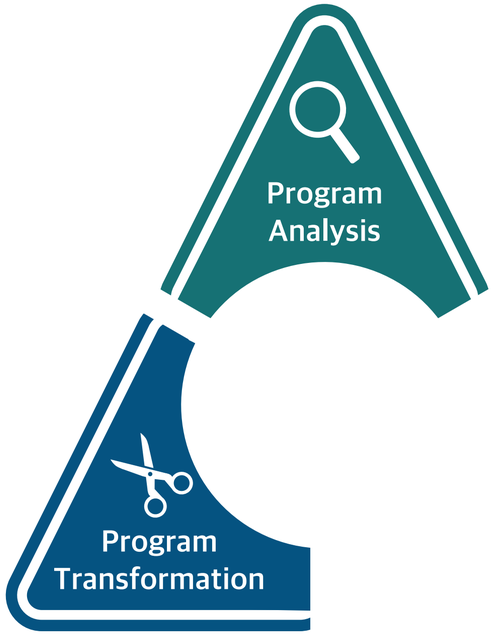
Next-generation
Programming Systems

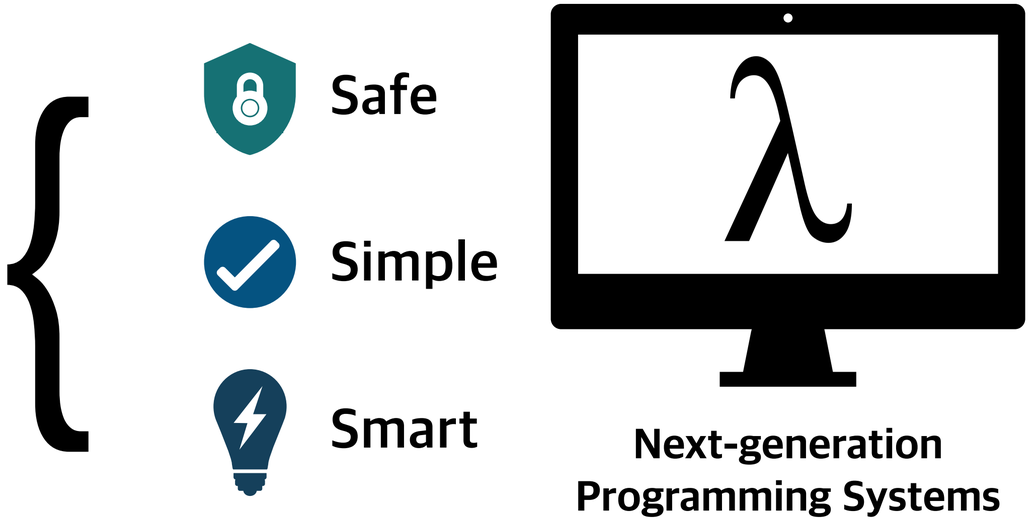
My Research

Program
Analysis

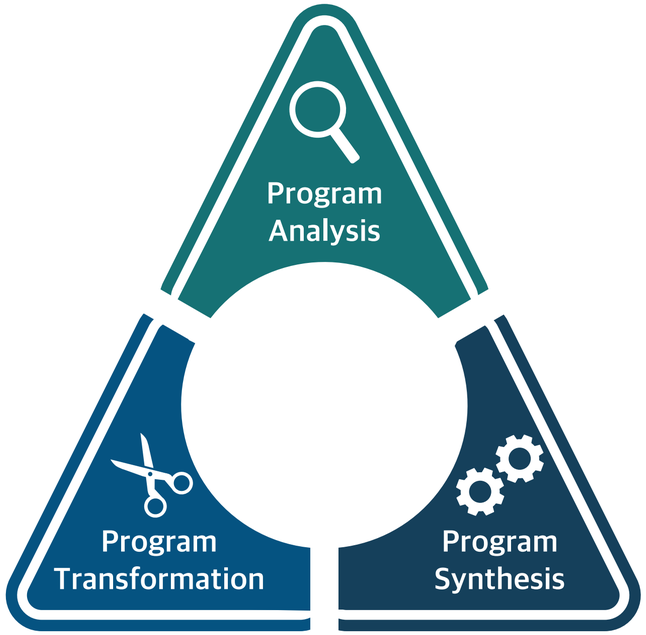

Safe
Simple
Smart
Next-generation
Programming Systems

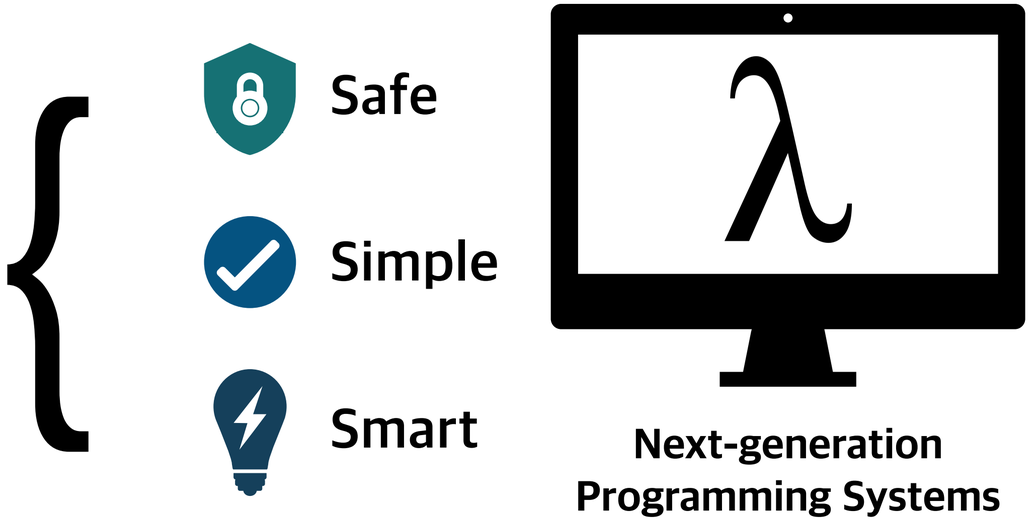
My Research


Program
Analysis
Program
Transformation

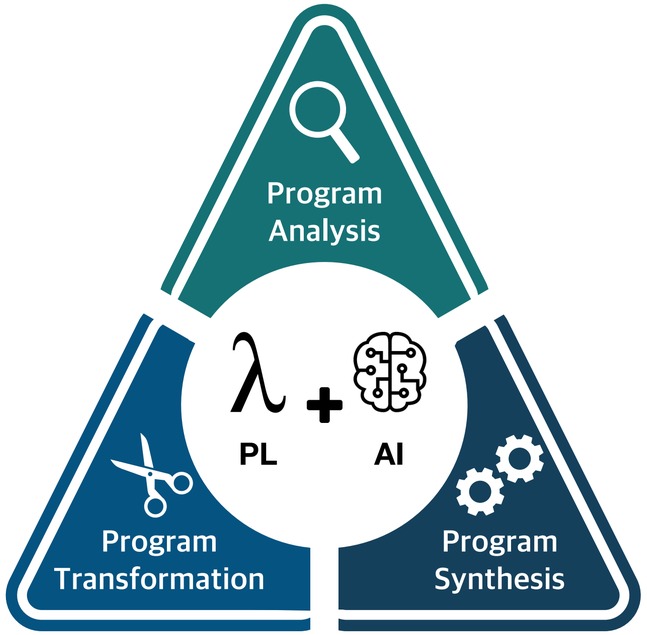

Safe
Simple
Smart
λ
Next-generation
Programming Systems

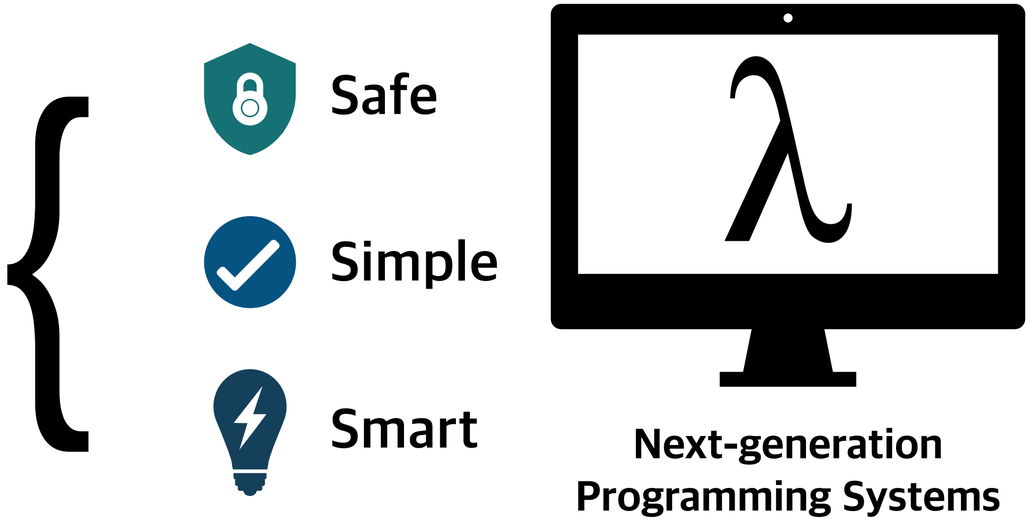
My Research


