

톰슨 샘플링 기반 지향성 협력 퍼저

모현민, 김윤호

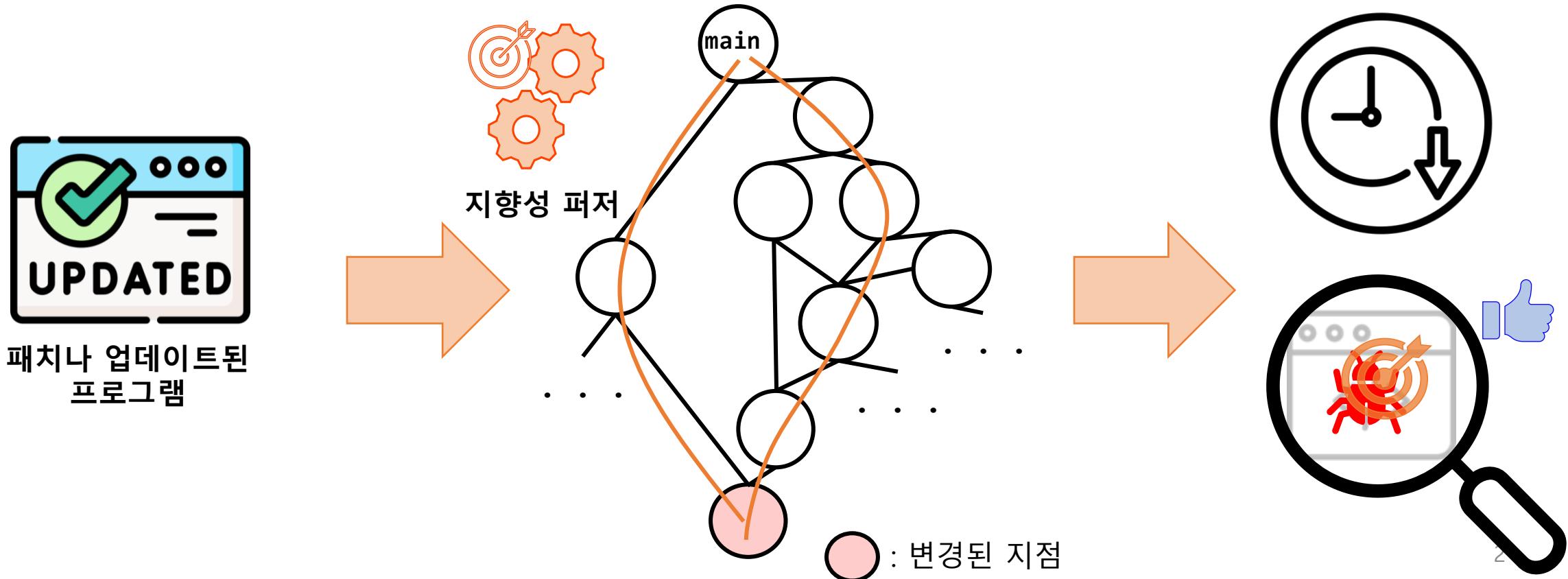
한양대학교 컴퓨터소프트웨어학부
소프트웨어공학연구실



소프트웨어재난연구센터

지향성 퍼징

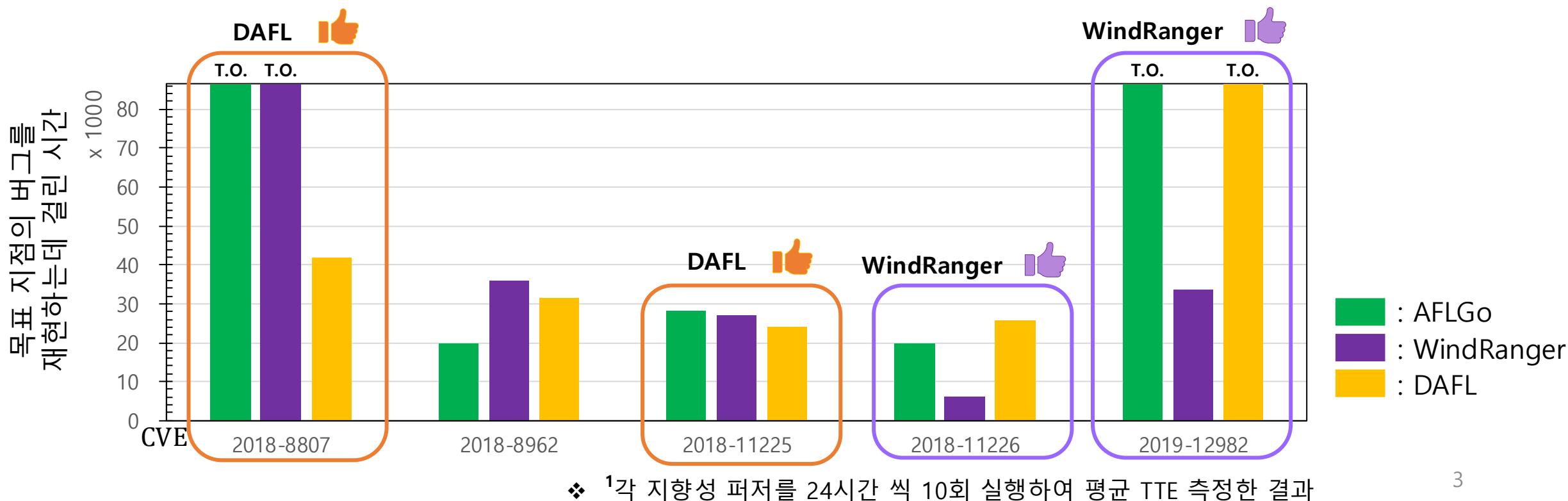
- 특정 목표 지점에 빠르게 도달하고 취약점을 재현할 수 있도록 탐색을 유도하여 입력을 자동 생성하는 퍼징 기법
 - 패치나 업데이트 등으로 변경된 지점에 빠르게 도달하여 오류 여부 검증하는 데 효과적임.



