

Advanced Software Security

1. Introduction

Kihong Heo

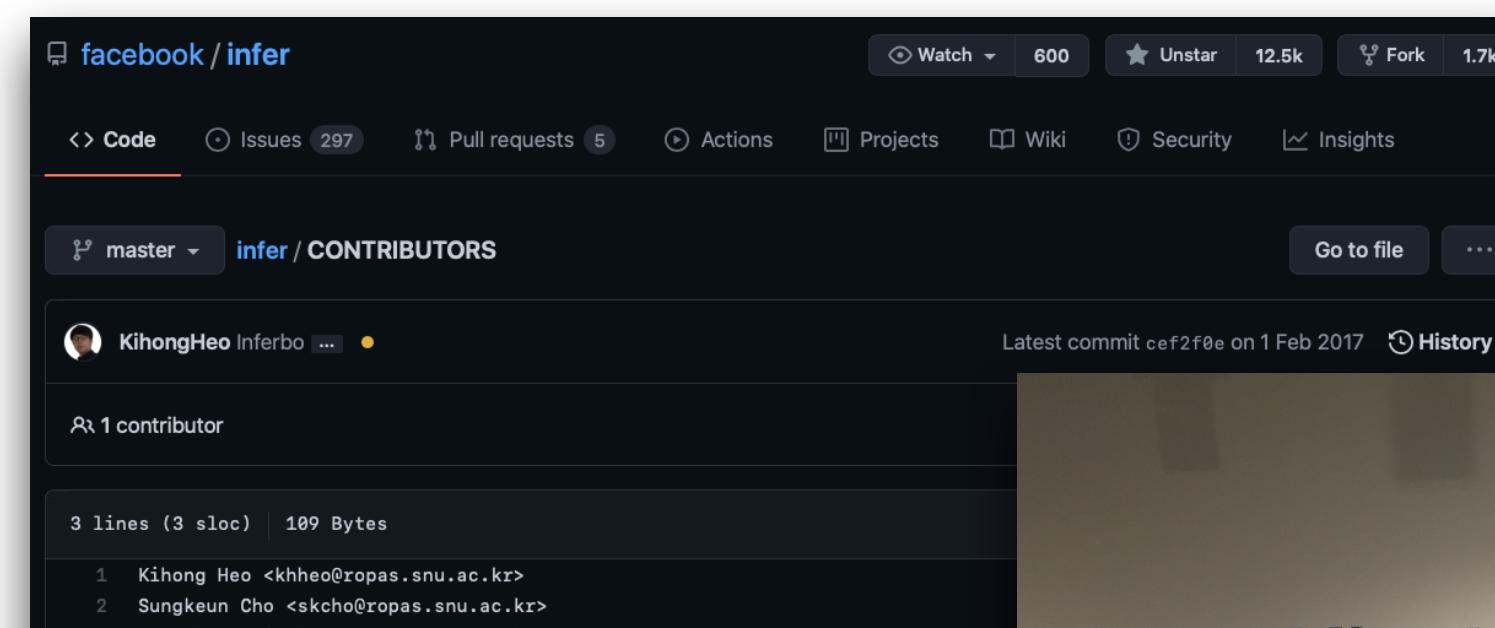


About Me

- Instructor: Kihong Heo (허기홍, kihong.heo@kaist.ac.kr)
- KAIST CS / GSIS / Programming Systems Lab.
- Homepage: <https://kihongheo.kaist.ac.kr> / <https://prosys.kaist.ac.kr>
- Office: N5 2321

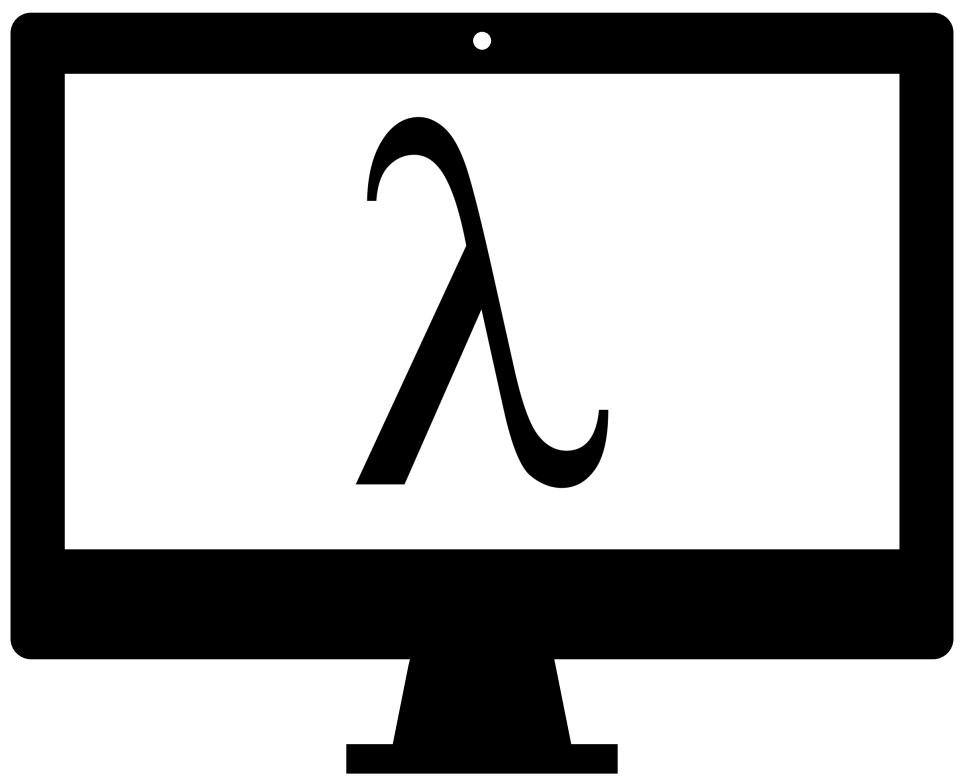
My Research

- Goal: solid PL theories \Leftrightarrow powerful programming systems
- Keywords: program analysis, programming language, SW engineering, SW security
- Good (also fierce) memories:



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

My Research

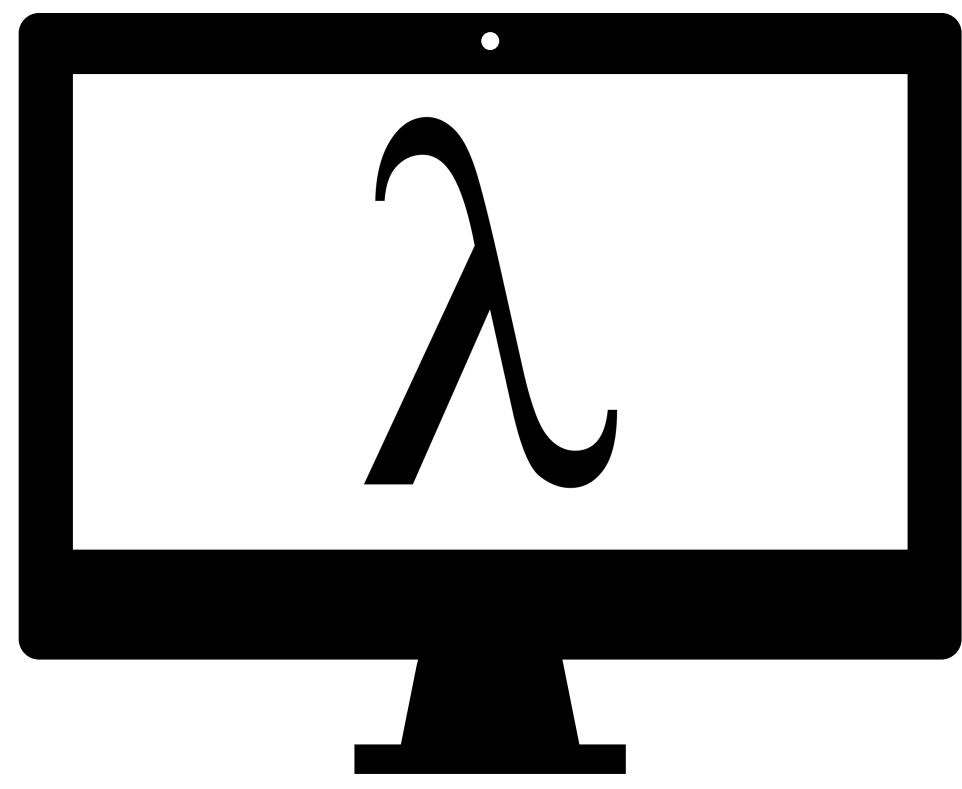


**Next-generation
Programming Systems**

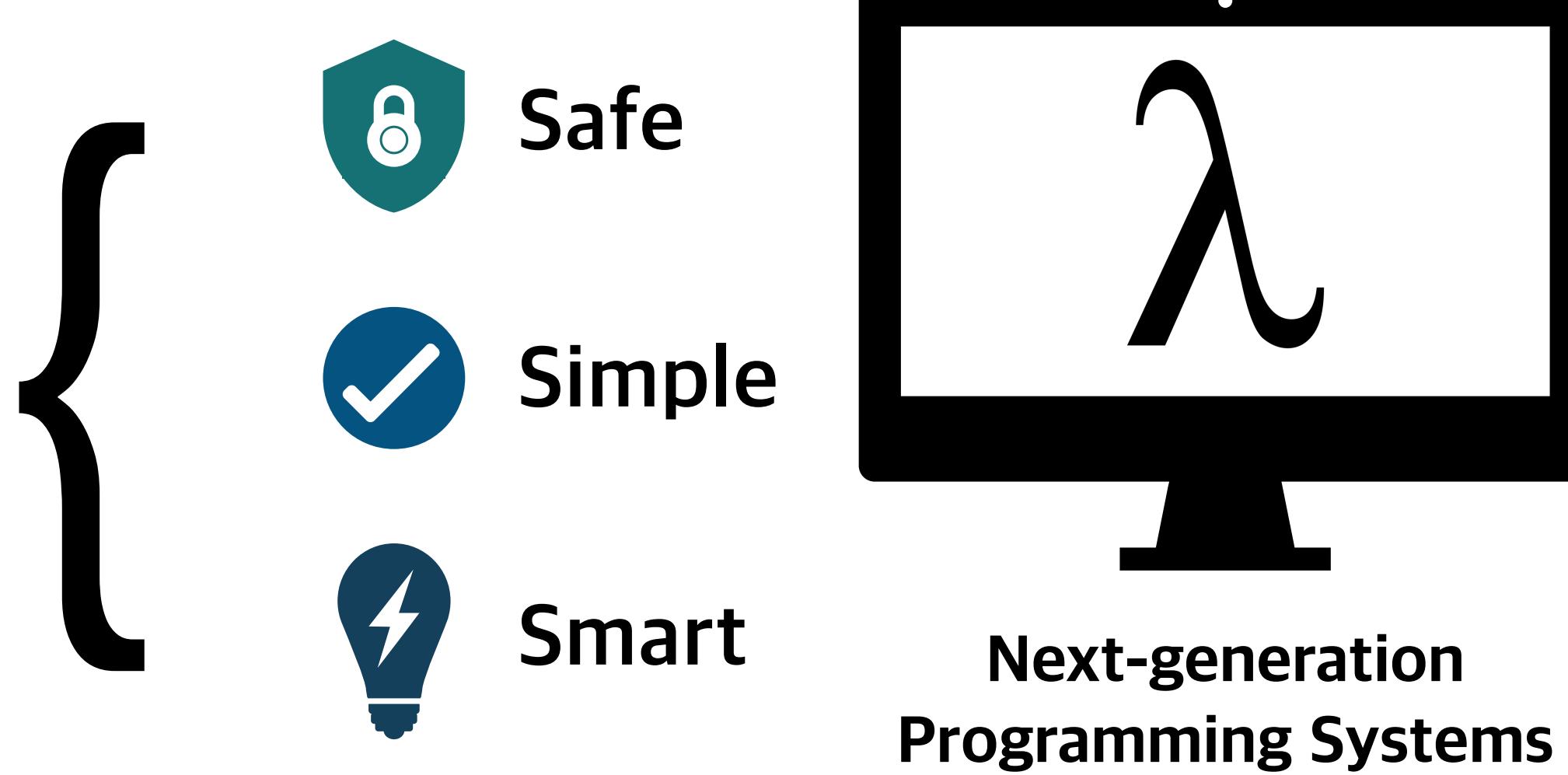
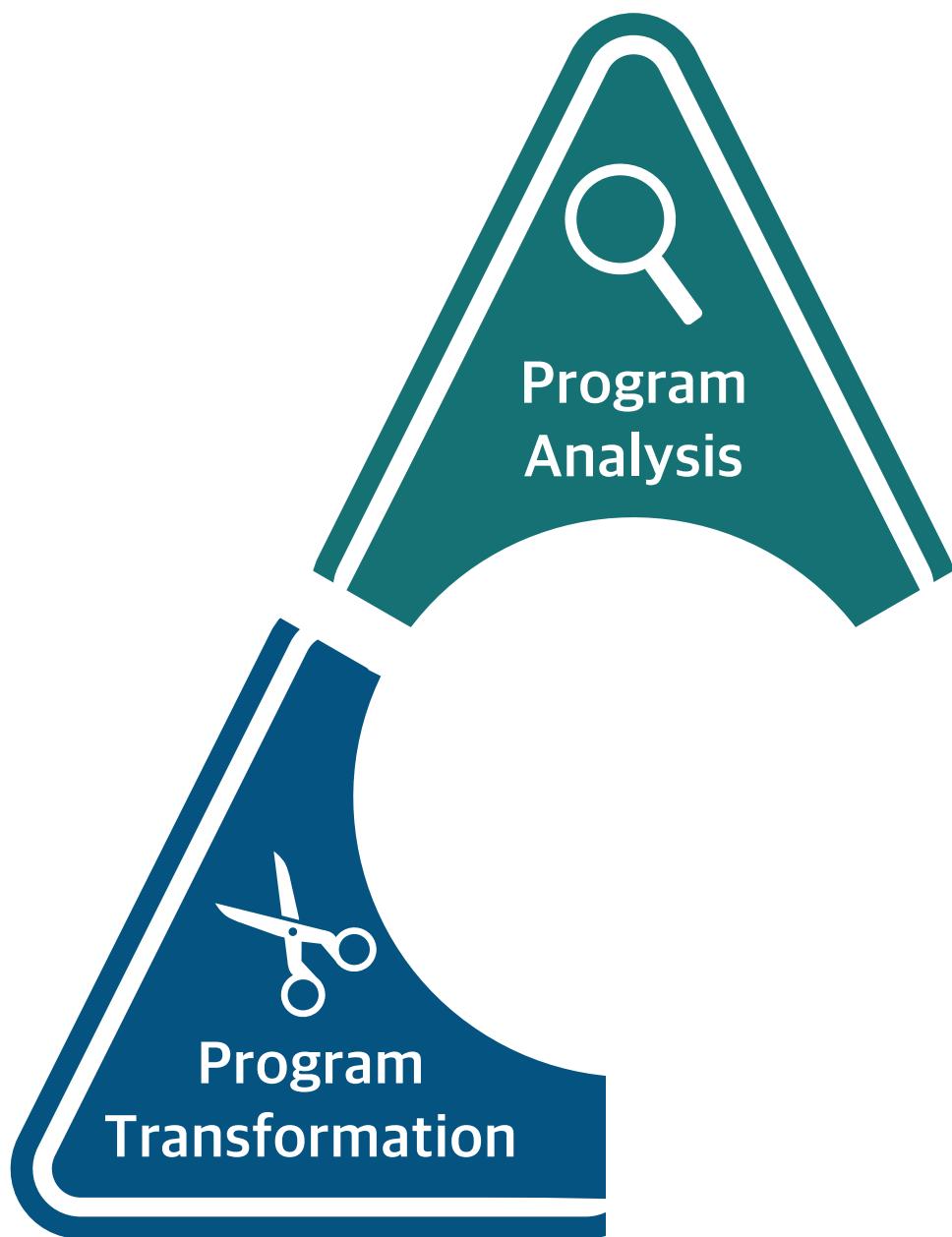
My Research