Program Analysis
Program Transformation
Program Synthesis


Safe
Simple
Smart
λ
Next-generation Programming Systems

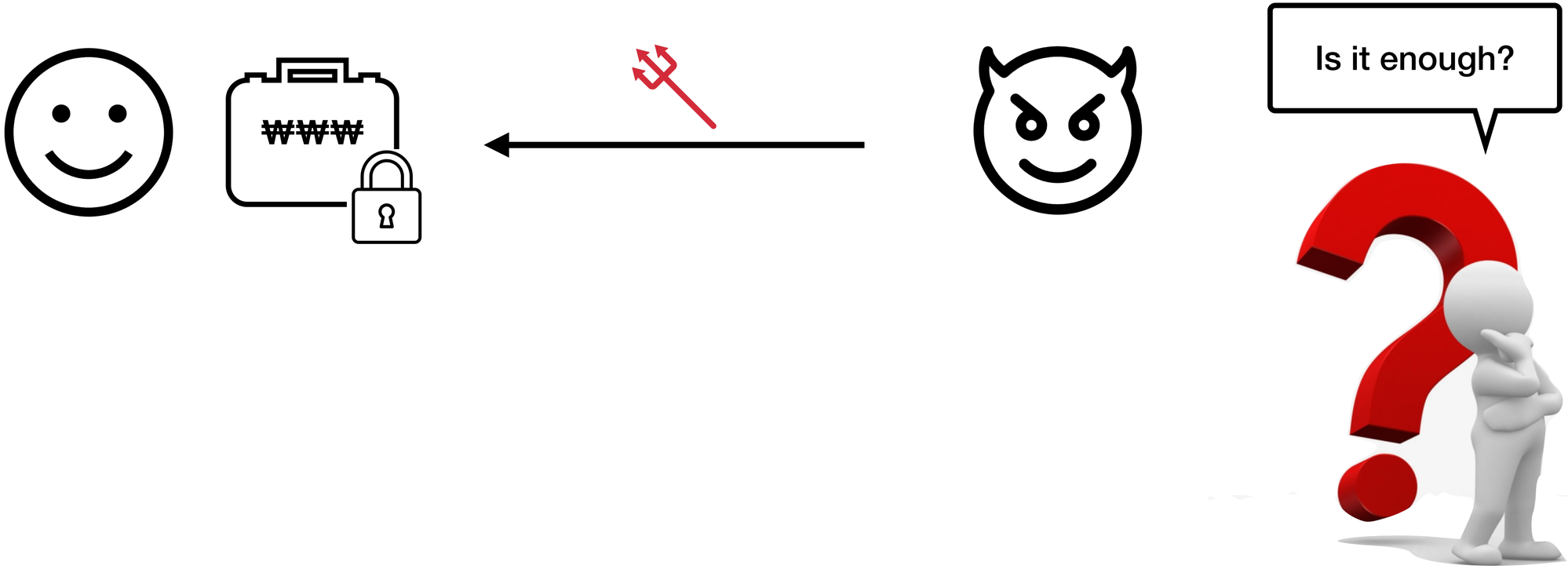
My Research


Program Analysis
λ
PL
AI
Program Transformation
Program Synthesis


Safe
Simple
Smart
λ
Next-generation Programming Systems

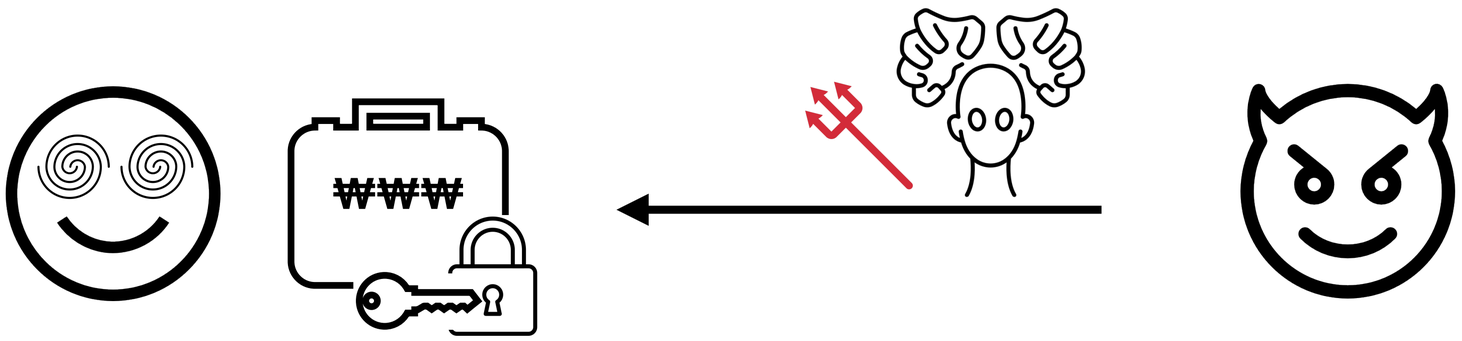
Security in a Nutshell (1)

- What to protect and how?



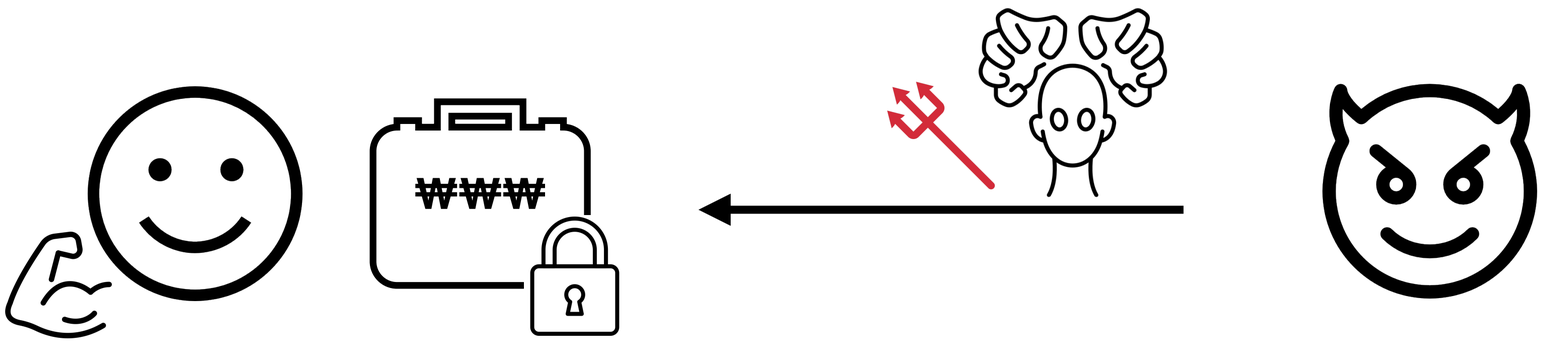
Security in a Nutshell (2)

- What to protect and how?