단일 지향성 퍼저의 한계

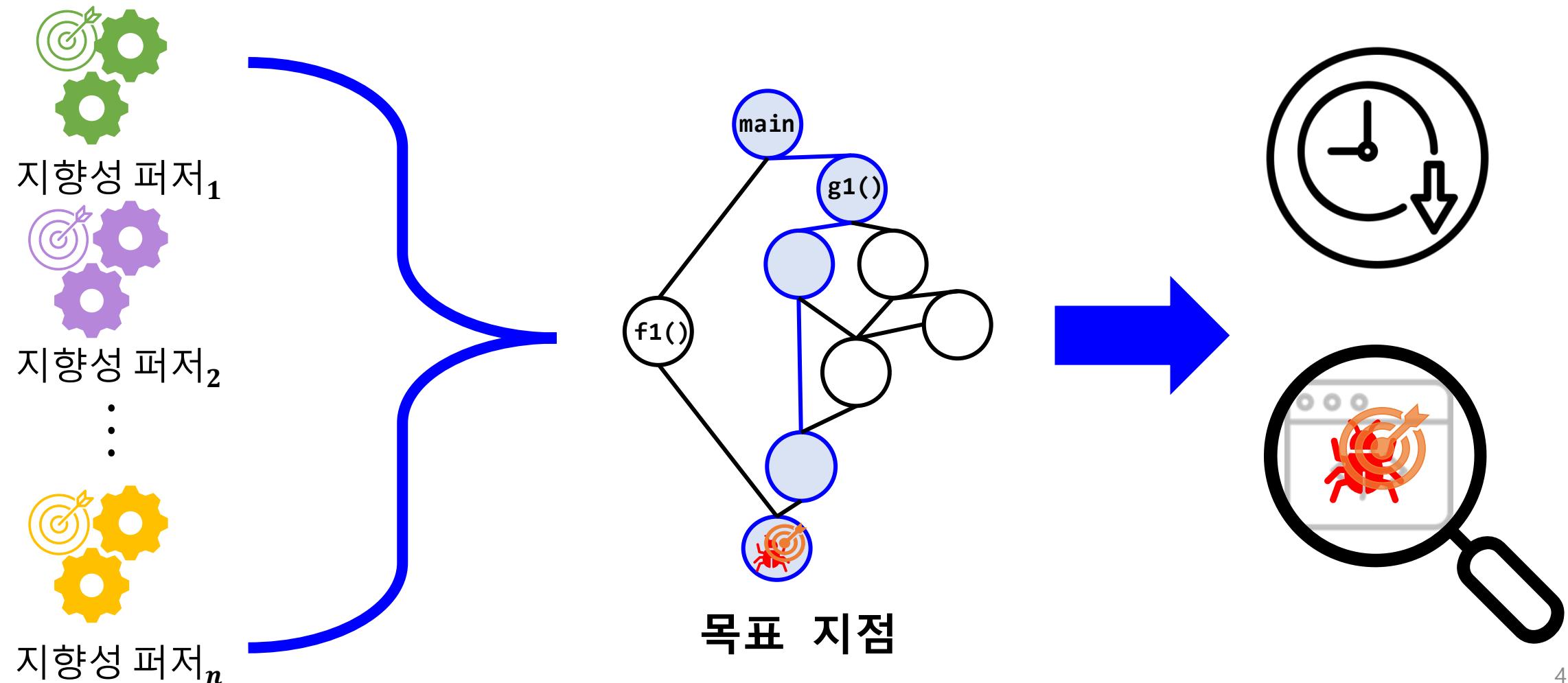
- 같은 프로그램에서도 **목표 지점마다 각 지향성 퍼저의 결과가 다르기 때문에 어떤 지향성 퍼저를 사용하는 것이 좋을지 알기 어려움.**
 - swftophp-2018-8807 과 2018-11225 에서는 **DAFL** 이 가장 성능이 좋음.
 - swftophp-2018-11226 과 2019-12982 에서는 **WindRanger** 가 가장 성능이 좋음.