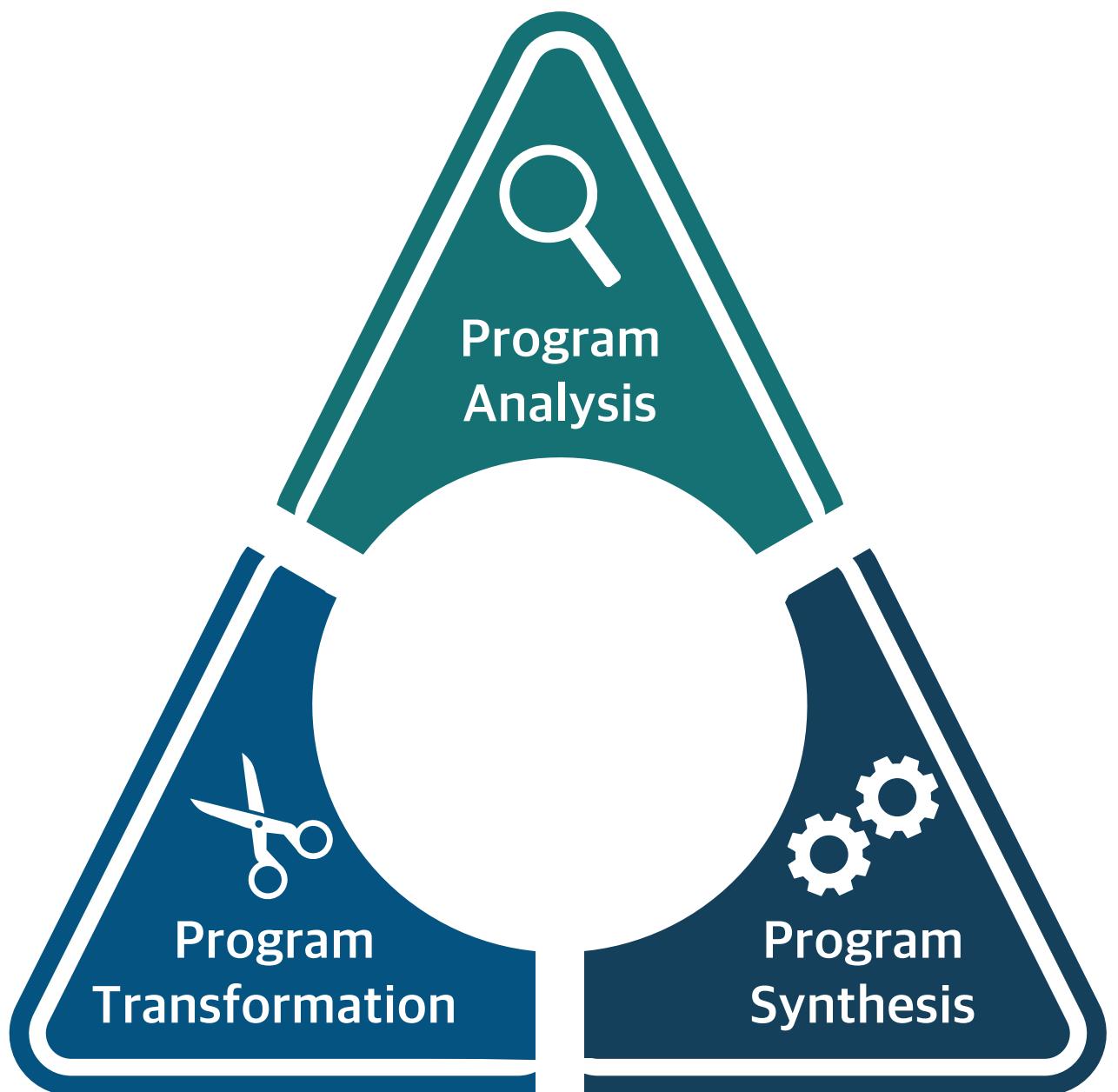
{

**Safe****Simple****Smart****Next-generation
Programming Systems**

My Research



My Research