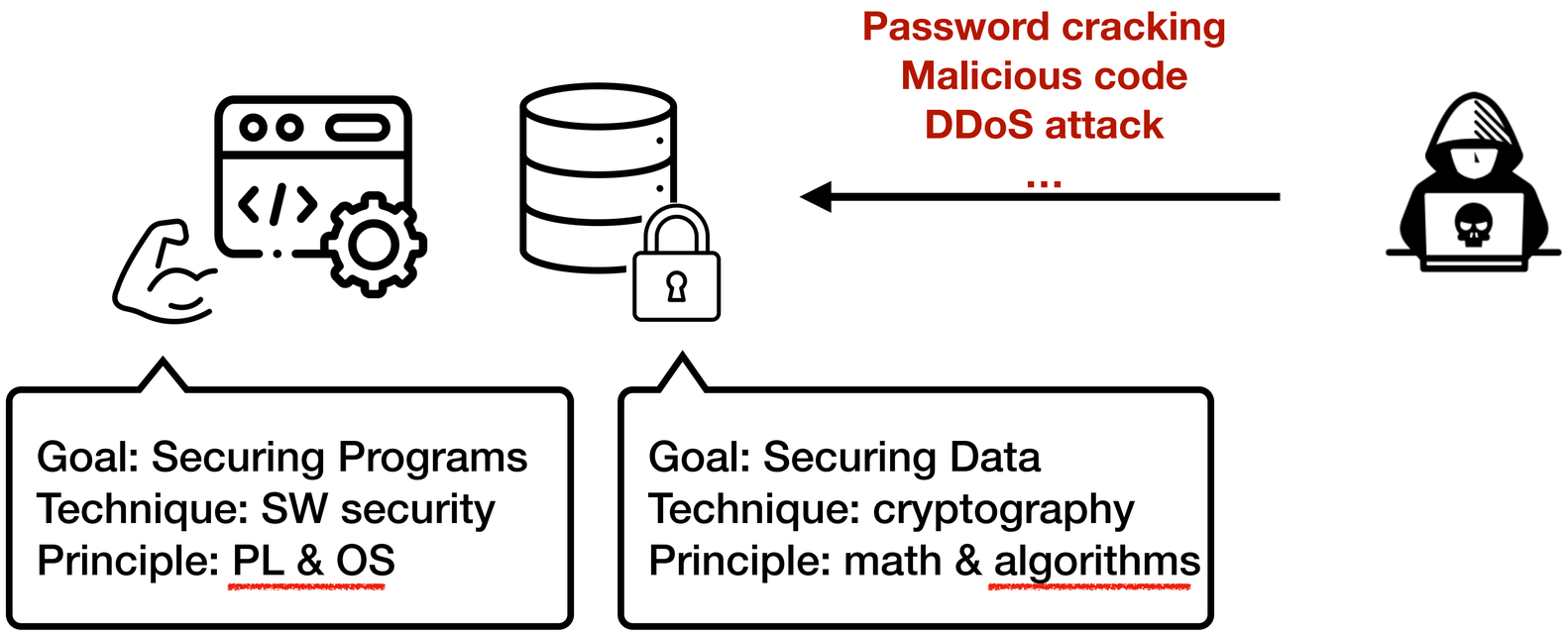
Security in a Nutshell (3)

- What to protect and how?



Security in a Nutshell (4)

- What to protect and how?



Course Information

- Course Website: https://github.com/prosyslab-classroom/cs348-information-security
- Q&A Board: https://github.com/prosyslab-classroom/cs348-information-security/discussions
- TAs (mailing list: cs348.ta@prosys.kaist.ac.kr)
  - Tae Eun Kim (김태은), Jaehoon Jagn (장재훈), Minsol Park (박민솔), Bongjun Jang (장봉준)
- Textbook:
  - Lecture slides will be provided
  - See more on the course website

Grading

- Homework: 40%
- Final exam: 40%
- Participation: 20%
  - Active participation, including various activities
- P/NR not allowed
- NOTE: nonnegotiable!
  - DO NOT send an email for a negotiation (cheating)

Important Notice (1): Academic Integrity

- DO NOT share the course contents (e.g., assignments or exams) with others
  - Esp., Github public repository, chegg.com, etc
- DO NOT discuss the details of solutions with others
- DO NOT plagiarize
  - We keep all the submissions from previous years!
  - We are programming language experts!
- Any integrity violation: at LEAST F
- If you have questions: QnA board > TAs > instructor

전산학부 명예규정 2022 봄학기 / School of Computing Honor Code 2022 Spring

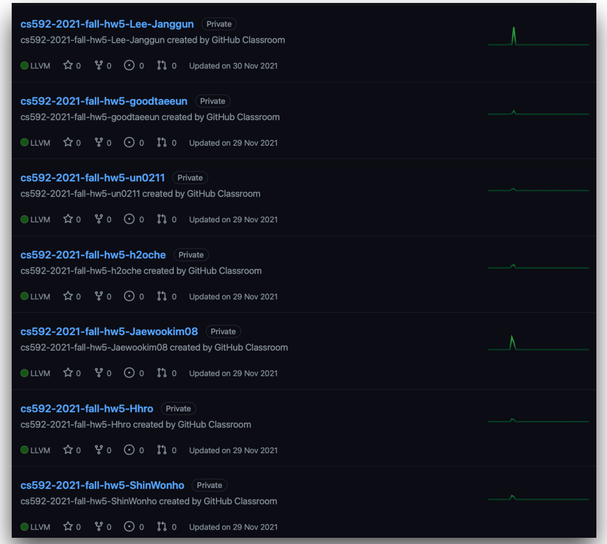
카이스트 전산학부가 운영하는 모든 수업에 참여하는 학생은 개인의 명예와 타인의 권리를 함께 존중하며 성실성과 정직성을 지키기 위하여 최선을 다합니다. 모든 시험 및 과제물 작성에 있어 허가되지 않은 어떤 형태의 도움도 받지 않습니다. 다음의 행위들은 학업의 성실성과 정직성을 위반하는 것으로 간주됩니다:

- 본인 이외의 사람/기관이 작성한 답안지, 숙제, 프로그램 소스 코드, 보고서 등을 참고 및 이용하는 행위
- 시험 및 과제물과 관련해 chegg.com과 같이 정답을 공유하는 온라인 서비스를 이용하는 행위
- GitHub 등의 코드 저장소에 본인의 과제 답안을 공개하거나, 타인이 공개된 답안을 참고 및 이용하는 행위
- 다른 학생이 본인이 작성한 답안지, 숙제, 프로그램 소스 코드, 보고서 등을 참고하도록 용인하는 행위
- 다른 학생이 작성한 결과물을 자신의 것인 양 제출하는 행위
- 다른 학생을 대신해 시험을 치루는 행위
- 개인이 수행하도록 되어있는 take-home 시험이나 과제물 작성에 있어 허락 없이 공동 작업을 하거나 부적절한 도움을 받는 행위
- 표절: 깊이와 무관하게 적절한 인용이나 언급 없이 타인의 창작물(참고서적, 문헌, 온라인상의 자료)을 무단으로 사용하는 행위

규정 위반 여부의 판단과 처벌 수위는 교과목 담당 교수에 의해 결정됩니다. 모든 부정행위는 전산학부 학사주임 교수 및 학부장님께 보고되며, 적발시 전산학부 내부적으로 아래와 같은 제약을 받습니다.

