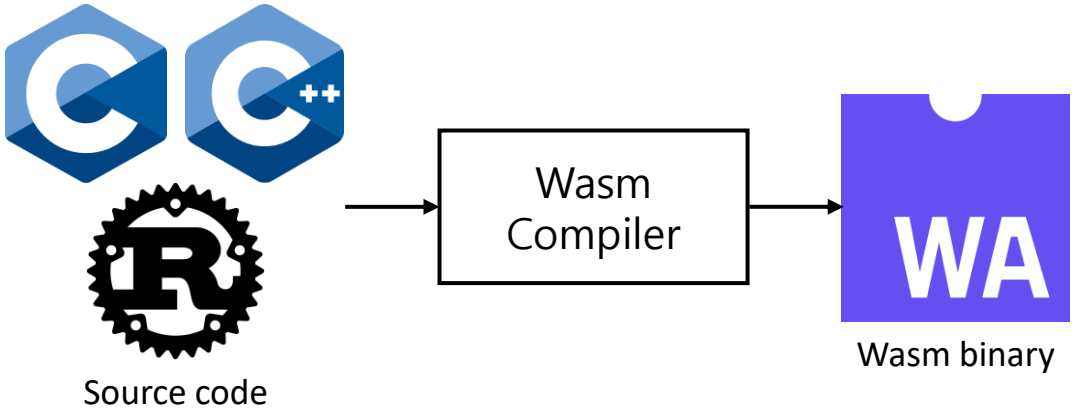
문법 기반 퍼징을 통한 WASI 런타임의 권한 취약점 탐지

이준호[1], 박요한[1], 김진우[2]

[1,2]광운대학교(학부생, 교수)

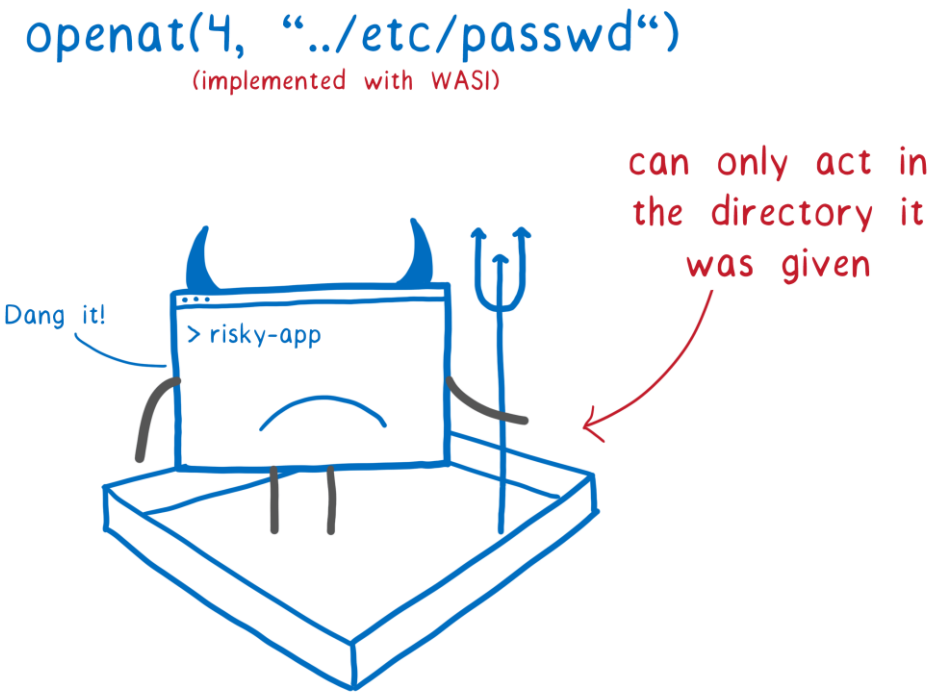
배경 지식

- WebAssembly (Wasm)
  - W3C에서 정의한 바이너리 코드 형식
  - 빠른 성능, 높은 이식성, 샌드박스 환경
  - 클라우드, 엣지, 서버리스 환경에서 활용



