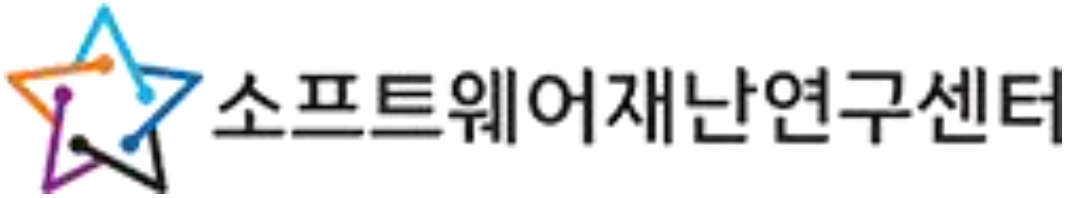
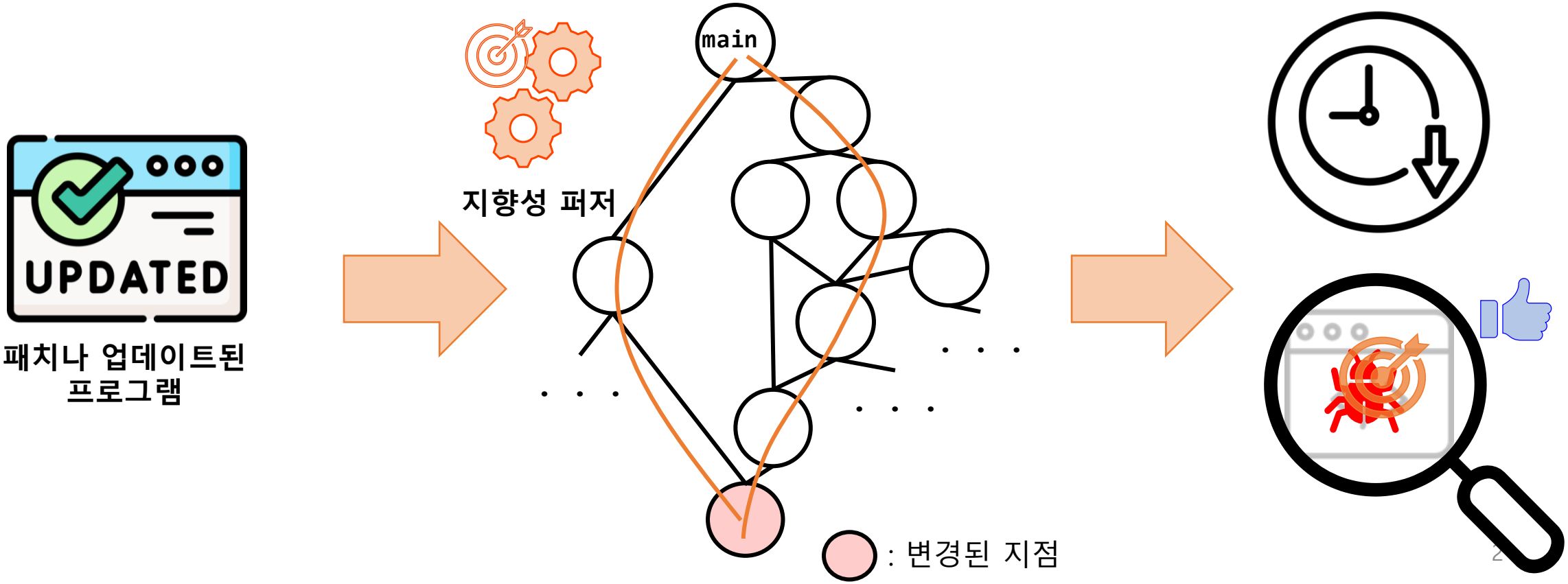
톰슨 샘플링 기반 지향성 협력 퍼저