Ex) swftophp 프로젝트의 목표 지점에 대한 각 퍼저의 TTE 결과¹



지향성 협력 퍼저

- 서로 다른 **지향성** 퍼저들의 전략 강점을 조합하여 **목표 지점**에 빠르게 도달하고 취약점을 재현하기 위해 협력하는 퍼징 기법



도전 과제

• 공통된 평가 기준 부재

- 목표 지점 도달 이전에 어떤 지향성 퍼저가 목표 지점에 더 가깝게 도달했는지 판단하기 어려움.

WindRanger

AFLGo



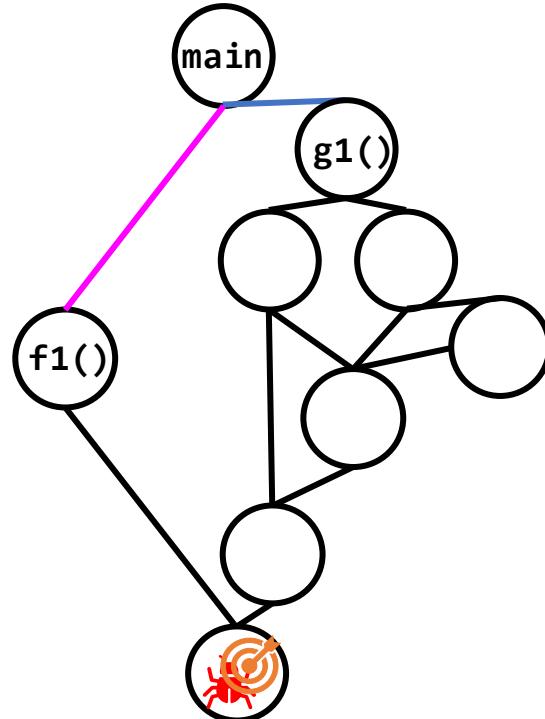
DAFL

공통된 평가 기준 부재

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