{



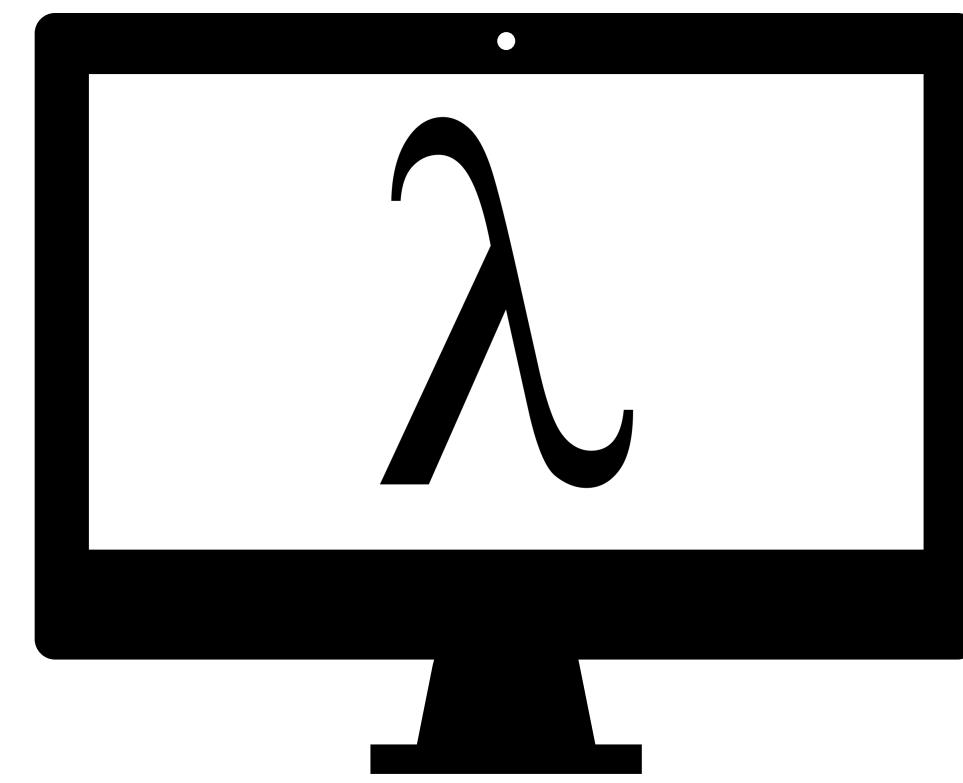
Safe



Simple

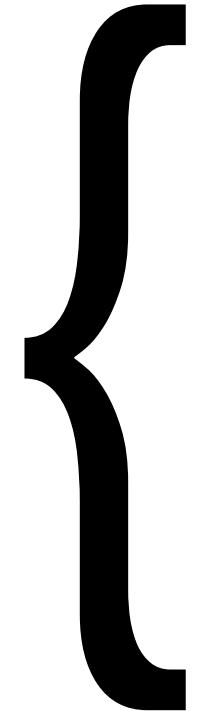
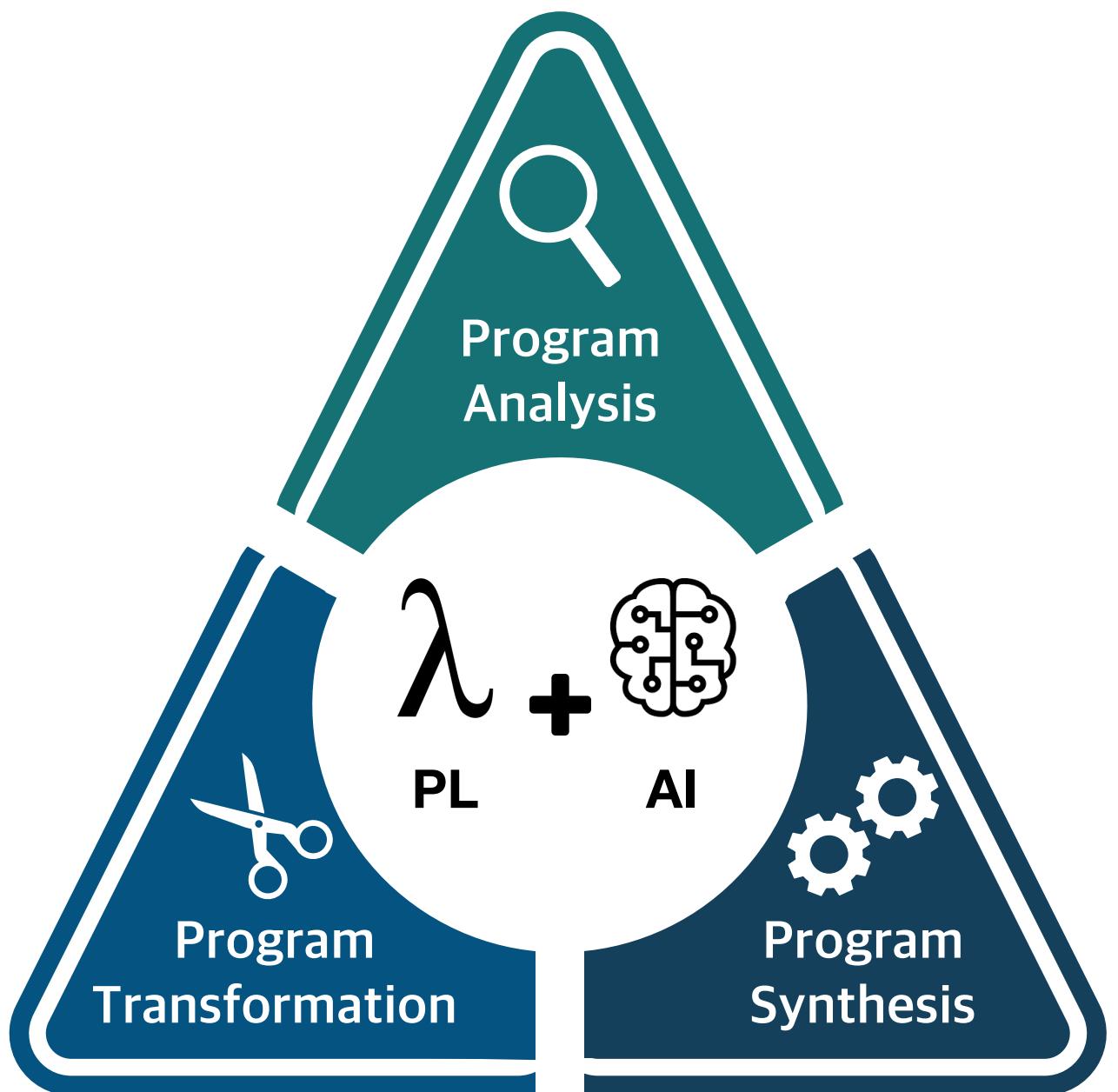