배경 지식

- WebAssembly System Interface (WASI)
  - 호스트 자원 접근 인터페이스
  - 권한 기반 보안 모델 (capability-based)
  - Wasmtime, WebAssembly Micro Runtime (WAMR), WasmEdge, Wasmer 에서 지원



서론

- WASI 권한 명세가 아직 불충분함
- 보안 모델 구현이 잘못되면 우회될 수 있음
- 문법 기반 퍼징 도구 WaCFuzz 개발
- 여러 취약점, 버그 발견 및 제보

WASI 분석

- WASI Preview 1 (WASI 0.1)
  - API 정의 위주로 존재
- WASI Preview 2 (WASI 0.2)
  - 권한 관련 내용 포함
  - 여전히 추상적이거나 설명이 불충분
  - Wasmtime만 Preview 2 지원

런타임 분석

- Wasmtime, WAMR, WasmEdge, Wasmer 대상
- 파일 시스템, 네트워크, 환경 변수 위주 분석

- CLI 옵션으로 특정 자원에 권한 부여

```
--dir /etc
--addr-pool=192.168.1.0/24
--env <KEY>=<VALUE>
```

파일 시스템

- 디렉터리에 권한 설정 (‘`--dir`’ 옵션)
- 호스트 경로를 가상 경로로 매핑하는 기능

런타임	다중 디렉터리 권한	심볼릭 링크 권한	읽기, 쓰기 권한
Wasmtime	O	O	X
WAMR	O	O	X
WasmEdge	X	X	O
Wasmer	O	△	X

파일 시스템

- 디렉터리에 권한 설정 (‘`--dir`’ 옵션)
- 호스트 경로를 가상 경로로 매핑하는 기능

런타임	다중 디렉터리 권한	심볼릭 링크 권한	읽기, 쓰기 권한
Wasmtime	O	O	X
WAMR	O	O	X
WasmEdge	**X**	**X**	**O**
Wasmer	O	△	X

네트워크

- 런타임 별로 차이가 많은 부분

런타임	기본 연결 정책	특정 주소 허용	트래픽 방향 설정
Wasmtime	모두 거부	X	X
WAMR	모두 거부	O	X
WasmEdge	모두 허용	X	X
Wasmer	모두 거부	O	O

네트워크

- 런타임 별로 차이가 많은 부분

런타임	기본 연결 정책	특정 주소 허용	트래픽 방향 설정
Wasmtime	모두 거부	X	X
WAMR	**모두 거부**	**O**	**X**
WasmEdge	모두 허용	X	X
Wasmer	**모두 거부**	**O**	**O**

네트워크

- 런타임 별로 차이가 많은 부분

런타임	기본 연결 정책	특정 주소 허용	트래픽 방향 설정
Wasmtime	모두 거부	X	X
WAMR	모두 거부	O	X
WasmEdge	**모두 허용**	**X**	**X**
Wasmer	모두 거부	O	O