모현민, 김윤호
한양대학교 컴퓨터소프트웨어학부
소프트웨어공학연구실



지향성 퍼징

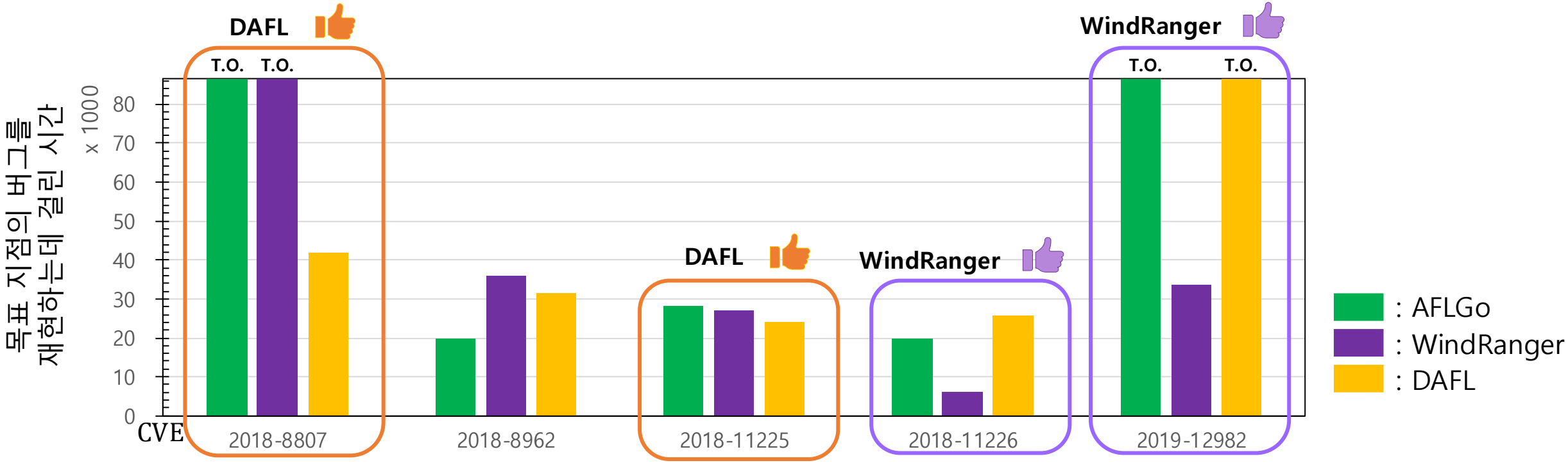
- **특정 목표 지점에 빠르게 도달**하고 **취약점을 재현**할 수 있도록 탐색을 유도하여 입력을 자동 생성하는 퍼징 기법
  - **패치나 업데이트 등**으로 변경된 지점에 **빠르게 도달하여 오류 여부 검증하는 데 효과적**임.



단일 지향성 퍼저의 한계

- 같은 프로그램에서도 **목표 지점마다 각 지향성 퍼저의 결과가 다르기** 때문에 어떤 지향성 퍼저를 사용하는 것이 좋을 지 알기 어려움.
  - swftophp-2018-8807 과 2018-11225 에서는 **DAFL** 이 가장 성능이 좋음.
  - swftophp-2018-11226 과 2019-12982 에서는 **WindRanger** 가 가장 성능이 좋음.