Smart



Next-generation
Programming Systems

My Research



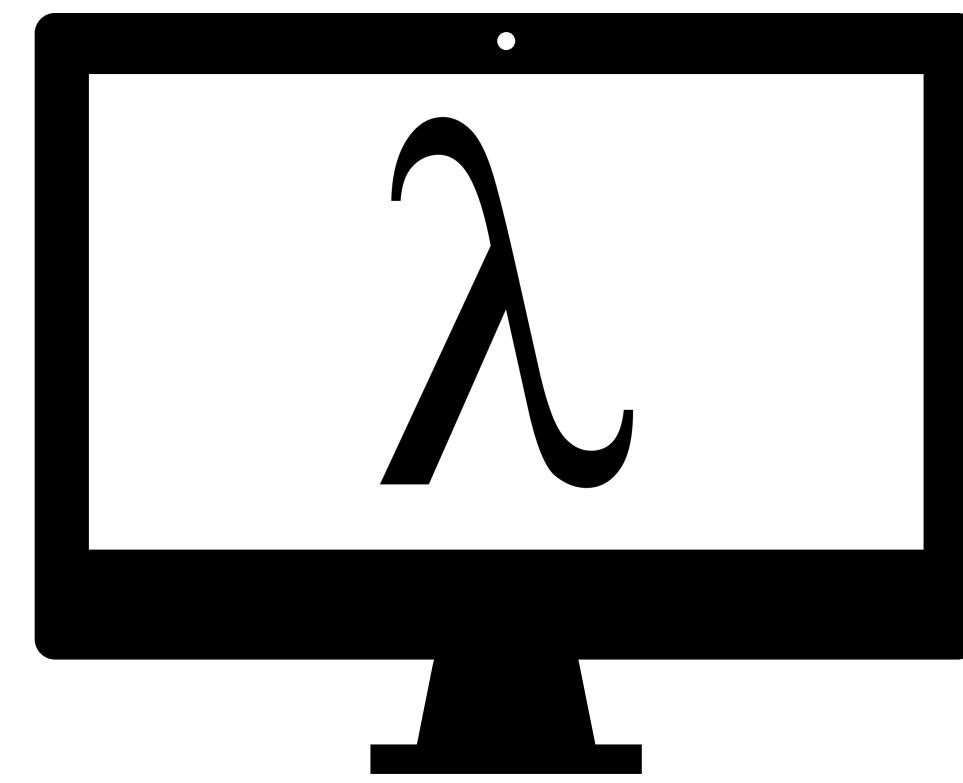
Safe



Simple



Smart



Next-generation
Programming Systems

Course Information

- Course Website: <https://github.com/prosyslab-classroom/is661-advanced-software-security>
- Q&A Board: <https://github.com/prosyslab-classroom/is661-advanced-software-security/issues>
- TAs (mailing list: is661.ta@prosys.kaist.ac.kr)
 - Yeonhee Ryou (류연희)
 - Jaeseong Kwon (권재성)

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
- Any integrity violation: at **LEAST F**
 - See the KAIST CS honor code
- 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 과제를 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 과제들과 관련해 [chegg.com](#)과 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 과제를 작성에 있어 허락 없이 공동 작업을 하거나 부적절한 도움을 받는 행위
- 표절: 길이와 무관하게 적절한 인용이나 언급 없이 타인의 창작물(참고서적, 문헌, 온라인상의 자료)을 무단으로 사용하는 행위

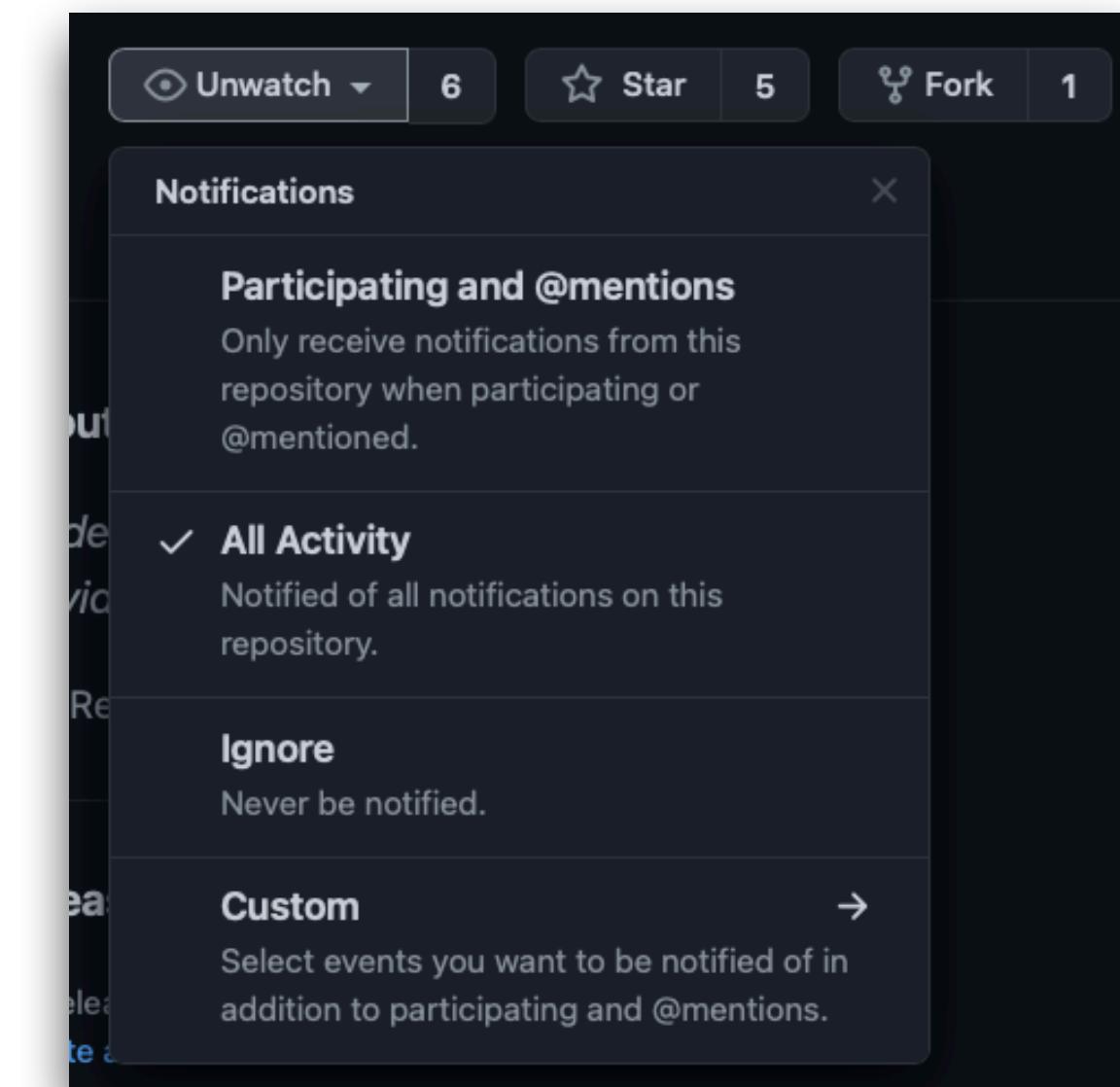
규정 위반 여부의 판단과 처벌 수위는 교과목 담당 교수에 의해 결정됩니다. 모든 부정행위는 전산학부 학사주임 교수 및 학부장님께 보고되며, 적발시 전산학부 내부적으로 아래와 같은 제약을 받습니다.