환경 변수

- 초기 샌드박스에는 환경 변수가 존재하지 않음
- ‘`--env key=value`’ 형태로 환경 변수 전달

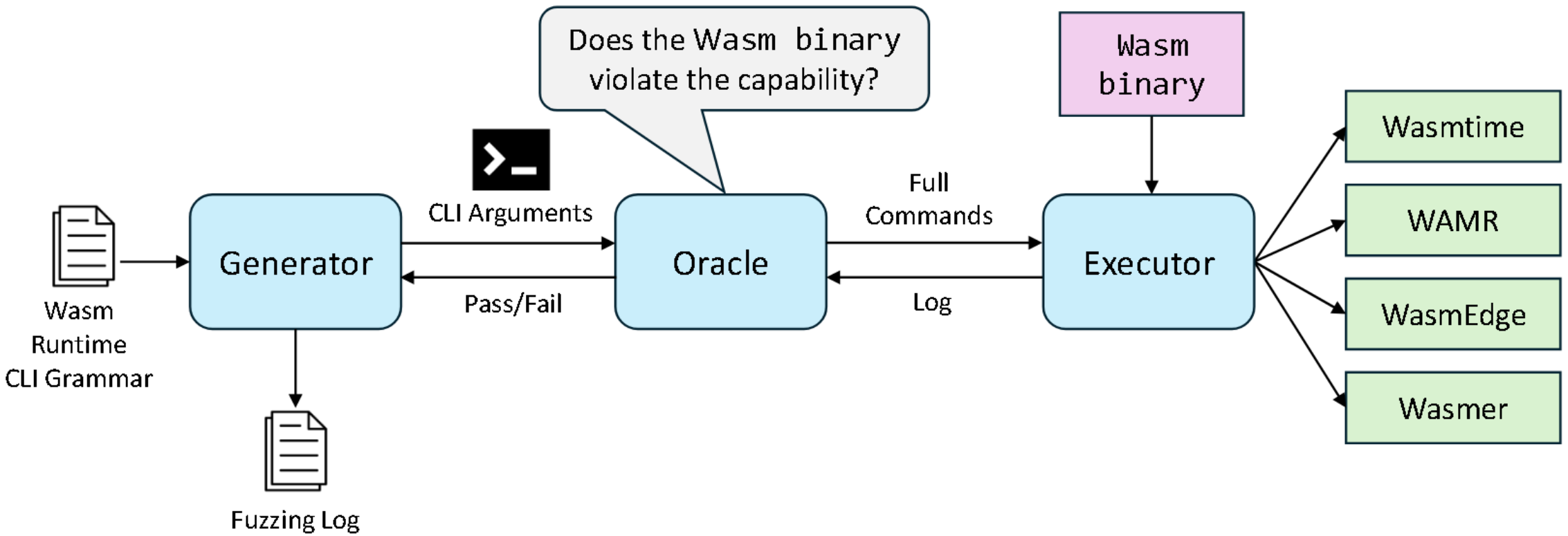
런타임	환경 변수 전달	호스트 환경 변수 접근
Wasmtime	O	O
WAMR	O	X
WasmEdge	O	X
Wasmer	O	O