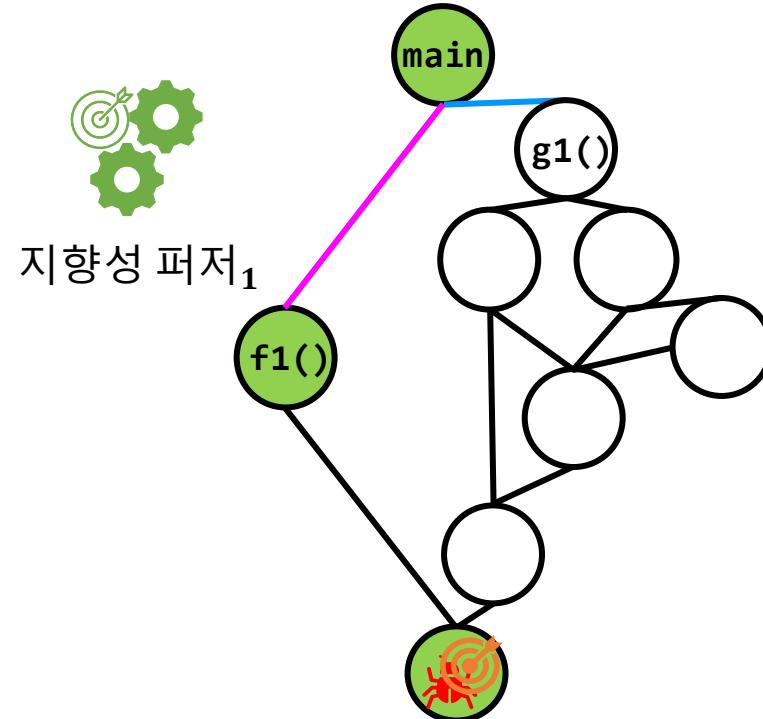
- ❖ 거리(엣지 수)로 평가

➤ main->f1() -> 목표지점 우선 선정



- ❖ 분기 조건으로 평가

➤ main->g1() -> ... -> 목표지점 우선 선정

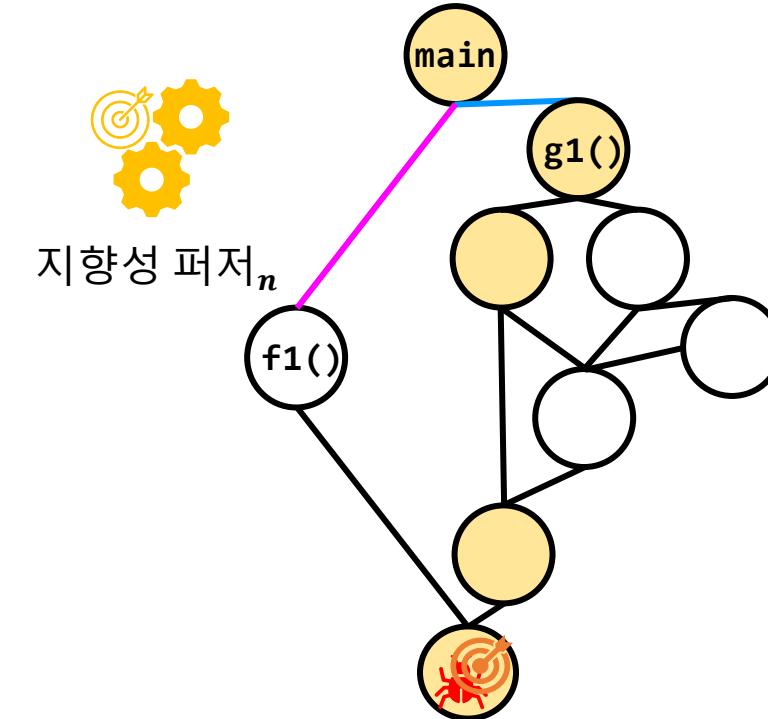


— : 쉬운 조건

ex) if($x > 10$) 등 ...

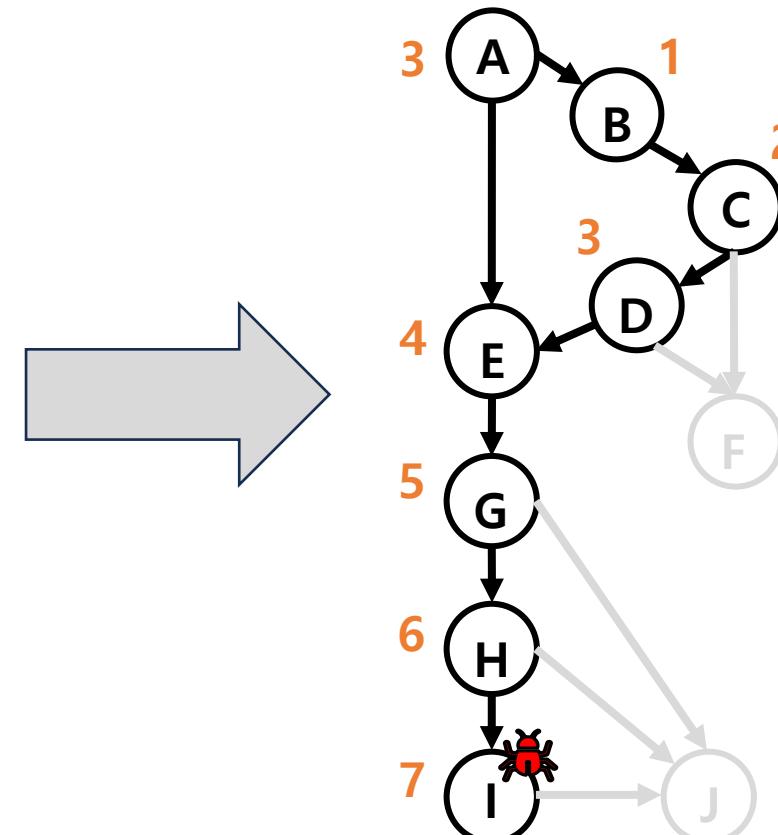
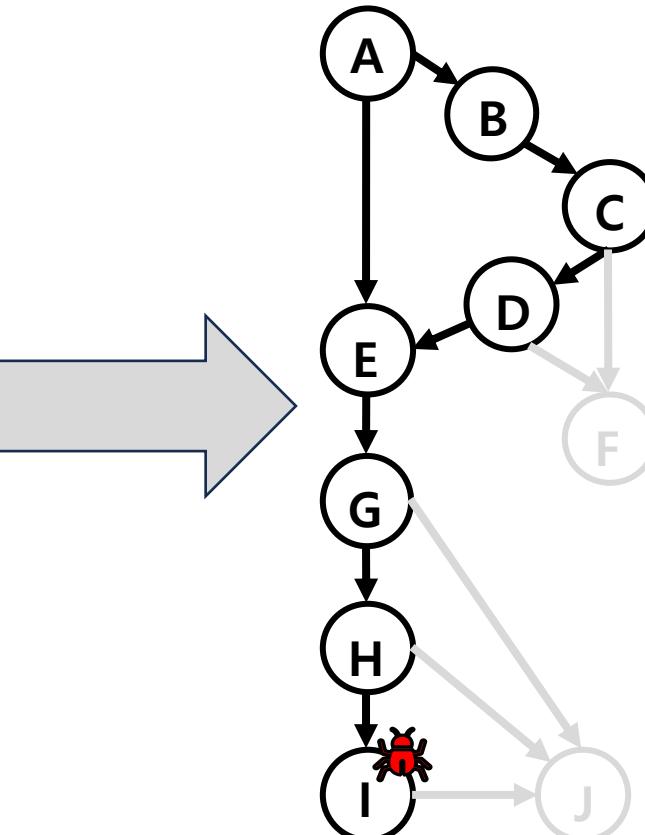
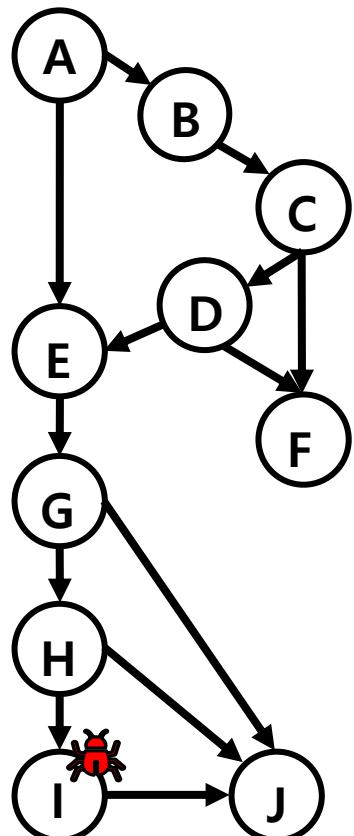
— : 어려운 조건