- 향후 2학기 동안 모든 포상 및 장학금 수여/추천 대상에서 제외함
- (주전공이 전산학부가 아닌 경우) 향후 2학기 동안 전산학부로의 전과 금지

위반의 심각성에 따라 학교 전체의 상벌위원회에 회부될 수 있습니다. 카이스트 학사규정이 허용하는 징계의 범위는 아래 첨부된 학생 징계 양형 기준을 참고하세요 (학생 핸드북 한글판 67페이지 , 다운로드는 https://portal.kaist.ac.kr/ennotice/student_notice/11614934649338)



cs592-2021-fall-hw5-Lee-Janggun Private
cs592-2021-fall-hw5-Lee-Janggun created by GitHub Classroom
LLVM 0 0 0 0 Updated on 30 Nov 2021

cs592-2021-fall-hw5-goodtaeeun Private
cs592-2021-fall-hw5-goodtaeeun created by GitHub Classroom
LLVM 0 0 0 0 Updated on 29 Nov 2021

cs592-2021-fall-hw5-un0211 Private
cs592-2021-fall-hw5-un0211 created by GitHub Classroom
LLVM 0 0 0 0 Updated on 29 Nov 2021

cs592-2021-fall-hw5-h2oche Private
cs592-2021-fall-hw5-h2oche created by GitHub Classroom
LLVM 0 0 0 0 Updated on 29 Nov 2021

cs592-2021-fall-hw5-Jaewookim08 Private
cs592-2021-fall-hw5-Jaewookim08 created by GitHub Classroom
LLVM 0 0 0 0 Updated on 29 Nov 2021

cs592-2021-fall-hw5-Hhro Private
cs592-2021-fall-hw5-Hhro created by GitHub Classroom
LLVM 0 0 0 0 Updated on 29 Nov 2021

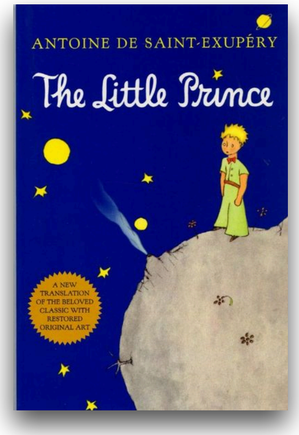
cs592-2021-fall-hw5-ShinWonho Private
cs592-2021-fall-hw5-ShinWonho created by GitHub Classroom
LLVM 0 0 0 0 Updated on 29 Nov 2021

Use of AI Tools

- “Am I allowed to use AI tools?”
- Stupid question! (like “Am I allowed to use Google?”)
- Important: use technology ethically
- Allowed: you take the lead, and AI assists
  - E.g., realize your idea using various AI tools for music, video, drawing, etc
- Not allowed: slave to AI
  - E.g., “Write a file read function in OCaml”
- What truly matters never changes!

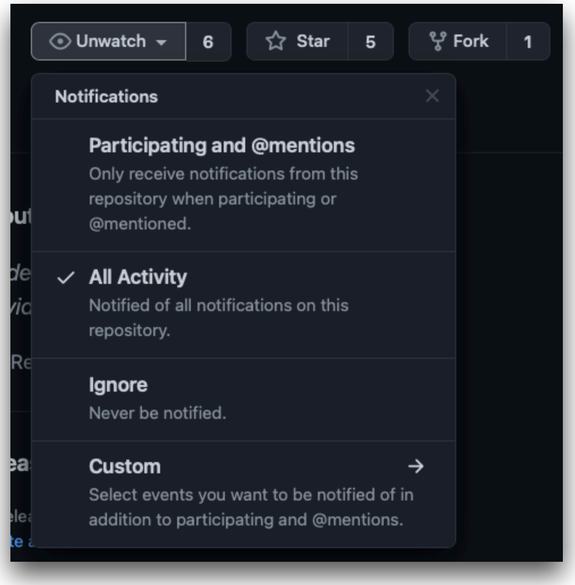
Important Notice (2): In-class

- Attendance: always (default), absence (if necessary)
  - No quantified attendance score
  - “What is essential is invisible to the eye” - The Little Prince
  - I expect you to be here, as you expect me to be here!
- Questions & discussion: highly encouraged
  - In Korean if you are a native speaker (I will translate)



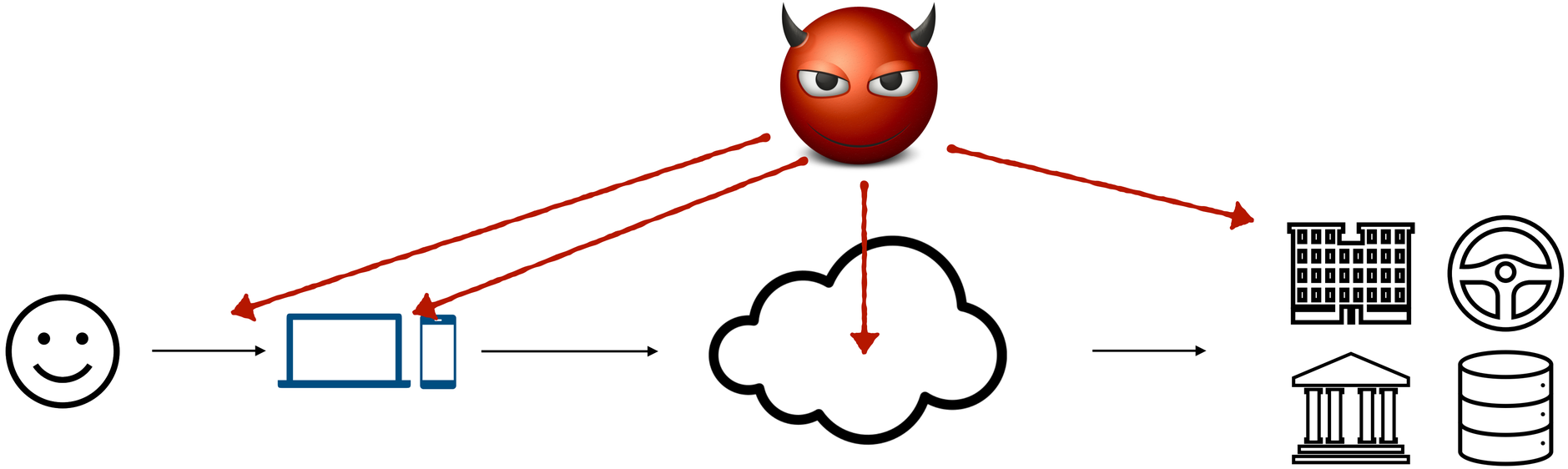
Important Notice (3): Out-of-class

- All Q&A and public notices: Github discussion board
  - “Watch” all notifications
- Private notices (grading, etc): KLMS
- Questions are always welcome except for
  - Too detailed ones (TAs are not debuggers!)
  - Directly related to the solutions
- Actively discuss with your classmates
- Write in Korean (for natives) and put the English version also (e.g., using AI translator)



Course Objectives: Principles

- What kinds of threats exist in computer systems?
- Why do the threats exist?
- How to design and implement secure computer systems?



Course Objectives: Practice & Challenge

- Homework: **design** & **implement** core concepts of information security
  - 8 (main) + 2 (dummy) assignments
- Programming assignments in OCaml
  - Cryptography algorithm, SW bug detector, etc
- Why OCaml? (https://ocaml.org)

The OCaml Language

- Simple, safe, and realistic programming language
  - Strong type system, higher-order functions, etc
- A lot of growing demands from academia and industry
- See the materials on the course webpage

Course Objectives: Active Learning

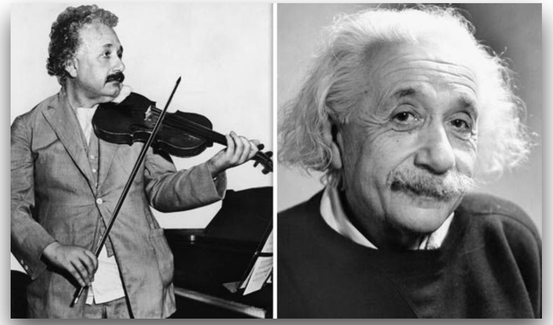
- The era of AI: NO free lunch and requires more creative thinking
  - Naively understanding & memorizing knowledge becomes obsolete
  - Creativity comes from “pain” (창의력은 노가다에서 나온다)
    - Training GPT-3: 355 yrs on a single GPU (2020)
- Three levels of knowledge
  - Understandable knowledge (이해 가능)
  - Explainable knowledge (설명 가능)
  - Artifiable knowledge (예술로 승화 가능)

by lecture, exam, programming assignment

by various activities

Activities

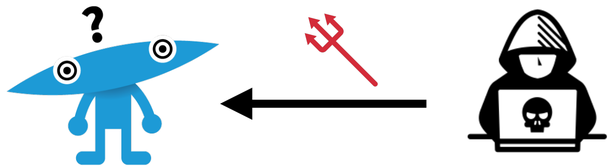
- Science = Art
- Encourage creative thinking
- Evaluate various aspects of students
- Various activities will be announced during the semester



"The greatest scientists are artists as well"
- A. Einstein

"A mathematician who is not also something of a poet will never be a complete mathematician."
- K. Weierstraß