- 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)

Important Notice (2): Out-of-class

- All Q&A and public notices: Github issue 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



Goal

**How to Be a Successful Grad Student in
Software Security, Programming Language, Software Engineering?**

Course Objective (1): Communication

- Science is communication!
 - Read (research papers, textbooks, etc)
 - Write (research proposals, papers, etc)
 - Talk (conference talk, etc)
 - Ask
 - Think
- Never become an “armchair hacker” (방구석 해커)

Topic and Activities

- Why do you do research?
- How to write scientific articles?
- How to give research talks?
- How to write a proposal?

Schedule			
Date	Topics	Watching	Homework
2/27	Introduction		
2/29	You and Your Research	▶	
3/5	Discussion		HW1: Essay (due: 3/3 23:59:59)
3/7	How to Write a Great Research Paper	▶	
3/12	How to Write Papers So People Can Read Them	▶	
3/14	Discussion		HW2: Your quick sort paper (due: 3/12 23:59:59)
3/19	How to Give a Great Research Talk	▶	
3/21	Research Talk 1		HW3: Essay (due: 3/19 23:59:59)
3/26	Research Talk 2		
3/28	Research Talk 3		
4/2	How to Write a Grant Proposal Talk	▶	
4/4	Project Proposal Talk 1		HW4: Project Proposal (due: 4/2 23:59:59)
4/9	Project Proposal Talk 2		
4/11	Project Proposal Talk 3		

Writing

- Main communication tool in academia
- Basic principle: top-down (두괄식) and short sentence
- Citation: acknowledge someone else's work
- Other details will be discussed later

Writing In Korean (국문 글쓰기)

- Roles of KAIST folks
 - World-leading researcher (in English)
 - Inspiring communicator to the community (in Korean)
 - For newcomers, public officials, etc
 - Idiot's transition algorithm

```
String.split_on_char ' ' word
|> List.map translate_word
|> String.concat " "
```

The screenshot shows a Twitter interface with a dark theme. At the top is a tweet from the account @urimal365 (@국립국어원) with the following content:

[우리말 다듬기] '변이 지방'은 '트랜스 지방'을 다듬은 말입니다.
"이 과자에는 변이 지방이 들어 있지 않다."처럼 다듬은 말 '변이
지방'을 쓸 수 있습니다. #다듬기

Below the tweet are three replies:

- A reply from @hanaosakas (@田舎暮らしアコア) dated March 19, 2013:

@urimal365 님에게 보내는 답글
@urimal365 트랜스 지방의 트랜스는 "변이"라는 의미가 아닙니다.. trans-/cis-로 구
조체의 형태가 다른 것입니다... 굳이 번역할 필요도 다듬을 필요도 없는 과학용어입니
다.. 과학과 관련된 말을 다듬을 때는 과학계에 자문을 구해보심이
- A reply from @urimal365 (@국립국어원) dated March 19, 2013:

건의하실 의견은 공식적인 민원(j.mp/zUyQoR)을 통하여 주시거나,
'우리말 다듬기(malteo.net)'를 이용해 주시기 바랍니다. #순화
- A reply from @Pylon_kr (@PYLON_ / 수정탑) dated March 19, 2013:

@urimal365 님에게 보내는 답글
@urimal365 trans가 변이면 cis는 뭐라고 해야하나요? 유기화학 책 좀 보고 오세요.

Course Objective (2): Critical Thinking

- Do not blindly accept someone else's arguments
 - Paper, proposal, etc
- Why is this problem important and challenging?
- What do they assume?
- What would happen if this technique is applied to my problem?
- How is this related to X?

Paper Review

- Read research papers and write reviews
 - What is this paper about?
 - What is your opinion? (accept or reject)
 - Why do you think so? (persuade other reviewers and authors)
- The same review process of major CS conferences