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 제한하여 목표 지점과 관련된 코드 부분만 측정.
 - 목표 지점 거리와 데이터 연관성을 결합한 의미적 관련성 측정을 통해 더 정밀하게 평가



○ : 목표 지점과 무관한 경로

1 : 의미적 관련성 측정

도전 과제

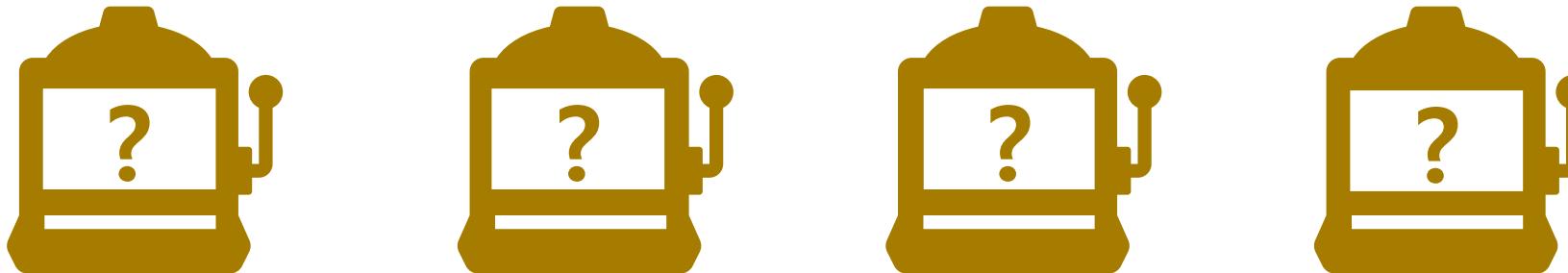
- 공통된 평가 기준 부재
 - 목표 지점 도달 이전에 어떤 지향성 퍼저가 목표 지점에 더 가깝게 도달했는지 판단하기 어려움.
- 퍼저 선택 문제
 - 성능이 서로 다른 여러 지향성 퍼저 중에서 최적의 지향성 퍼저를 실시간으로 선택하기 어려움.