Activity (1): Threat Hunt



- Save KAIST!
- If you find any security problems on campus, report them to me!
  - Physical (e.g., building) or cyber (e.g., portal, klms, email, etc)
- Depending on the severity, bonus points will be given
  - E.g., A+ > 1 letter grade up > 10% score up > … > 1 drink > …
- **DO NOT** try anything illegal
  - “REAL” education (참교육) will be given instead
  - If you cannot decide by yourself, discuss it with us first!
- Detailed instructions will be announced later

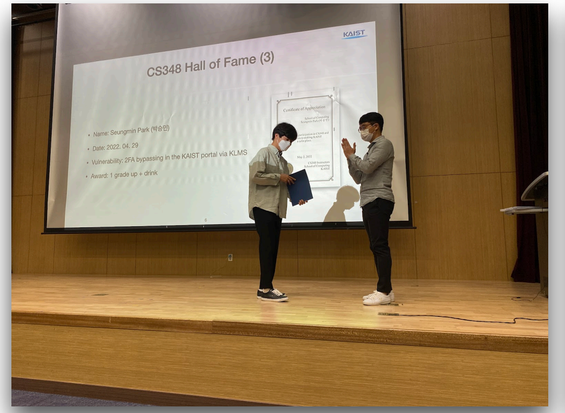
Hall of Fame

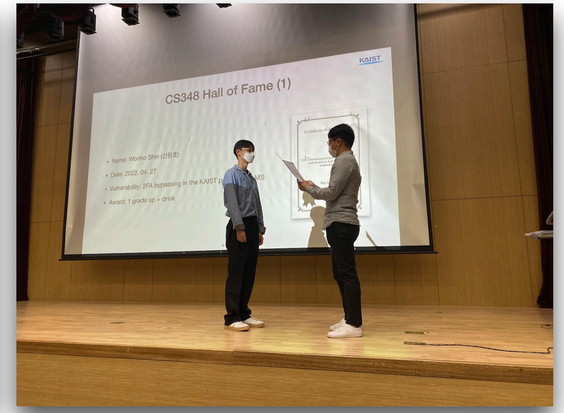
CS348 Hall of Fame

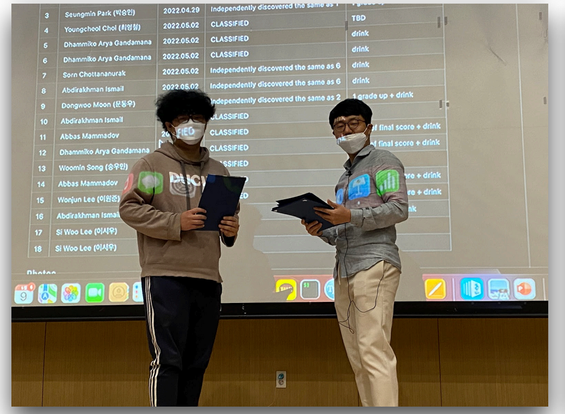
We appreciate the following students for their outstanding participation in CS348 and contribution to making KAIST a safer place.

The description of the vulnuerabilities will be disclosed until they are patched.

No	Name	Date	Vulnerability	Award
1	Wonho Shin (신원호)	2022.04.27	2FA bypassing	1 grade up + drink
2	Jun Cho (조준)	2022.04.27	Access control bypassing	1 grade up + drink
3	Seungmin Park (박승민)	2022.04.29	Independently discovered the same as 1	1 grade up + drink
4	Youngcheol Choi (최영철)	2022.05.02	Access control bypassing	2 grade up
5	Dhammiko Arya Gandamana	2022.05.02	Unauthorized request	drink
6	Dhammiko Arya Gandamana	2022.05.02	Access control bypassing	drink
7	Sorn Chottananurak	2022.05.02	Independently discovered the same as 6	drink
8	Abdirakhman Ismail	2022.05.02	Independently discovered the same as 6	drink
9	Dongwoo Moon (문동우)	2022.05.02	Independently discovered the same as 2	1 grade up + drink
10	Abdirakhman Ismail	2022.05.06	Breaking 2FA	1 grade up
11	Abbas Mammadov	2022.05.06	Denial-of-service	+5% of final score + drink
12	Dhammiko Arya Gandamana	2022.05.06	Access control bypassing	+1% of final score + drink
13	Woomin Song (송우민)	2022.05.06	Physical access control bypassing	drink
14	Abbas Mammadov	2022.05.06	Access control bypassing	+1% of final score + drink
15	Wonjun Lee (이원준)	2022.05.06	Access control bypassing	+1% of final score + drink
16	Abdirakhman Ismail	2022.05.06	XSS + CSRF	1 grade up + drink
17	Si Woo Lee (이시우)	2022.05.06	Unauthorized request	drink
18	Si Woo Lee (이시우)	2022.05.06	Not using HTTPS	drink
19	Murad Aghazada	2022.05.16	Access control bypassing	drink
20	Jiyeon Kim (김지연)	2022.05.16	2FA bypassing	+1% of final score + drink
21	Jiyeon Kim (김지연)	2022.05.16	Denial-of-service	drink
22	Aziz Huseynov	2022.05.16	Access control bypassing	drink
23	Moon Dongwoo (문동우)	2022.05.16	XSS	1 grade up + drink
24	Aziz Huseynov	2022.05.20	Authentication bypassing	3 grade up
25	Minhee Kim (김민희)	2022.05.27	2FA bypassing	drink
26	Seungjin Yu (유승진)	2022.05.30	Functional incorrectness	drink

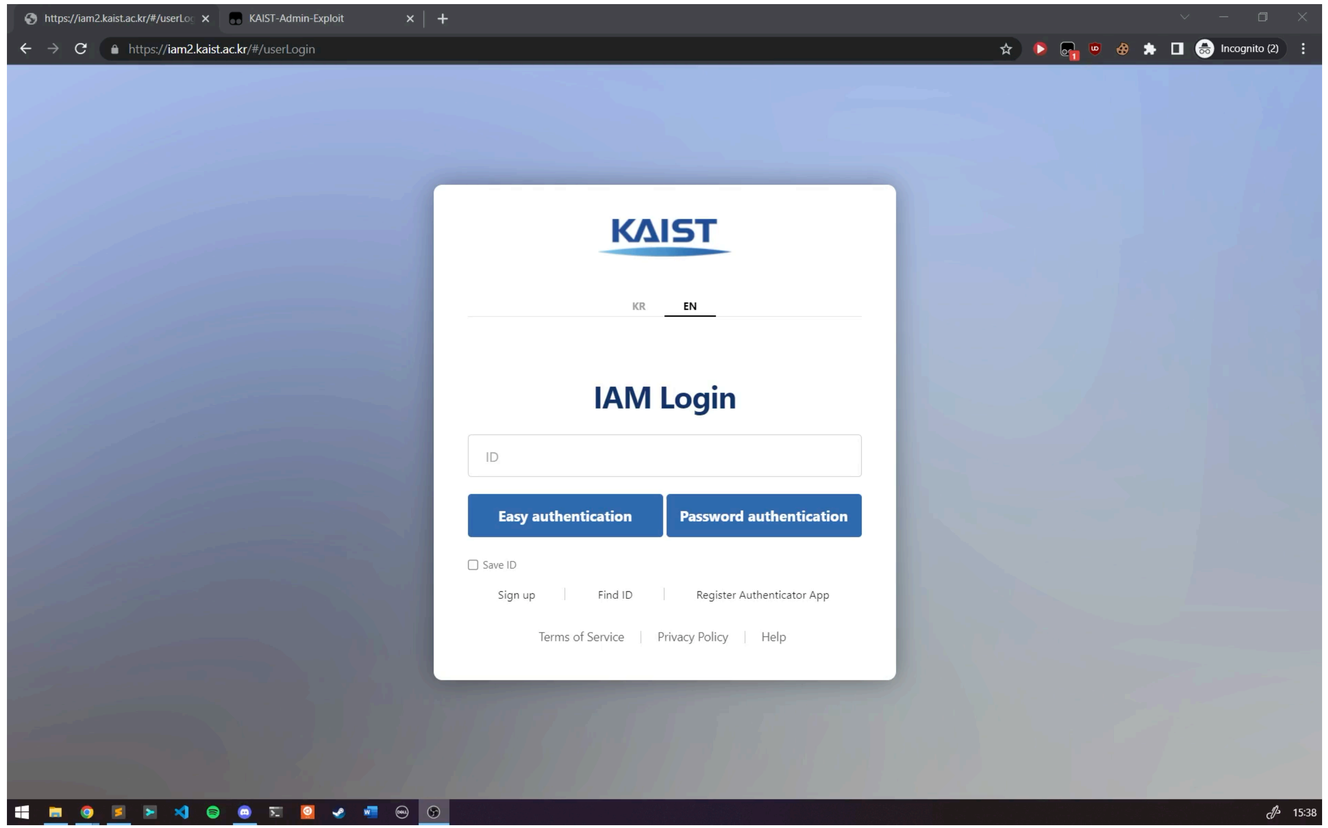






https://github.com/prosyslab-classroom/cs348-information-security/blob/main/hof.md

Top Secret



Certificate of Appreciation

School of Computing

For outstanding participation in CS348 and contribution to making KAIST a safer place.