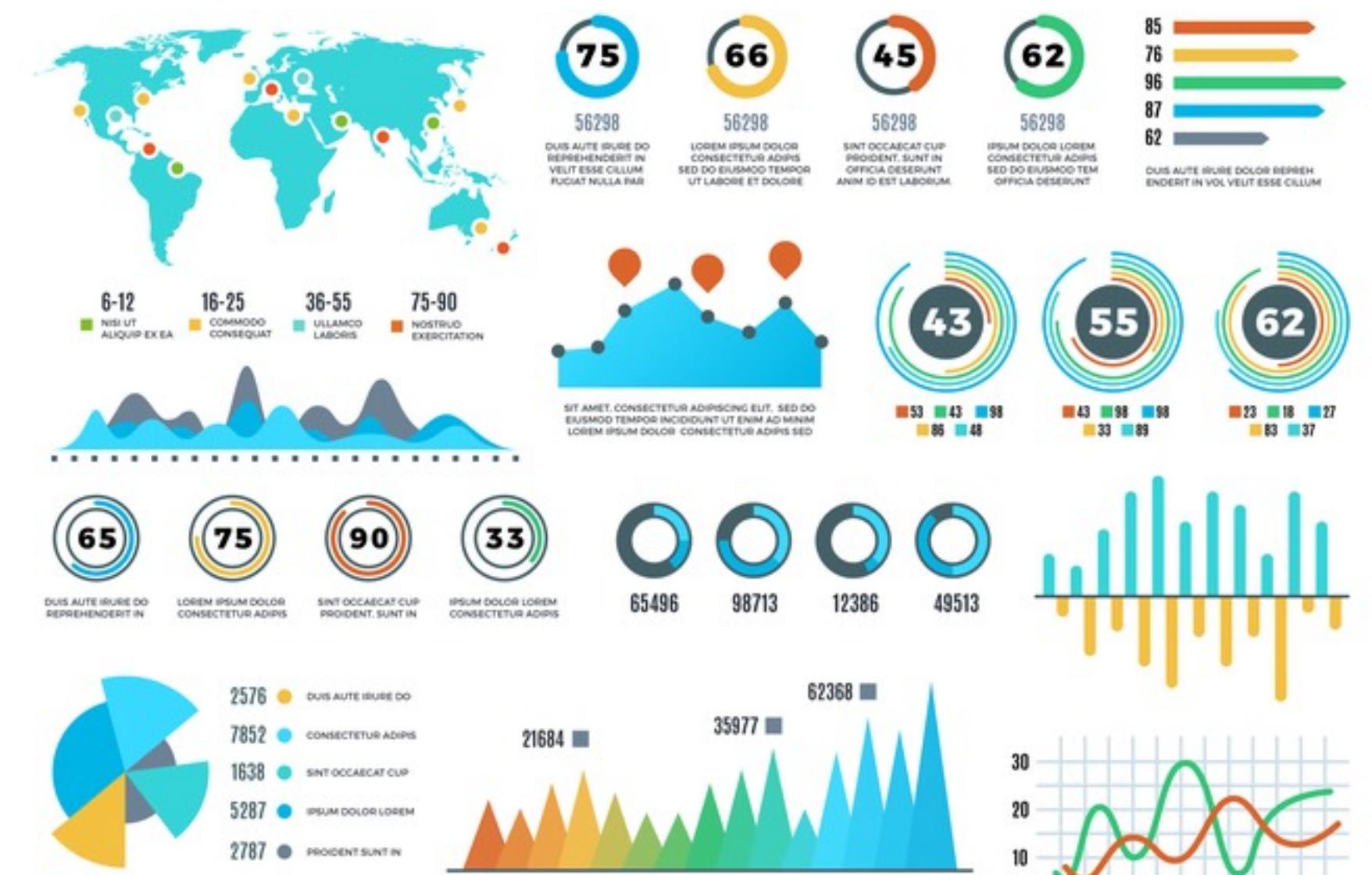
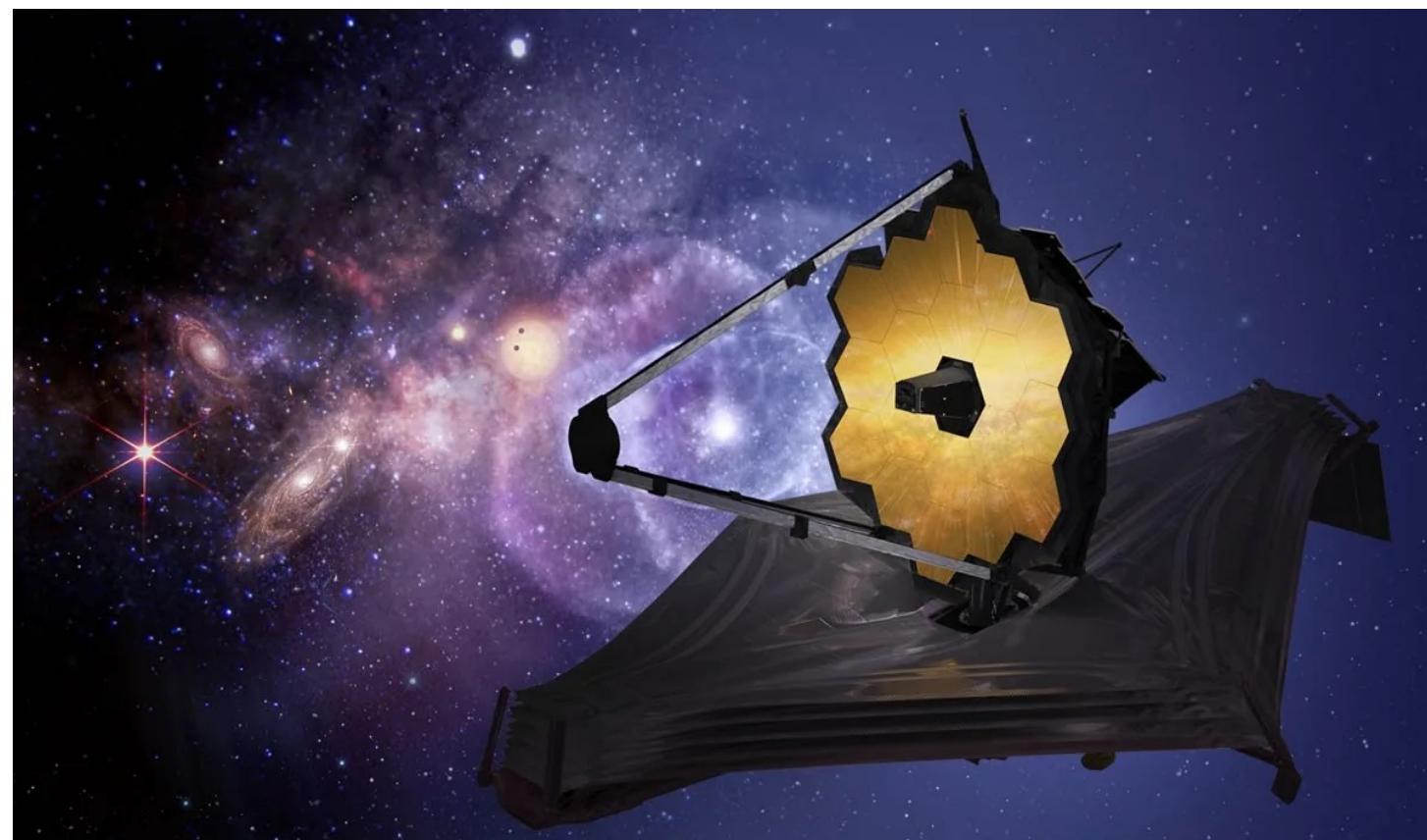
The screenshot shows the KAIST ASOS 2024 conference management system. At the top right, there is a user menu with the email 'kihong.heo@kaist.ac.kr' and a dropdown icon. Below the menu are search and filter fields: '(All)' and 'in Submitted ▾' with a 'Search' button. A red banner at the top center reads 'KAIST ASOS 2024'. On the left, there's a sidebar with navigation links: 'Search', 'Reviews', 'Submissions', 'Administration', 'Settings', 'Users', 'Assignments', 'Mail', 'Action log', 'Conference information', 'Deadlines', and 'Program committee'. The main content area has sections for 'Search', 'Reviews', and 'Submissions'. The 'Search' section contains a search bar with '(All)' and 'in Submitted ▾' dropdown. The 'Reviews' section displays a message: 'The average PC member has submitted 0.0 reviews. ([details](#) · [graphs](#))' and 'As an administrator, you may review [any submitted paper](#)'. It also includes a link to 'Offline reviewing' and a 'Recent activity' section. The 'Submissions' section is currently empty.