WindRanger



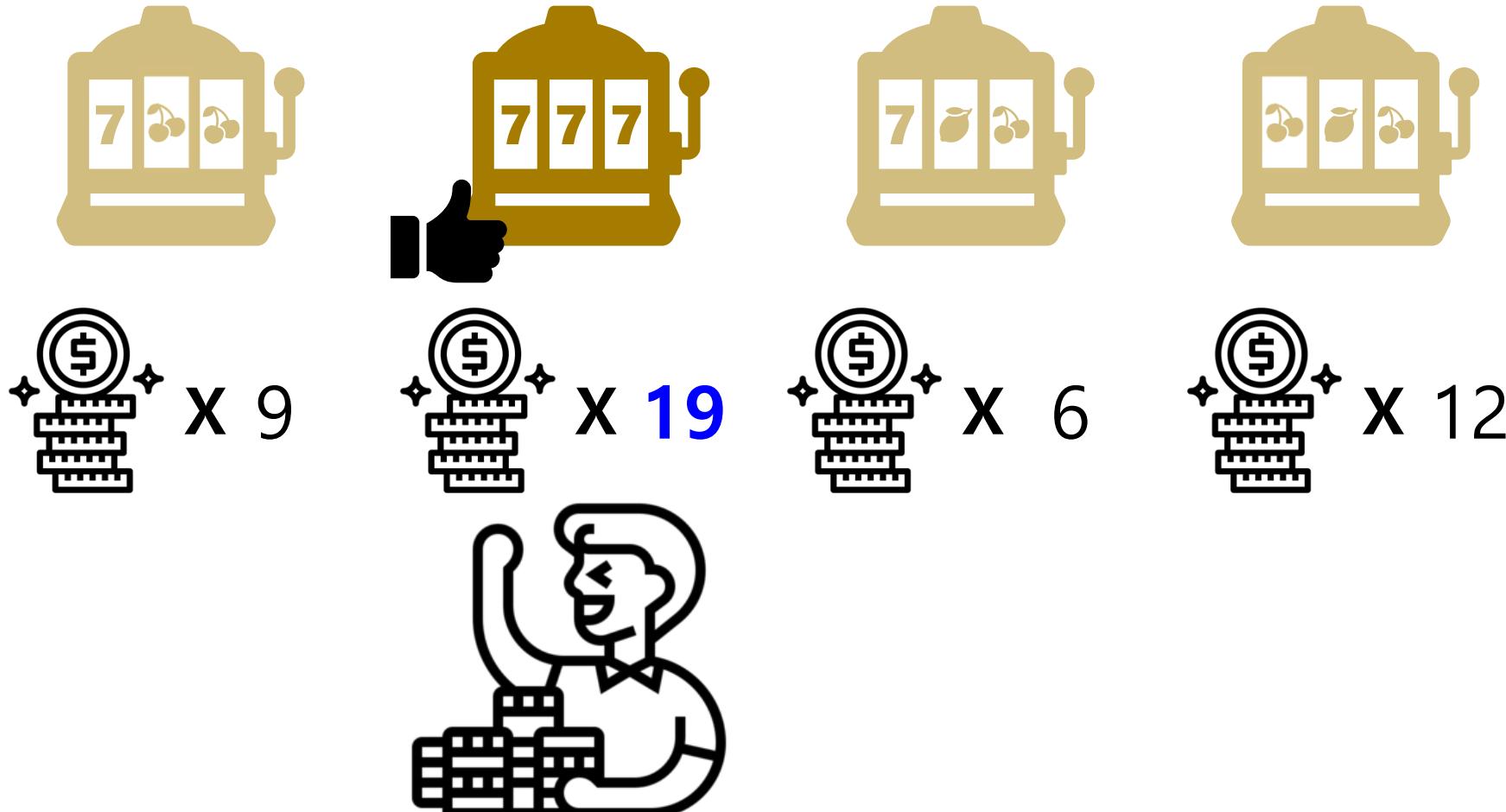
Multi-Armed Bandit(MAB) 문제

- 서로 다른 보상 분포를 가진 여러 개의 슬롯머신 중에서 누적 보상을 최대화하기 위해 어떤 슬롯머신을 선택할지 결정하는 문제



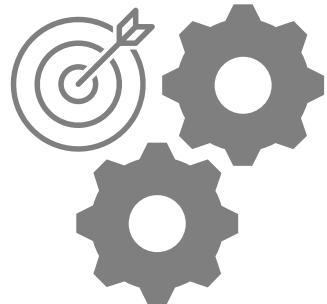
MAB 문제 해결 방안

- 강화학습의 핵심 아이디어 : 탐색과 활용의 균형
 - 탐색 : 보상이 불확실한 슬롯머신을 선택하여, 더 많은 정보를 수집하는 과정
 - 활용 : 현재까지 가장 성능이 좋은 슬롯머신을 선택하여 즉각적으로 보상을 최대화하는 것.



퍼저 선택 문제를 MAB 문제로 모델링

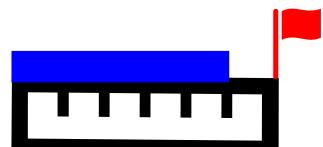
- 실시간으로 성능이 서로 다른 여러 지향성 퍼저들 중에서 **가장 빠르게 목표 지점에 도달할 것 같은 지향성 퍼저를 선택**하는 문제