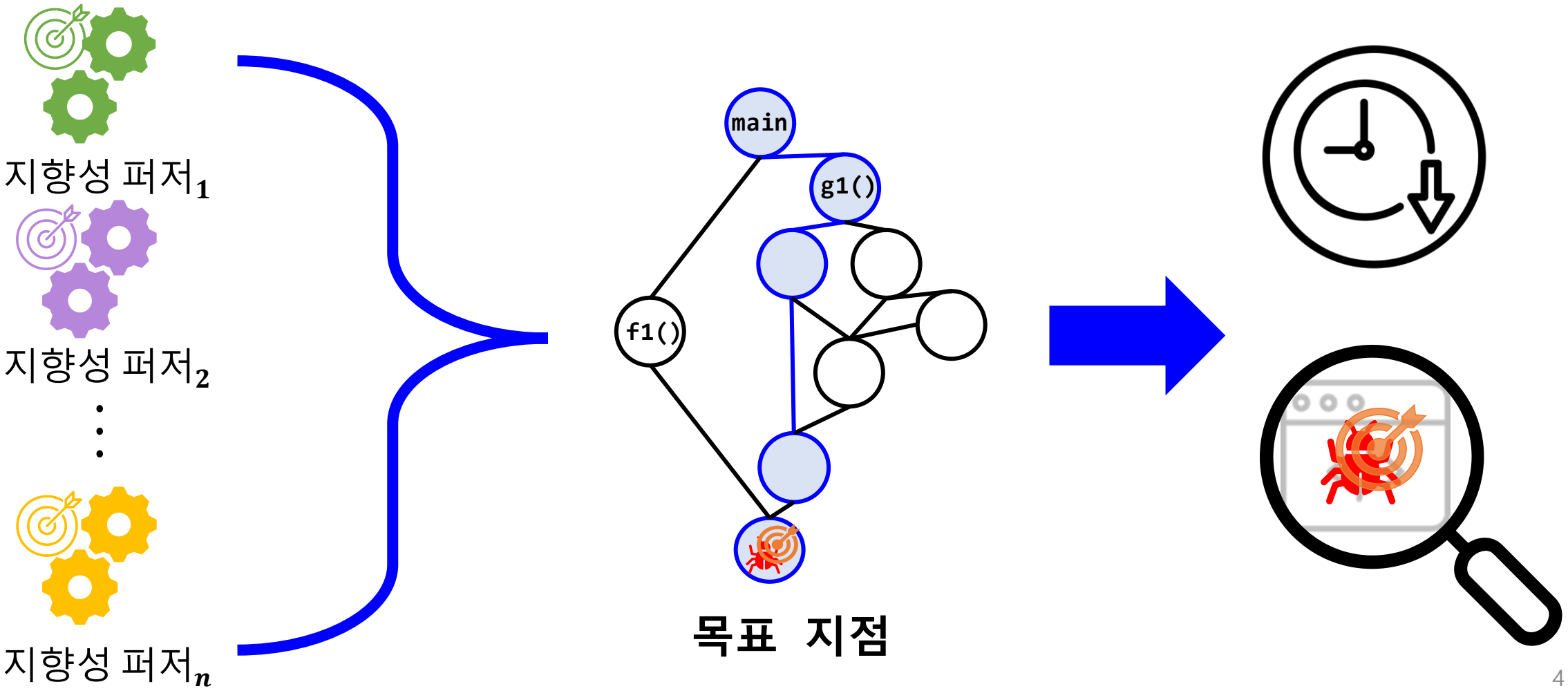
Ex) swftophp 프로젝트의 목표 지점에 대한 각 퍼저의 TTE 결과[1]



❖ [1]각 지향성 퍼저를 24시간 씩 10회 실행하여 평균 TTE 측정한 결과

지향성 협력 퍼저

- **서로 다른 지향성 퍼저들의 전략 강점을 조합**하여 **목표 지점에 빠르게 도달**하고 **취약점을 재현**하기 위해 협력하는 퍼징 기법



도전 과제

- **공통된 평가 기준 부재**
  - **목표 지점 도달 이전**에 **어떤 지향성 퍼저가 목표 지점에 더 가깝게 도달했는지 판단**하기 어려움.