환경 변수

- 초기 샌드박스에는 환경 변수가 존재하지 않음
- ‘`--env key=value`’ 형태로 환경 변수 전달

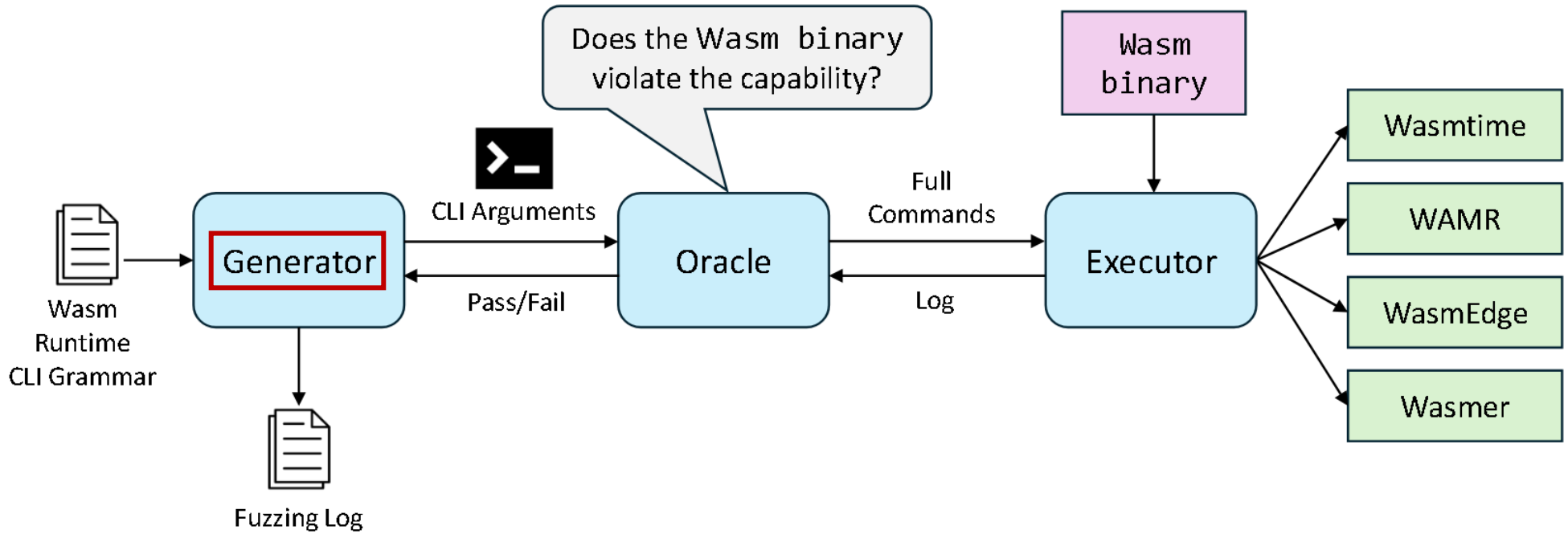
런타임	환경 변수 전달	호스트 환경 변수 접근
Wasmtime	**O**	**O**
WAMR	O	X
WasmEdge	O	X
Wasmer	**O**	**O**

WaCFuzz 개요


Does the Wasm binary violate the capability?
Wasm binary
Wasmtime
WAMR
WasmEdge
Wasmer
CLI Arguments
Full Commands
Wasm Runtime CLI Grammar
Generator
Oracle
Executor
Pass/Fail
Log
Fuzzing Log