Course Objective (3): Finding Your Problem

- Problem-finding is much more important than problem-solving
 - Undergrad: solve a given problem
 - Grad: find your own problem, solve it, and argue that the problem/solution is great
- How to find a good research problem?

Observation

- Beginning of all sciences

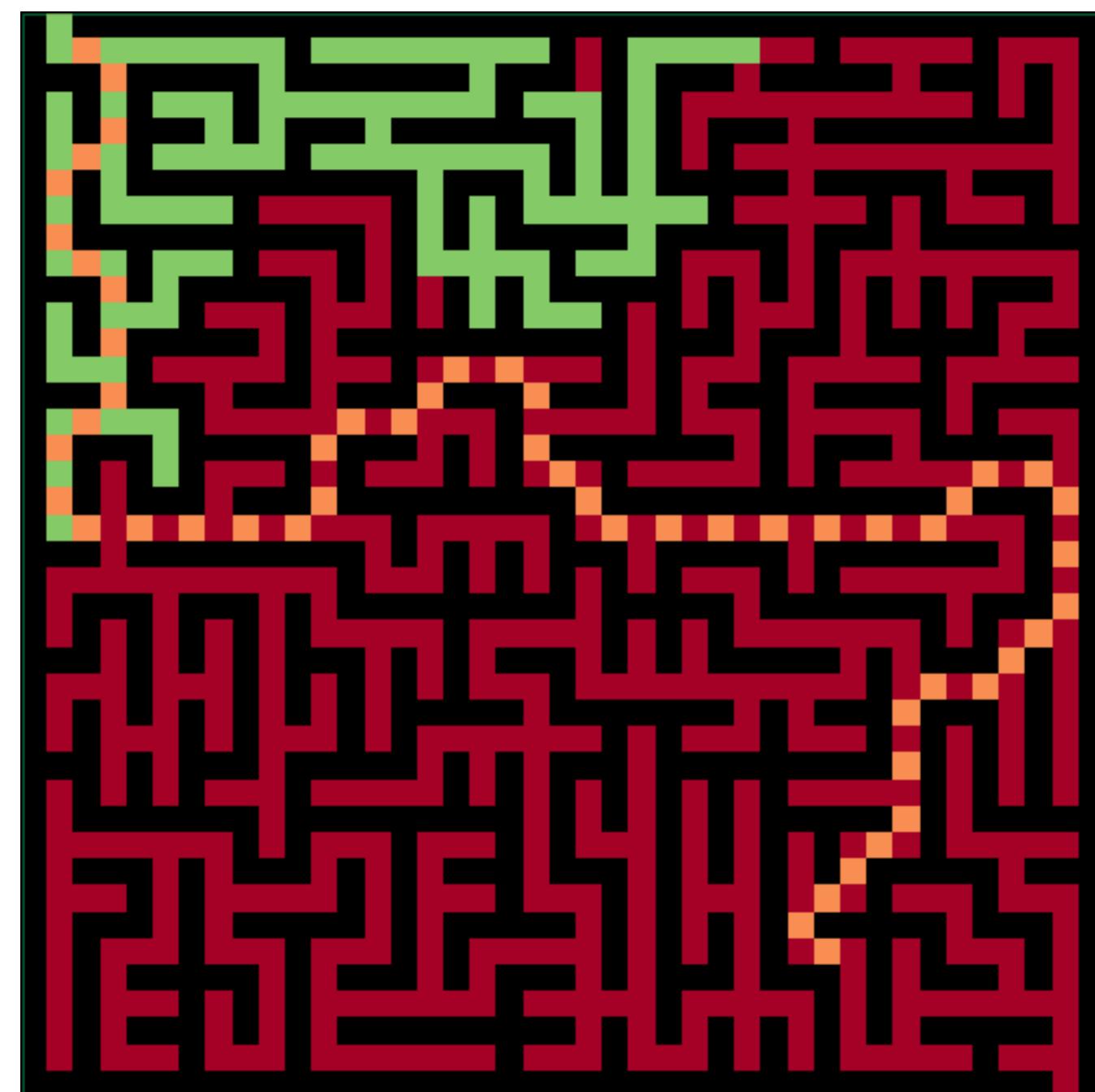


Project

- Make a visualizer for any programming system (hopefully, related to your thesis topic)
 - e.g., program analyzer, fuzzer, synthesizer, compiler, etc
- Clearly shows the behavior of the chosen tool for some aspects using the visualizer
- Argue why this observation is necessary
- See the schedule and prepare your topic in advance

Example

- A visualizer for fuzzer by Haeun Lee, Soomin Kim and Sang Kil Cha. KAIST



Course Activities

- Online lecture: YouTube
- Discussion (mandatory)
 - At least one question or comment for each student

Date	Topics	Watching	Homework
2/27	Introduction		
2/29	You and Your Research	▶	
3/5	Discussion		HW1: Essay (due: 3/3 23:59:59)
3/7	How to Write a Great Research Paper	▶	
3/12	How to Write Papers So People Can Read Them	▶	
3/14	Discussion		HW2: Your quick sort paper (due: 3/12 23:59:59)
3/19	How to Give a Great Research Talk	▶	
3/21	Research Talk 1		HW3: Essay (due: 3/19 23:59:59)
3/26	Research Talk 2		
3/28	Research Talk 3		
4/2	How to Write a Grant Proposal Talk	▶	
4/4	Project Proposal Talk 1		HW4: Project Proposal (due: 4/2 23:59:59)
4/9	Project Proposal Talk 2		
4/11	Project Proposal Talk 3		

Grading

- Homework, discussion, presentation: 60%
 - HW1: Essay & discussion,
 - HW2: Paper & discussion
 - HW3: Review
 - HW4: Essay & research talk
 - HW5: Project proposal & talk
 - HW6: Project proposal review
 - HW7: Paper review & presentation
- Project: 30%
 - Paper
 - Presentation
- Participation: 10%

Homework 1: Writing a Critique

- Watch/read “You and Your Research” on the course webpage
- Write a critique in
 - Korean if you are a native Korean speaker
 - English otherwise
- Read carefully the syntactic and semantic requirements
- Must: proper title (NOT “hw1”, “critique 1” etc), your name and email
- Must NOT: student ID
- All articles will be publicized via the course webpage later

Discussion

- Next class: 3/5
- Topics:
 - Why do you do research rather than any other things?
 - What is great research?
 - What skill sets are needed to do great research?
 - How would you find an important problem?
 - Etc.