WindRanger

AFLGo

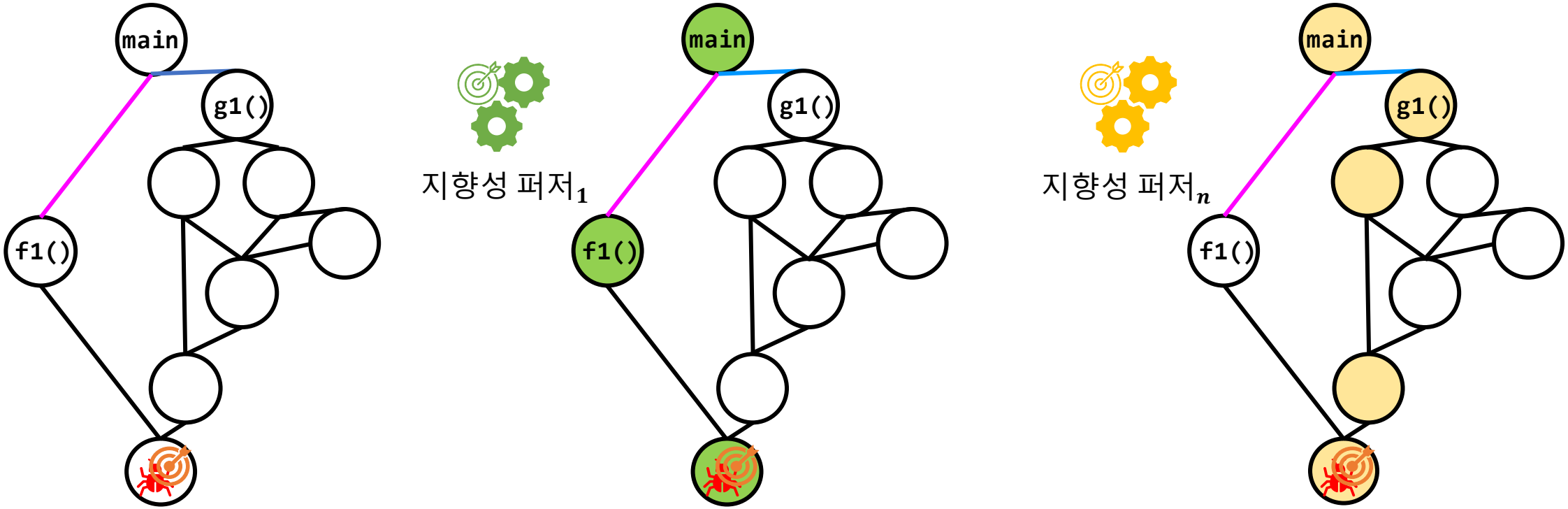
DAFL

공통된 평가 기준 부재

- **각 지향성 퍼저마다의 거리 측정 방식이 달라서** 어떤 지향성 퍼저가 목표 지점에 더 가깝게 도달했는지 판단하기 어려움.