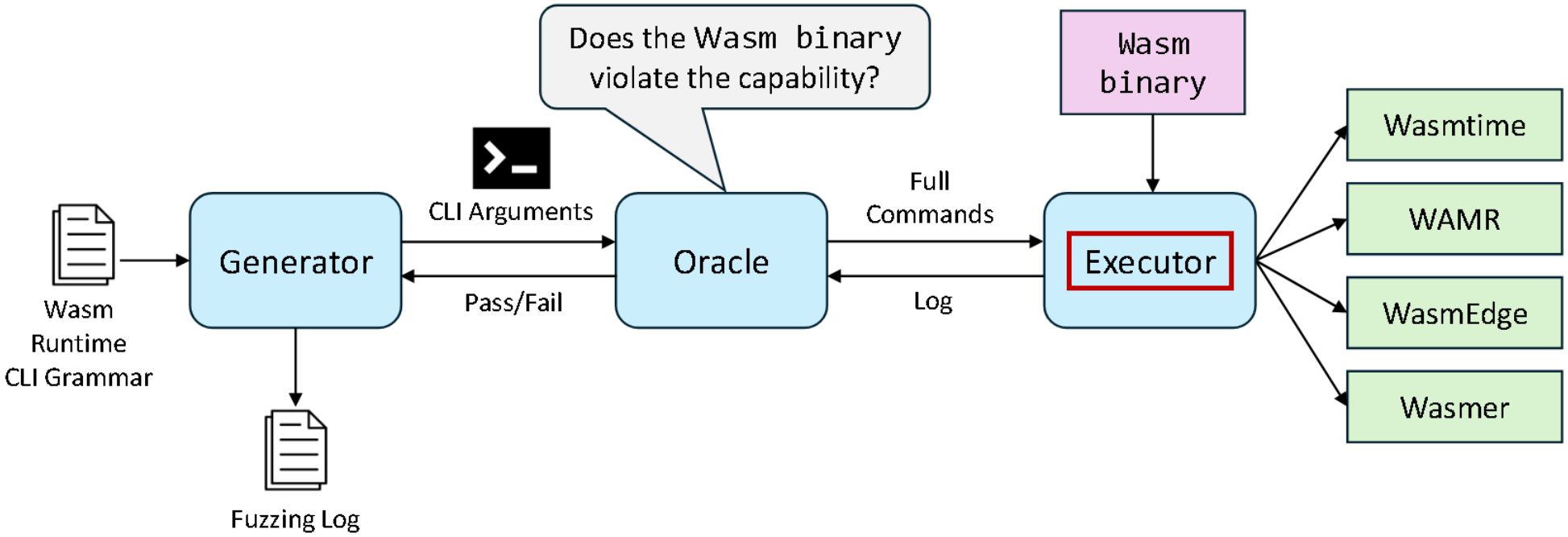
WaCFuzz 개요

- Generator
  - 런타임 CLI 문법 기반 옵션 생성



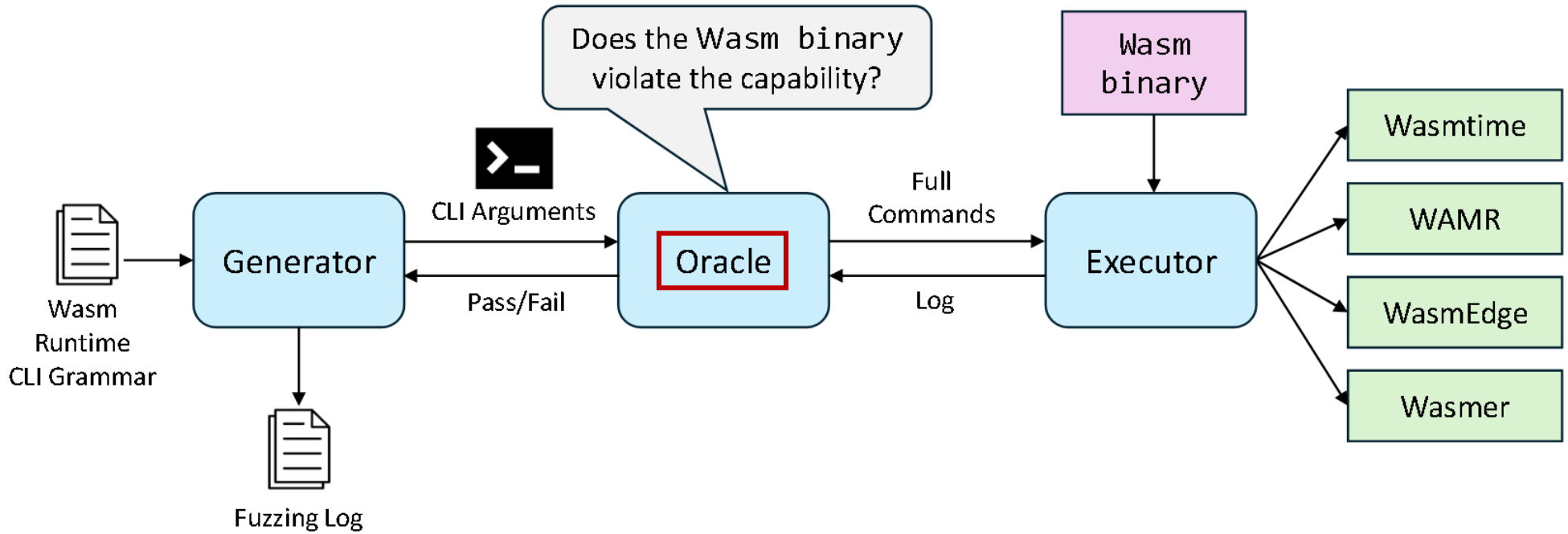
WaCFuzz 개요

- Executor
  - 생성한 옵션으로 프로그램 실행



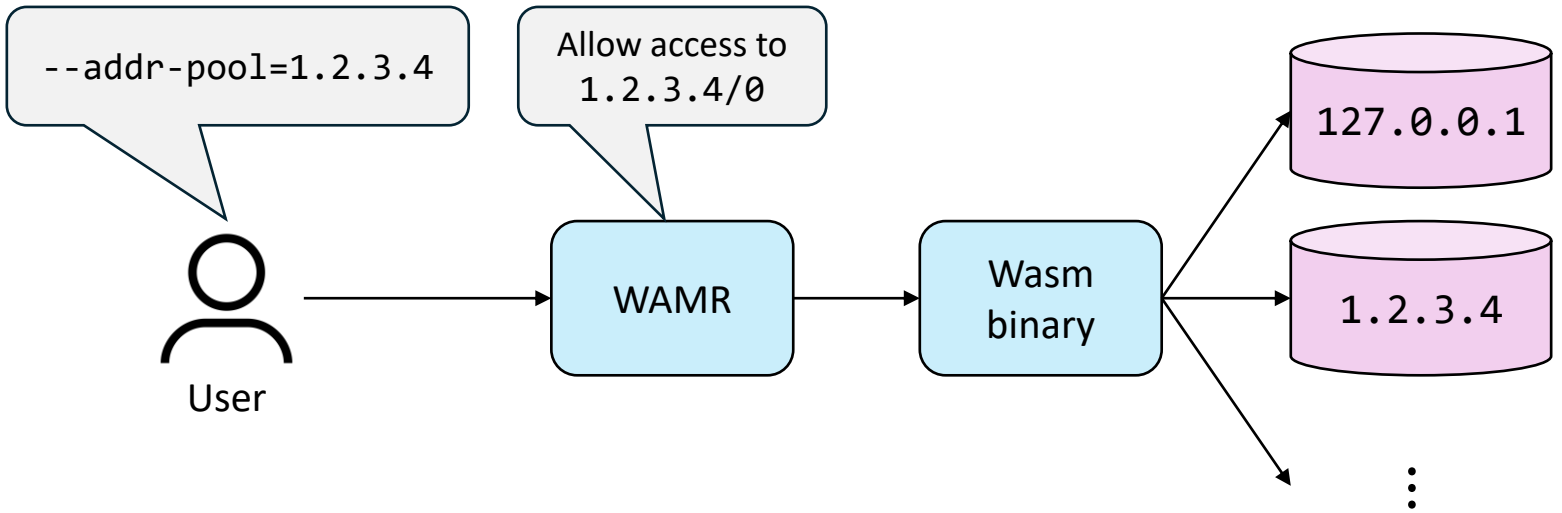
WaCFuzz 개요

- Oracle
  - 로그 분석, 권한 우회 탐지



네트워크 권한 구성 오류

- WAMR의 '`--addr-pool`' 옵션은 CIDR 형태의 입력을 받음
- 마스크 없이 주소만 입력되는 경우 '`/0`'으로 처리됨



심볼릭 링크 권한 부여 혼선

- ‘`--dir`’ 옵션으로 심볼릭 링크에 권한 부여 가능 (Wasmtime, WAMR)
- 사용자 입장에서 실제 권한이 어디에 적용되는지 알기 어려움

- 개선 방안
  - 해석된 실제 경로를 사용자에게 명확히 알려주거나 허용 여부를 확인
  - 사용자가 의도치 않은 권한 부여 방지

결론

- WASI 런타임 간 옵션 및 권한 구현상의 차이 확인
- WaCFuzz로 실제 취약점, 버그 발견 및 제보
- WASI 명세 및 입력 검증 강화 필요
- 향후, 더 넓은 API·복합 환경 기반 취약점 탐지로 확장

감사합니다