지향성 퍼저



슬롯 머신



목표 지점 도달

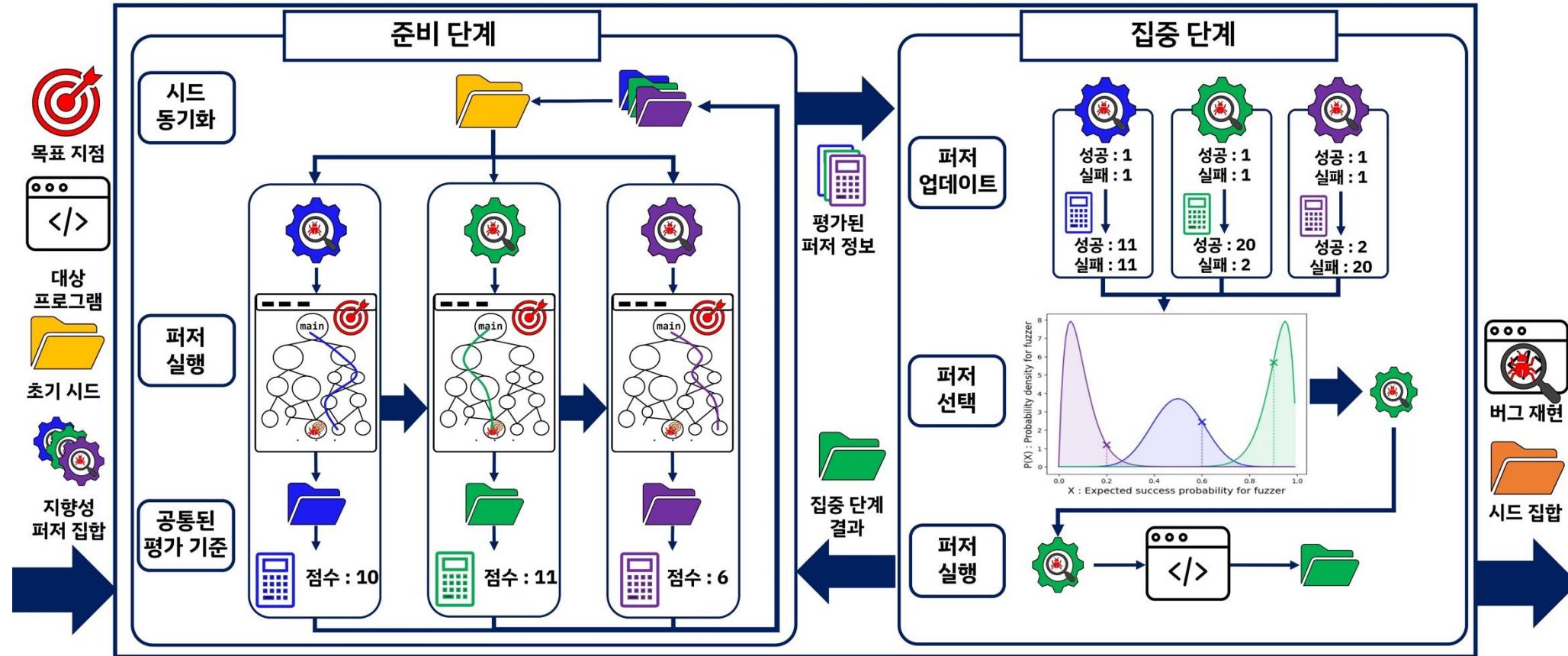


보상

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



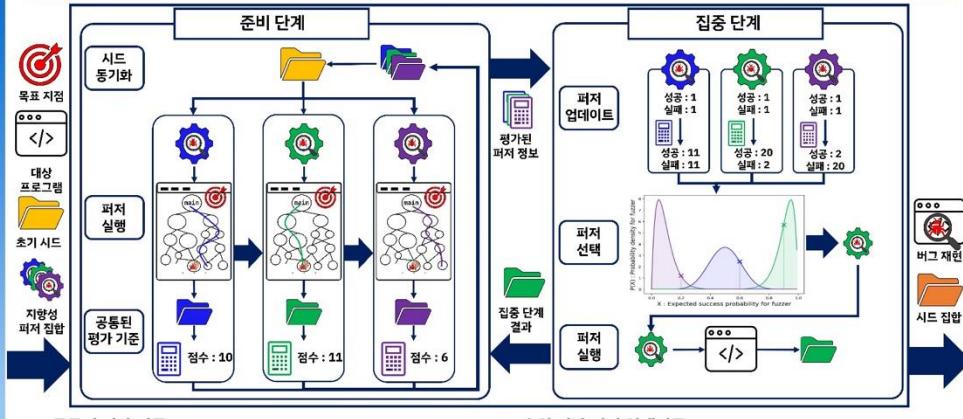
톰슨 샘플링 기반 지향성 협력 퍼저

모현민, 김윤호
한양대학교 소프트웨어공학연구실

배경 및 동기

- 단일 지향성 퍼징의 한계
 - 같은 프로그램에서도 지향성 퍼저마다 결과가 다르기 때문에 최적의 지향성 퍼저를 선택하는 것이 어려움.
- 지향성 퍼저 성능 비교를 위한 공통된 기준 부재
 - 각 지향성 퍼저마다 거리 계산 방식(예: CFG, DFG, ...)이 달라 퍼저 간 성능을 일관되게 비교하기 어려움.