❖ 거리(엣지 수)로 평가
  ➢ main->f1() -> 목표지점 우선 선정

❖ 분기 조건으로 평가
  ➢ main->g1() -> … -> 목표지점 우선 선정

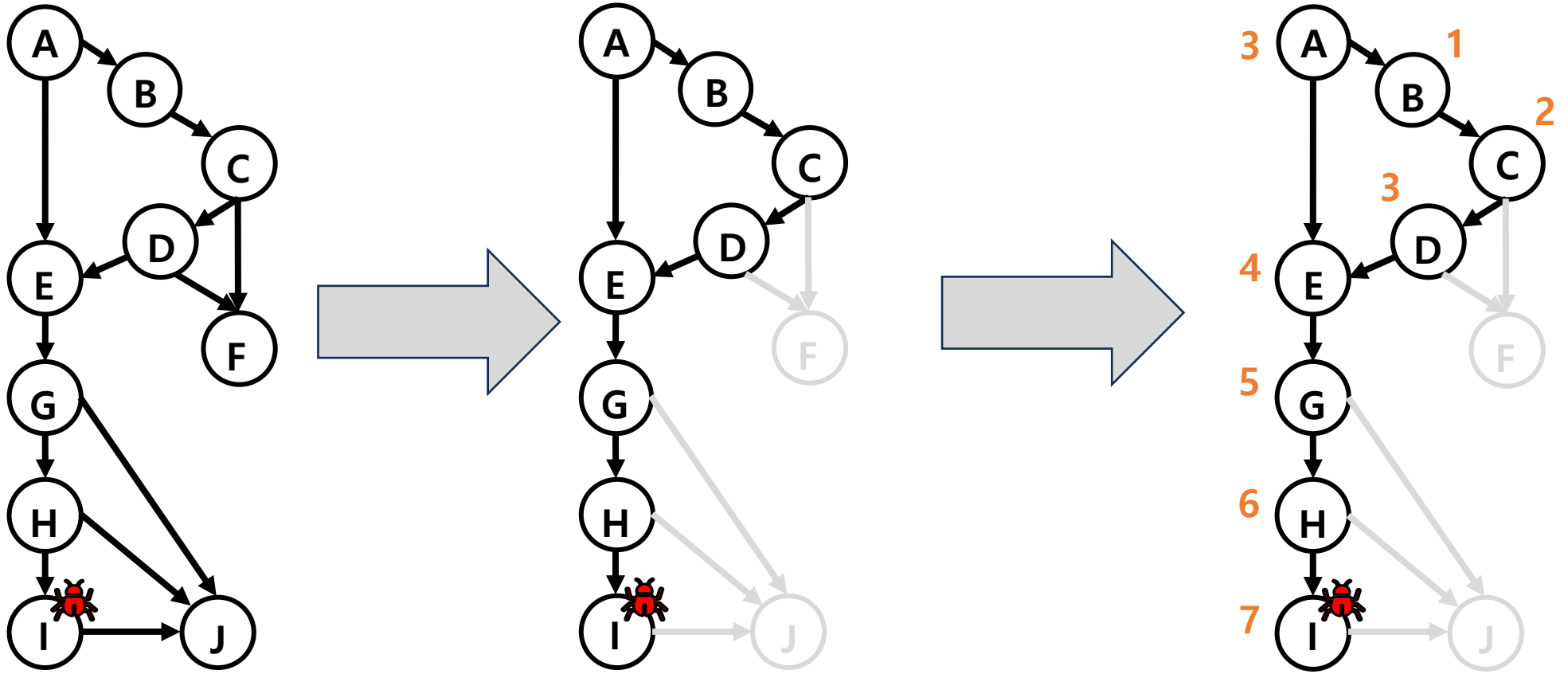


: 쉬운 조건 ex) if(x>10) 등 ...

: 어려운 조건 ex) if(hash(input) == 0xDEABEEF) 특정 해쉬 값 등

공통된 평가 기준 선정

- **DAFL** 논문의 **의미적 관련성 점수** 방식으로 선정
  - **목표 지점과 무관한 경로 측정을 제한**하여 목표 지점과 관련된 코드 부분만 측정.
  - **목표 지점 거리**와 **데이터 연관성을 결합**한 의미적 관련성 측정을 통해 더 정밀하게 평가



도전 과제

- **공통된 평가 기준 부재**
  - **목표 지점 도달 이전**에 **어떤 지향성 퍼저가 목표 지점에 더 가깝게 도달했는지 판단**하기 어려움.

- **퍼저 선택 문제**
  - 성능이 서로 다른 **여러 지향성 퍼저 중**에서 **최적의 지향성 퍼저**를 **실시간으로 선택**하기 어려움.