May 2, 2022

CS348 Instructors
School of Computing
KAIST

By Aziz Huseynov, 2022 Spring

Hacking Ethics

- Hacking: seek to compromise computer systems or networks by exploiting vulnerabilities
  - E.g., stealing confidential data, DDoS
- White hackers: hired for penetration testing to find vulnerabilities
  - Give contributions to the society
  - DO NOT disclose the bug publicly before the fix is released
  - DO NOT exploit
- Be careful! KAIST is a national institute

Agreement

보 안 서 약 서

(학생용)

본인은 년 월 일 부터 년 월 일 까지 한국과학기술원 _____ _____ 학과의 _____ 과목에서 _____ 과제를 수행함에 있어, 다음과 같이 1)한국과학기술원의 규정과 통제절차 및 상급기관의 2)법적 보안사항을 준수할 것을 엄숙히 서약 합니다.

1. **나는 상기한 과제를 수행하며, 습득한 IT 정보 및 보안관련 사항 등의 기관정보와 관련된 어떠한 정보도 외부에 일체 발설하거나 노출 또는 반출하지 않을 것을 서약한다.**
   - 가. 네트워크/시스템/보안 등 IT인프라 관련구성 일체
   - 나. 시스템 접근권한 정보 일체
   - 다. 한국과학기술원 내에 있는 모든 개인정보 일체
   - 라. DB 정보 일체
   - 마. 정보시스템 취약점 등의 정보 일체
   - 바. 기타 한국과학기술원 정보보안 관련 대외비, 비밀 일체
2. **나는 위의 사항을 위반했거나 기밀을 누설한 경우, 아래의 관계 법규에 따라 엄중한 처벌을 받을 것을 서약한다.**
   - 가. 『형법』 및 『개인정보 보호법』
   - 나. 『정보통신망 이용촉진 및 정보보호 등에 관한 법률』
   - 다. 한국과학기술원 『학칙』 제59조
   - 라. 한국과학기술원 『학생 징계지침』 별표 제2호
3. **서약자 연명부**

연번	소속	연락처(Tel)	성명	서명	서명(강의교수)

제출일: 년 월 일

수 신 : 정보보안담당관(정보보안담당자)

1) 한국과학기술원『정보보안지침』(https://rule.kaist.ac.kr)
2) 과학기술정보통신부『정보보안 기본지침』및 국가정보원『국가정보보안기본지침』

Information Security Agreement

(for students)

From YYYY-MM-DD to YYYY-MM-DD, I solemnly pledge to comply with the regulations and control procedures of KAIST, the Ministry of Science and ICT, and the National Information Security Guidelines in carrying out the _____ course _____ project of _____ department.

1. I pledge not to disclose, expose or take out any information related to KAIST institutional information, such as acquired IT information and security related matters included but not limited to
   - A. All IT infrastructure-related configurations, including network/system/security
   - B. All system access information
   - C. All personal information in KAIST
   - D. All DB information
   - E. All information, such as information system weaknesses, etc
   - F. All other confidential information related to KAIST
2. I pledge to be severely punished in accordance with the relevant laws and regulations below in case of violations regarding the above.
   - A. Korean Criminal Law, Personal Information Protection Act
   - B. Korea Information and Communication Network Act
   - C. Article 59 of the KAIST School Regulations
   - D. KAIST Student Disciplinary Guidelines Appended Table 2
3. A List of vows

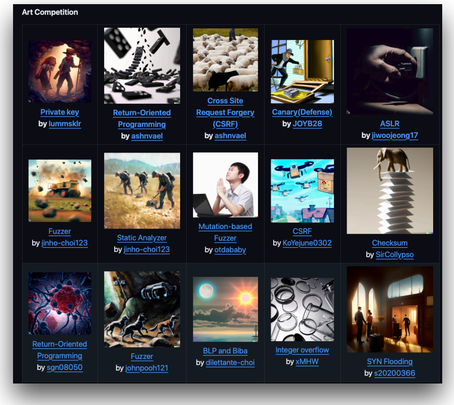
No.	Dept.	Contacts.	Name.	Signature.	Signature. (Prof.)

Date of Agreement : YYYY-MM-DD

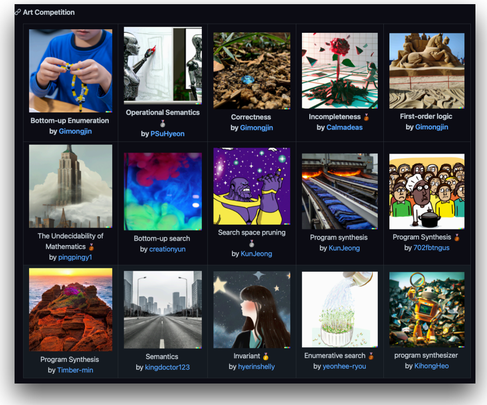
A Recipients : Information Security Officer

Activity (2): Art Competition (천하제일 예술대회)

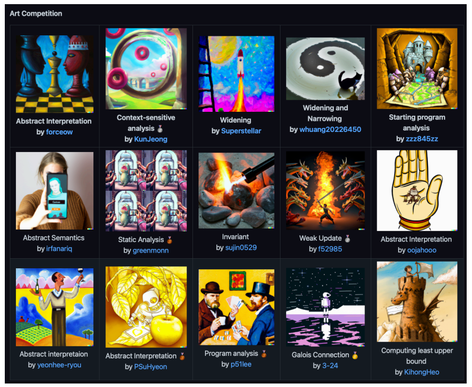
- What does X mean to you?
- Pick a concept X you have learned in this class
- Create artwork that succinctly represents the concept using any tools (e.g., AI tools)
- Requirement: 1 submission/month (due: last day of each month)
- Detailed instructions will be announced later