톰슨 샘플링 기반 지향성 협력 퍼저



● 공통된 평가 기준

- 각 퍼저가 생성한 시드를 DAFL 논문의 Semantic Relevance Score 방식으로 측정해서 가장 높은 점수 시드를 해당 퍼저의 성능으로 선정

$$\text{Score}_{G_t}(s) = \sum_{c \in C_t} (L - |c - t| + 1)$$

- ✓ Score_{G_t}(s) : 각 시드 경로에서 목표 지점과 의미적으로 관련된 노드들의 점수 합
- ✓ L : 목표 지점으로부터 가장 먼 차원까지의 거리
- ✓ C_t : 정의 사용 그래프 상에서 목표 지점 t 까지 도달 가능한 노드 집합

실험 환경

- 벤치마크(총 25개) : 기존 지향성 퍼징 연구에서 사용된 CVE로 선정함.
- 비교 대상 퍼저 : AFLGo, Windranger, DAFL
- 평가지표 : 최초 목표 지점 도달 시간(TTR)과 최초 목표 지점 취약점 재현 시간(TTE)로 측정함.(단위: 초)

연구 질문 1 – 최초 목표 지점 도달 시간 비교

- DCFuzz는 AFLGo, Windranger, DAFL에 비해 17개, 19개, 10개 목표 지점에서 더 빠르게 목표 지점에 도달함.

연구 질문 2 – 최초 취약점 재현 시간 비교

- DCFuzz는 AFLGo, Windranger, DAFL에 비해 18개, 16개, 14개 목표 지점에서 더 빠르게 목표 지점 취약점을 재현함.

Prog	CVE	A	W	D	DC	Prog	CVE	A	W	D	DC	Prog	CVE	A	W	D	DC			
cxx	2016-4489	243.0	281.4	225.1	250.5	2017-9988	2053.0	2807.0	2601.0	1838.3	2016-4489	201.0	442.4	737.2	569.9	2017-9988	T.O	T.O	T.O	T.O
cxx	2016-4490	162.3	118.2	28.4	38.8	2017-11728	617.5	350.2	89.1	219.4	2016-4490	100.0	170.0	46.2	80.3	2017-11728	4108.3	3035.3	1536.1	1632.3
cxx	2016-4491	39.2	120.9	32.1	28.5	2017-11729	107.6	94.6	76.2	56.4	2016-4491	3153.8	1722.3	3580.1	1296.7	2017-11729	5128.4	1388.9	1789.3	1386.5
cxx	2016-4492	1472.3	1768.3	336.7	693.4	2018-7668	T.O	31584.6	19477.4	2016-4492	2120.0	38564.4	1864.4	372.0	2018-7668	T.O	2175.3	11050.3	2018-7668	
cxx	2016-4493	6.9	5.7	0.1	4.0	2018-8007	T.O	36587.8	29783.5	2016-4493	2384.0	4382.0	267.9	488.2	2018-8007	T.O	2174.0	22358.1	2018-8007	
cxx	2017-14940	0.0	0.0	0.0	0.0	2018-1223	27397.0	26750.0	26976.0	14356.8	2017-14940	T.O	T.O	T.O	T.O	2018-1223	19557.0	25774.0	31118.4	26351.7
cxx	2017-8392	0.0	0.0	0.0	0.0	2018-1224	17939.0	35358.0	34676.0	24593.3	2017-8392	T.O	T.O	56476.0	27398.8	2018-1224	28259.0	26597.0	24044.6	15732.8
cxx	2017-8396	0.0	0.0	0.0	0.0	2018-12427	96.8	58.0	25.5	20.7	2017-8396	39765.0	T.O	T.O	T.O	2018-12427	10788.7	5938.0	25331.0	19270.2
cxx	2017-8397	29.5	41.1	2.6	6.0	2018-12428	19.2	21.3	36.6	31.5	2017-8397	30693.0	22552.0	45326.7	11071.0	2018-20427	8177.5	8335.9	T.O	T.O
cxx	2017-8398	611.3	541.7	743.0	277.6	2018-12982	19.2	T.O	T.O	T.O	2017-8398	T.O	T.O	T.O	T.O	2018-12982	T.O	35325.4	T.O	18069.5
cxx	2016-9027	43.3	43.8	34.5	42.4	2019-9-114	13078.3	12464.6	28126.0	11663.7	2016-9027	4692.5	1931.2	1076.5	1545.5	2019-9114	T.O	T.O	T.O	T.O
cxx	2016-9629	135.2	68.8	25.7	38.7	2020-6-628	11002.7	37398.7	19693.8	18320.0	2016-9629	6646.7	11258.8	3701.8	1828.0	2020-6-628	38295.3	29030.5	19292.5	20051.3
cxx	2016-9831	0.0	0.0	0.0	0.0	A	AfLGo	W	Windranger	D	DAFL	D	DCFuzz	A	AfLGo	W	Windranger	D	DCFuzz	

향후 연구

- 목표 지점 도달 이후 목표 지점 취약점 재현을 위한 정밀한 평가 기준 선정
 - 연관성 점수 방식은 목표 지점 도달에 기여한 퍼저 선택에 초점을 두고 있어, 목표 지점 도달 이후 취약점 재현 단계에서 어떤 퍼저가 더 효과적인지는 알기 어려우므로, 여러 기준(크레시 탐색, 경로의 다양성 등)을 통합하여 정밀한 평가 기준을 설계할 예정