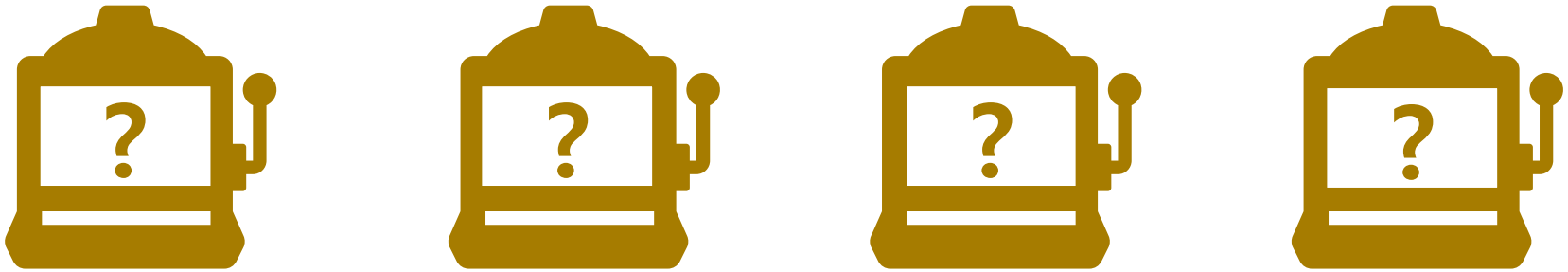
WindRanger

AFLGo

DAFL

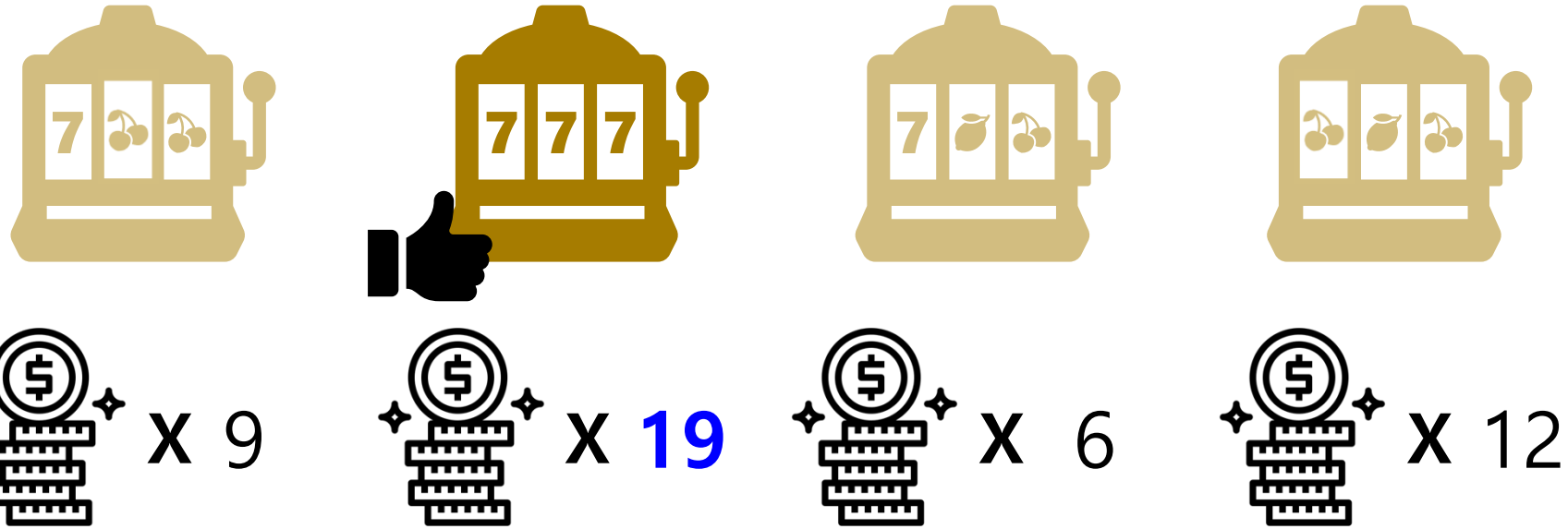
Multi-Armed Bandit(MAB) 문제

- **서로 다른 보상 분포**를 가진 여러 개의 슬롯머신 중에서 누적 보상을 최대화하기 위해 **어떤 슬롯머신을 선택할 지 결정**하는 문제



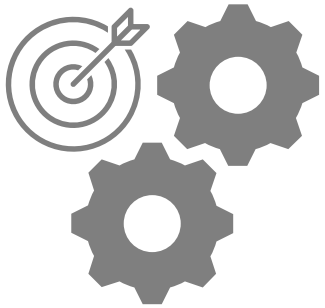
MAB 문제 해결 방안

- 강화학습의 핵심 아이디어 : **탐색과 활용의 균형**
  - 탐색 : 보상이 불확실한 슬롯머신을 선택하여, **더 많은 정보를 수집**하는 과정
  - 활용 : 현재까지 **가장 성능이 좋은 슬롯머신을 선택**하여 즉각적으로 **보상을 최대화**하는 것.