CS348: Intro to Information Security

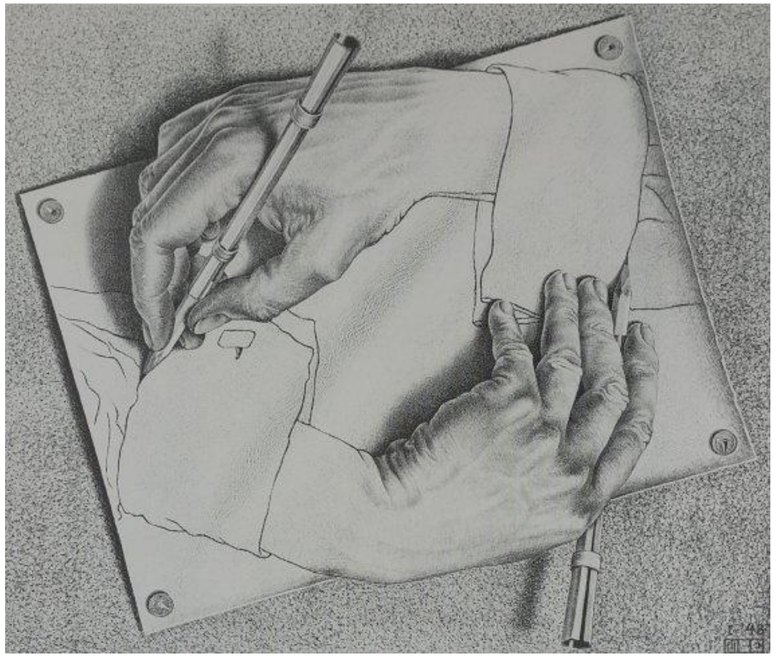


CS424: Program Reasoning

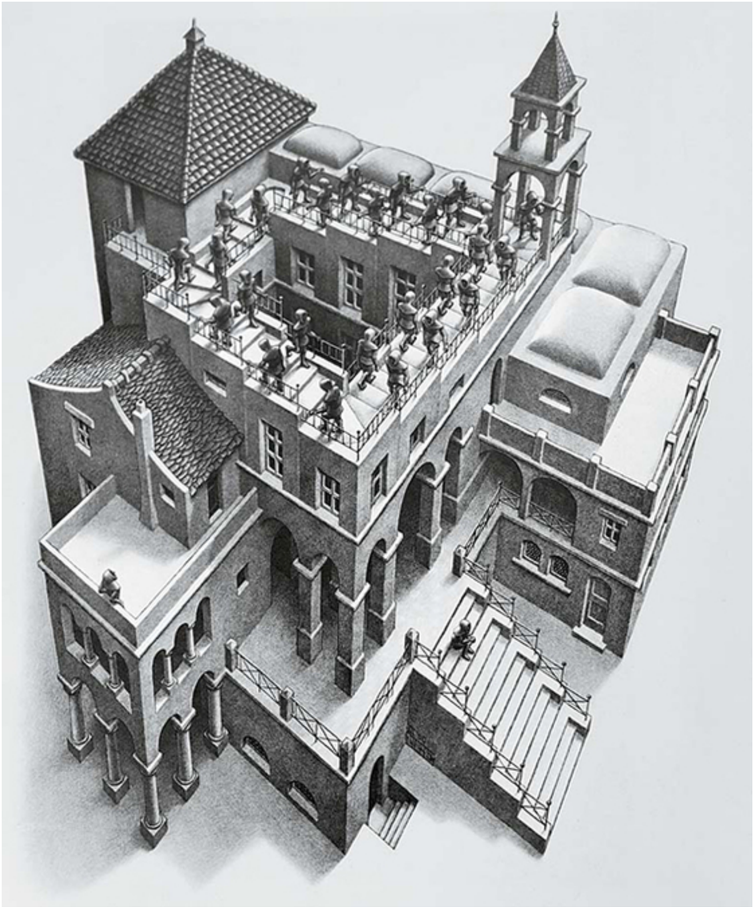


CS524: Program Analysis

Example: Recursion



M. Escher, *Drawing Hands*, 1948



M. Escher, *Ascending and Descending*, 1960

*See http://recursion.kaist.ac.kr/

Activity (3): Writing

- Science is communication
  - Writing: main communication tool
- Roles of KAIST folks
  - World-leading researcher (in English)
  - Inspiring communicator to the community (in Korean)
    - For newcomers, public, etc
  - High-quality training data for AI

Requirements

- Syntactic requirements
  - Typeset your document in Latex using a provided template (maximum 2 pages)
  - Korean (if you are a native Korean speaker), English (otherwise)
- Semantic requirements: Top-down (두괄식)
  - For each paragraph, write the topic sentence first followed by the details.
- See the README for the details
- The invitation URL will be posted on the course webpage

국문 글쓰기

- 제대로 된 우리말 번역과 전문 용어 원문 병기
  - 예: 프로그램 검증 (program verification), 덮이 (coverage), 요약 (abstract)
- 바보들의 전문 용어 번역 알고리즘:

  1. 영문 용어를 단어별로 쪼갠다
  2. 각 용어를 사전에서 찾아 제일 처음 나오는 우리말 단어로 바꾼다
  3. 바뀐 단어들을 순서대로 나열한다
- 일류 과학자의 전문 용어 번역 알고리즘: 개념을 제대로 이해하고 핵심을 설명하는 쉬운 우리말로
- 참고: PL-Wiki, easyword.kr 의 번역어

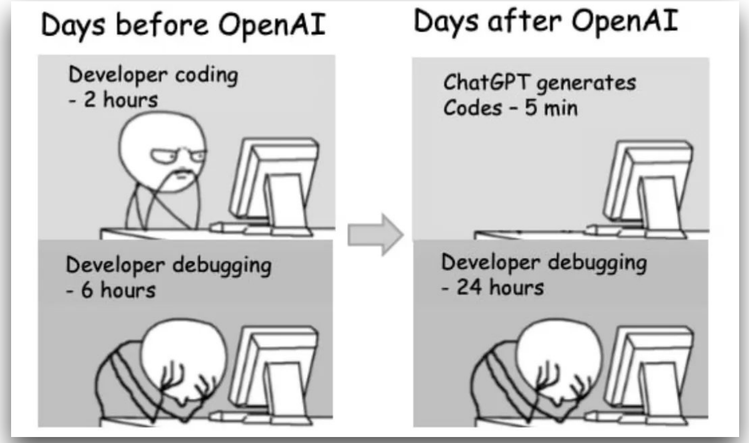
Essay Topics

- Look into real cybersecurity issues that have occurred over the past 2 years
- Think about the following:
  - What are the major security issues in today's cyber world?
  - What does the future look like?
  - How can we overcome the current challenges?
- Provide your opinion and write an essay
  - Rewards will be given depending on the quality
  - E.g., participation point, questions for the final exam, drink, fame, etc
- Other topics will be announced later

Activity (4): Responsibility of Intellectuals

- Learn and then share with others! (배워서 남주자, 홍익인간, 훈민정음)
- Contribute to knowledge-sharing platforms based on what you've learned in class
  - Korean jargon or article: easyword.kr, PL wiki
  - General: Wikipedia, Namu wiki
  - Etc
- NOTE: NO VANDALISM
- Report your contributions on the course web board

Activity (5): HackGPT



- Does ChatGPT become a friend or villain?
- Detect when ChatGPT becomes HackGPT!
- Igagine NEW security threats that can be caused by ChatGPT
  - Read “Large Language Models like ChatGPT say The Darnedest Things” [CACM’23]
  - DO NOT report known issues (e.g., generating buggy code): a lot of studies already done
  - Describe a concrete and detailed scenario
- Detailed instructions will be announced later

Homework

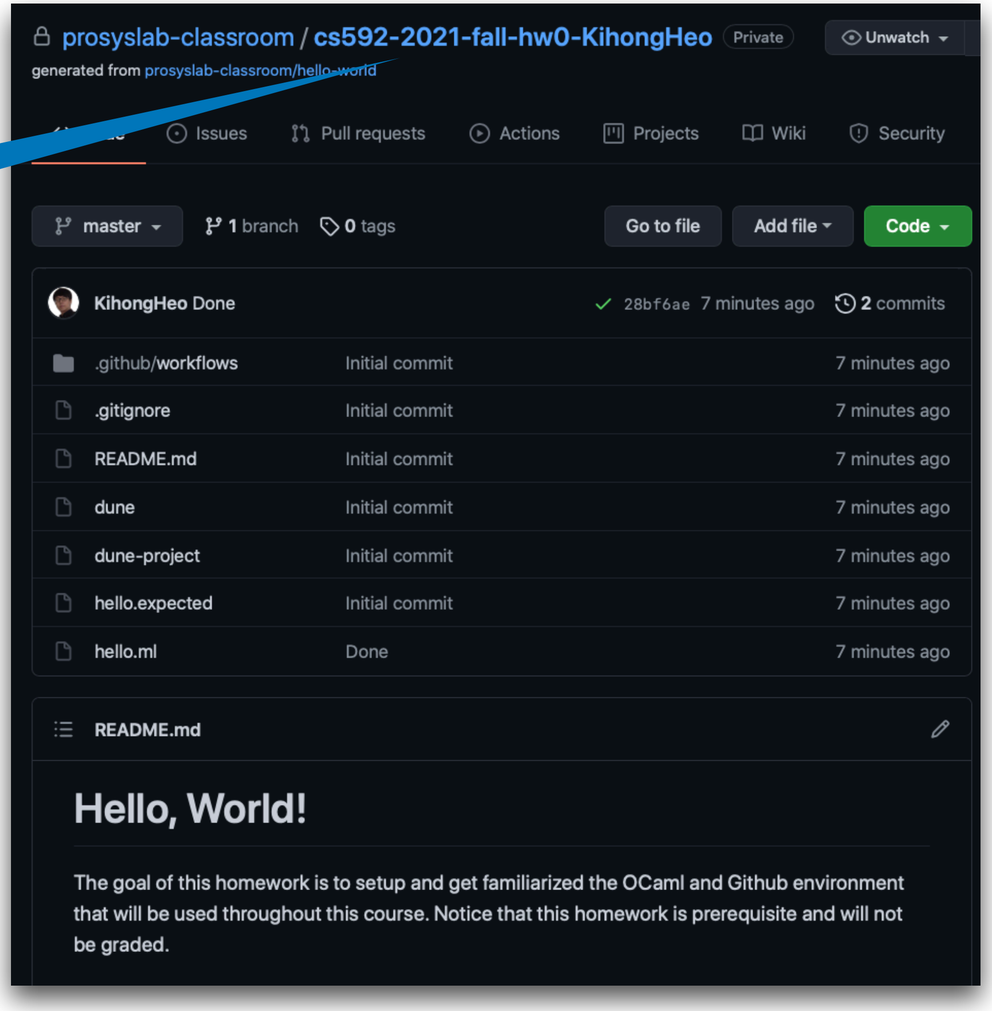
- All submissions will be managed using Github / Github Classroom
  1. For each HW, a unique invitation URL will be posted on the issue board
  2. Once you accept, a private repo for your assignment will be created
  3. You can push as many commits as you want before the deadline
  4. The final commit of your main branch will be graded
- Gradescope will be used for written assignments and exams
- 80% credit for 1-day late, 50% credit for 2-days late, NO credit otherwise