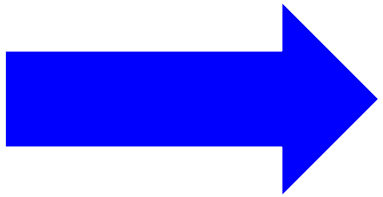


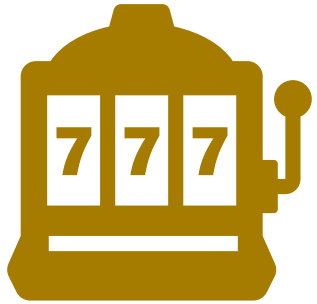
퍼저 선택 문제를 MAB 문제로 모델링

- 실시간으로 성능이 **서로 다른 여러 지향성 퍼저들** 중에서 **가장 빠르게 목표 지점에 도달할 것 같은 지향성 퍼저를 선택**하는 문제

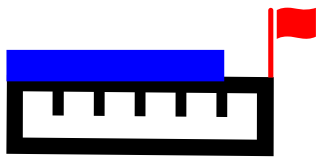


지향성 퍼저

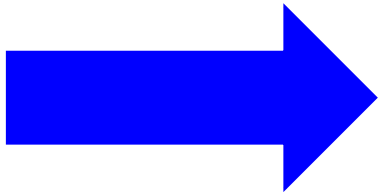




슬롯 머신



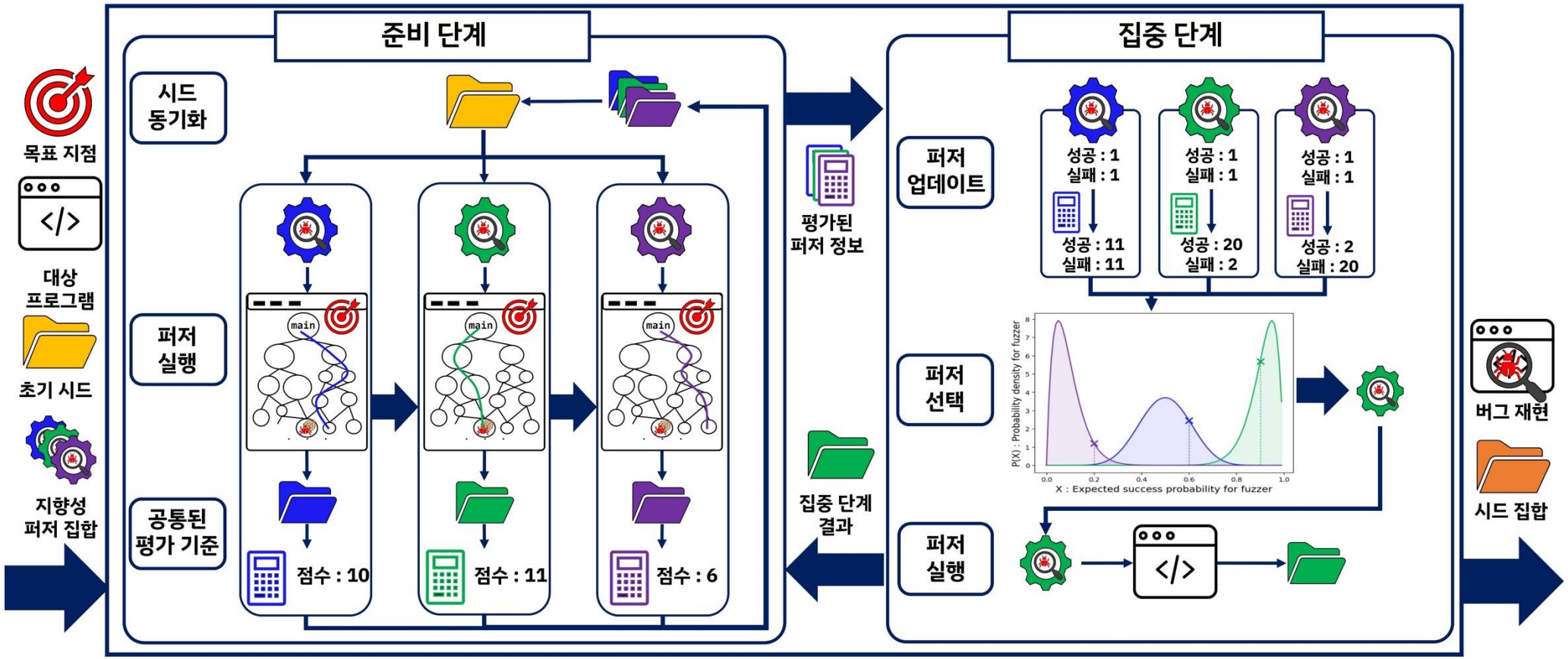
목표 지점 도달



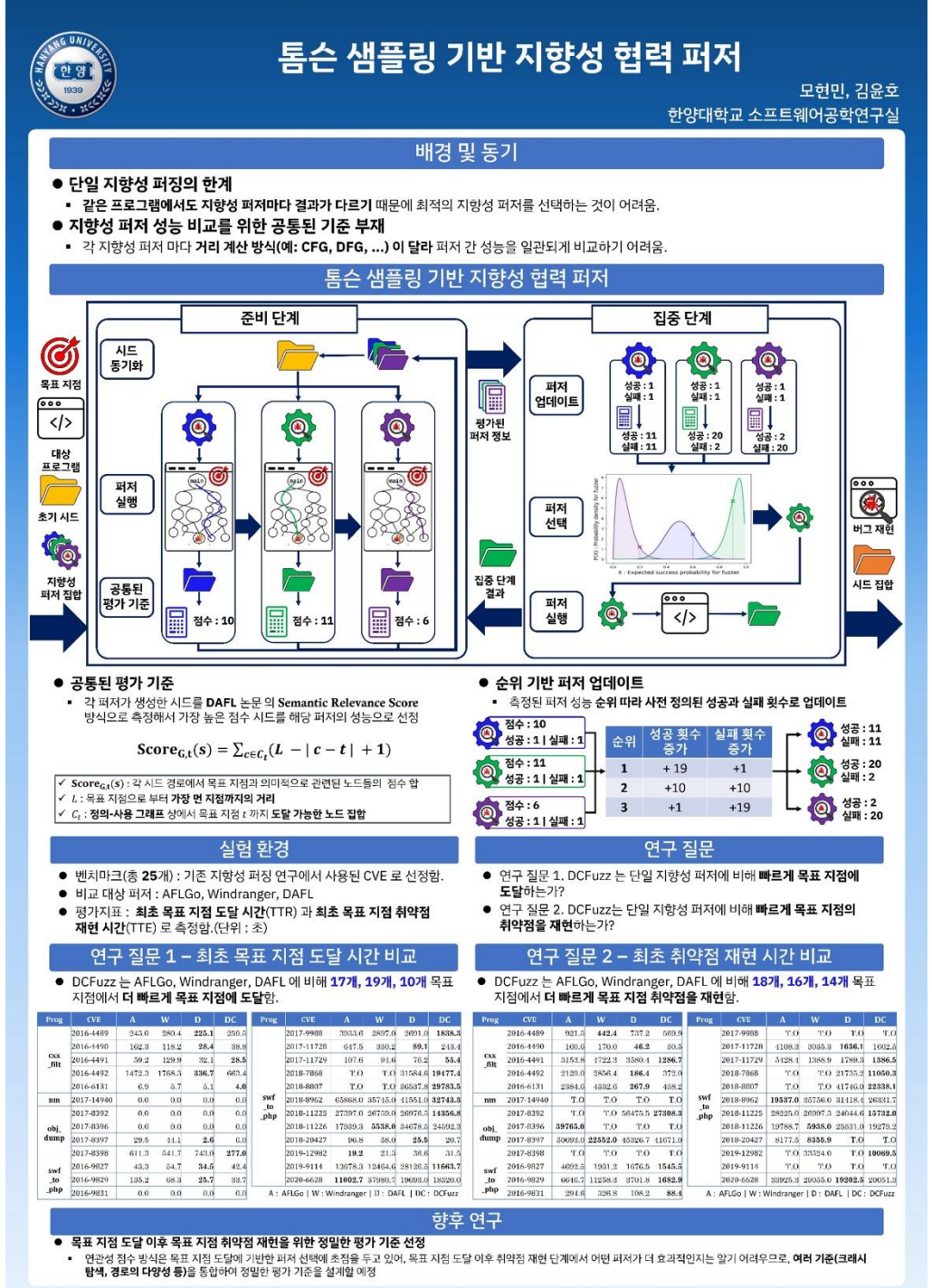
보상

DCFuzz

- **DCFuzz(Directed Collaborative Fuzzer)**
  - **준비 단계**: 각 지향성 퍼저를 실행해서 **공통된 평가 기준**으로 성능 정보를 수집하는 단계
  - **집중 단계**: 수집된 성능 정보를 바탕으로 **순위 기반 퍼저 업데이트**와 **톰슨 샘플링 기반 퍼저 선택**으로 목표 지점 도달 및 취약점 재현 효율을 극대화하는 단계



포스터 세션 때 뵙겠습니다.



소프트웨어재난연구센터