Homework 0.1: Hello, World!

- Goal: setting up and getting familiarized with OCaml and Git environments
  - Implement your “hello-world” program in OCaml
  - Test on your machine
  - Push to your Github repository
  - See the result in Github Action
- The invitation URL will be posted on the course webpage
- Will not be graded

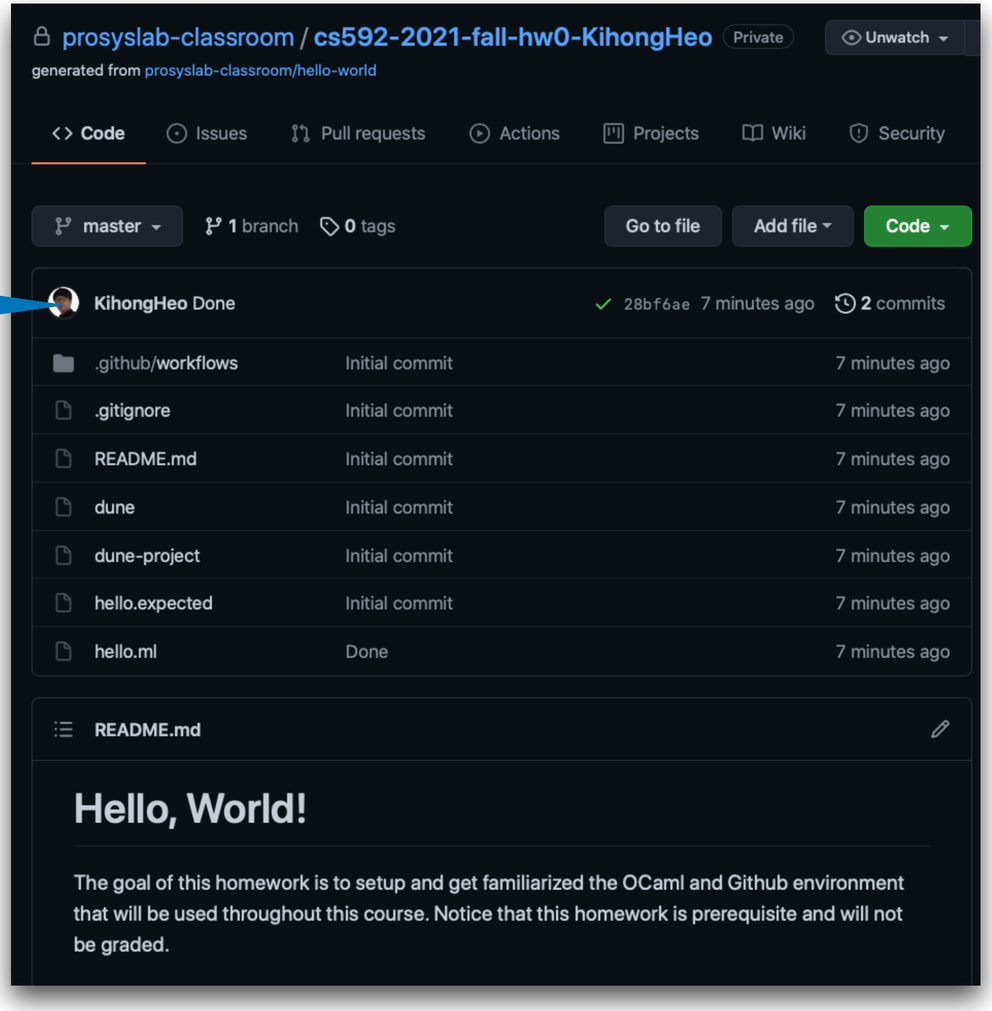
Homework 0.1: Hello, World!

1. Accept the invitation and have your repository



Homework 0.1: Hello, World!

2. Commit your code



Homework 0.2: OCaml Programming

- Goal: getting familiarized with basic OCaml programming
  - Solve a few programming problems in OCaml
  - Test on your machine
  - Push to your Github repository
  - See the result in Github Action
- The invitation URL will be posted on the course webpage
- Will not be graded but highly recommended if you are not familiar with OCaml

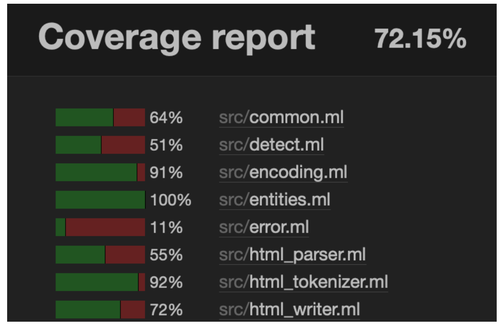
Requirement: Software Engineering Practices

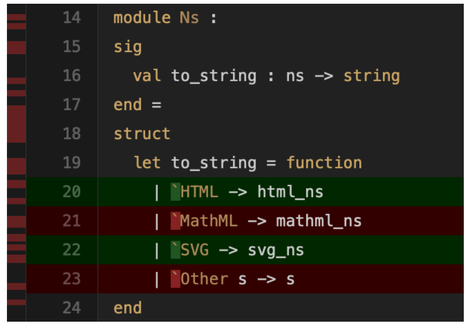
- All programming assignments submissions must follow basic SE practices
  - Remove all compile errors and warning
    - Remember: warning is error
  - Clean code via formatting
  - Acceptable code coverage
- Otherwise, NO points will be given
- Detailed instructions will be provided

```
File "src/semantics.ml", line 39, characters 6-11:
39 |   let count = 1 in
         ^^^^^
Warning 26 [unused-var]: unused variable count.
```

```
let rec
  fact n =
    match n with
  | 0 | 1 -> 1
  | _ ->  n *
      fact (n - 1)
```

```
let rec fact n =
  match n with
  | 0 | 1 -> 1
  | _ -> n * fact (n - 1)
```





Misc (1): Github, Gradescope

- Submit your Github account following the TA's announcement
  - Otherwise, no homework points will be given
- Join Gradescope (see the GitHub discussion)
  - For written assignments and the final exam
- Rules for programming assignments
  - Preserve the structures (directories, files, types, etc)
  - Don't install any Github App

Misc (2): Email Communication

- Primary communication tool for business
  - NOT for instant messages like Kakao Talk
  - But try to respond as soon as possible (within 24hrs)
- Include all relevant persons by using “CC” (참조) and “Reply All” (전체답장)
- International communication: you can send emails anytime
  - Professionals do not use notifications for emails
  - Do you send it to the US at 3 am?
- Other details: Google “email etiquette”

Misc (3): WoW

- Make an early decision then keep going
- Don’t drop the course; finish it to the end
- W = Wow sign = Warning of weakness
- Hope we go together until the end of the semester!