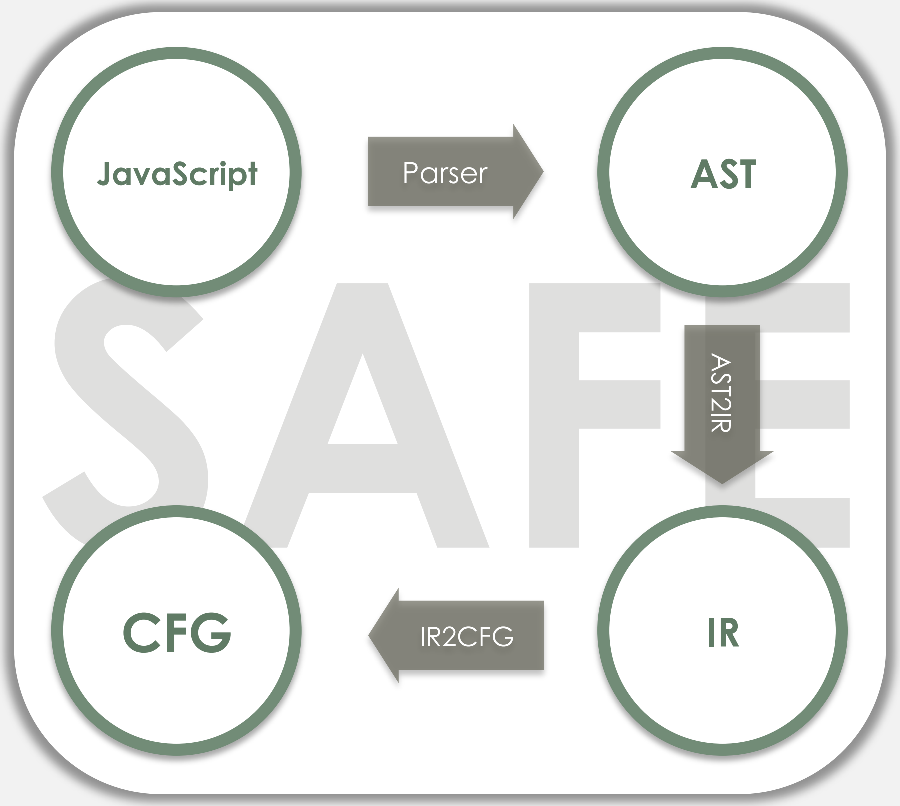
# Bug Detector

## Based on SAFE Analyzer

| | |
|---|---|
| when | 2013. 02. 01 |
| who | **Junho Jin** |
| from | PLRG @ **KAIST** |
| at | **ERC** Workshop |

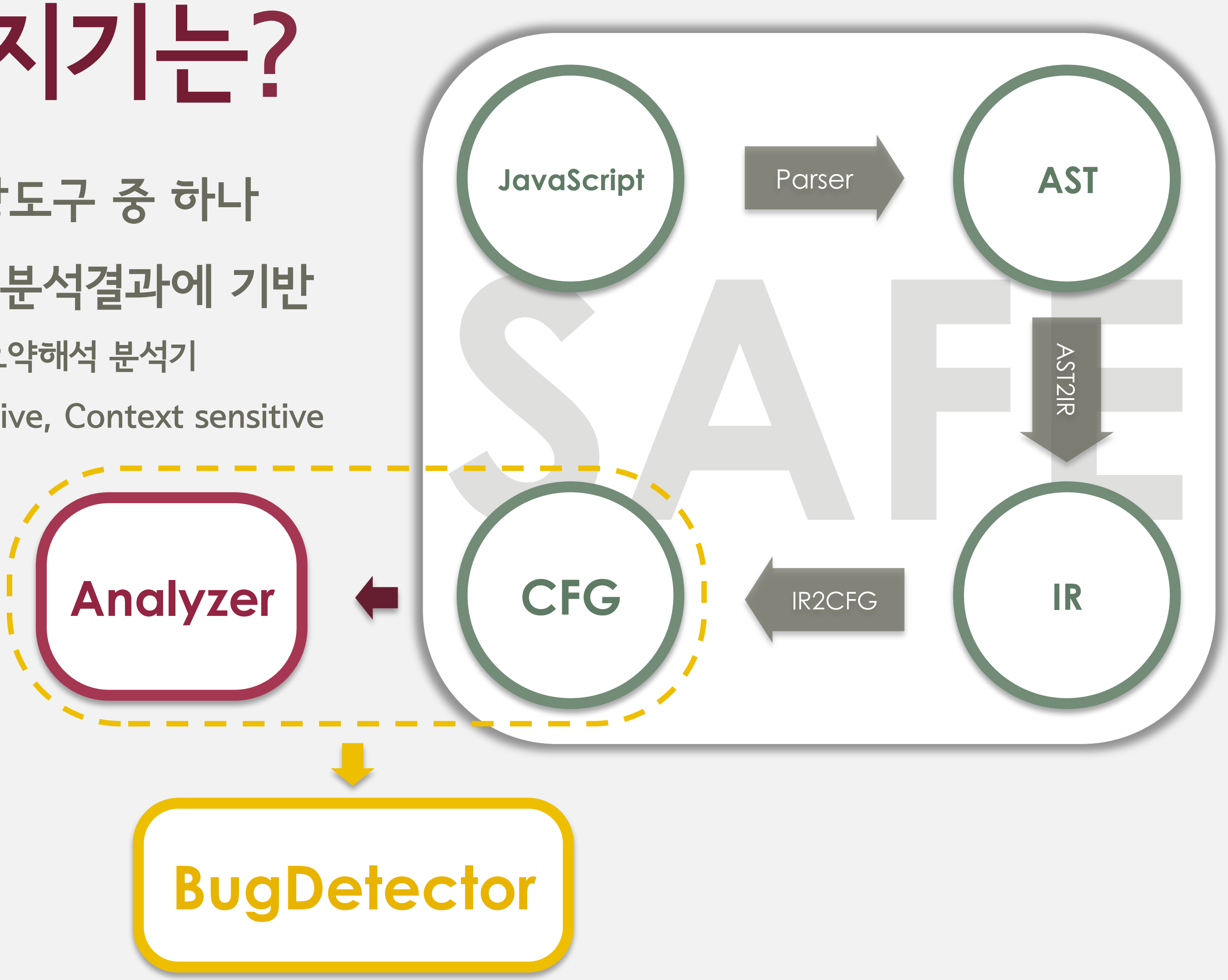
# 버그감지기는?

- SAFE의 확장도구 중 하나
- Analyzer의 분석결과에 기반



# 버그감지기는?

- SAFE의 확장도구 중 하나
- Analyzer의 분석결과에 기반
  - CFG 기반 요약해석 분석기
  - Flow sensitive, Context sensitive



# 어떤 버그?

Error

프로그램의 비정상 종료

&

Warning

정상종료 하지만
예기치 못한 일을 발생시킬 수 있음

# 프로그램의 비정상 종료

## Type Error

| | |
|---|---|
| AbsentVariableRead | Absent인 변수를 읽을 때 |
| BuiltinArgumentSize | Builtin 함수의 인자 수가 잘못되었을 때 |
| BuiltinWrongType | Builtin 함수의 인자 타입이 틀렸을 때 |
| CallNonFunction | Function이 아닌 것을 call 했을 때 |
| NullOrUndefined | Null 또는 Undefined 인 객체의 속성에 접근할 때 |

# Warning

**정상종료 하지만**
**예기치 못한 일을 발생시킬 수 있음**

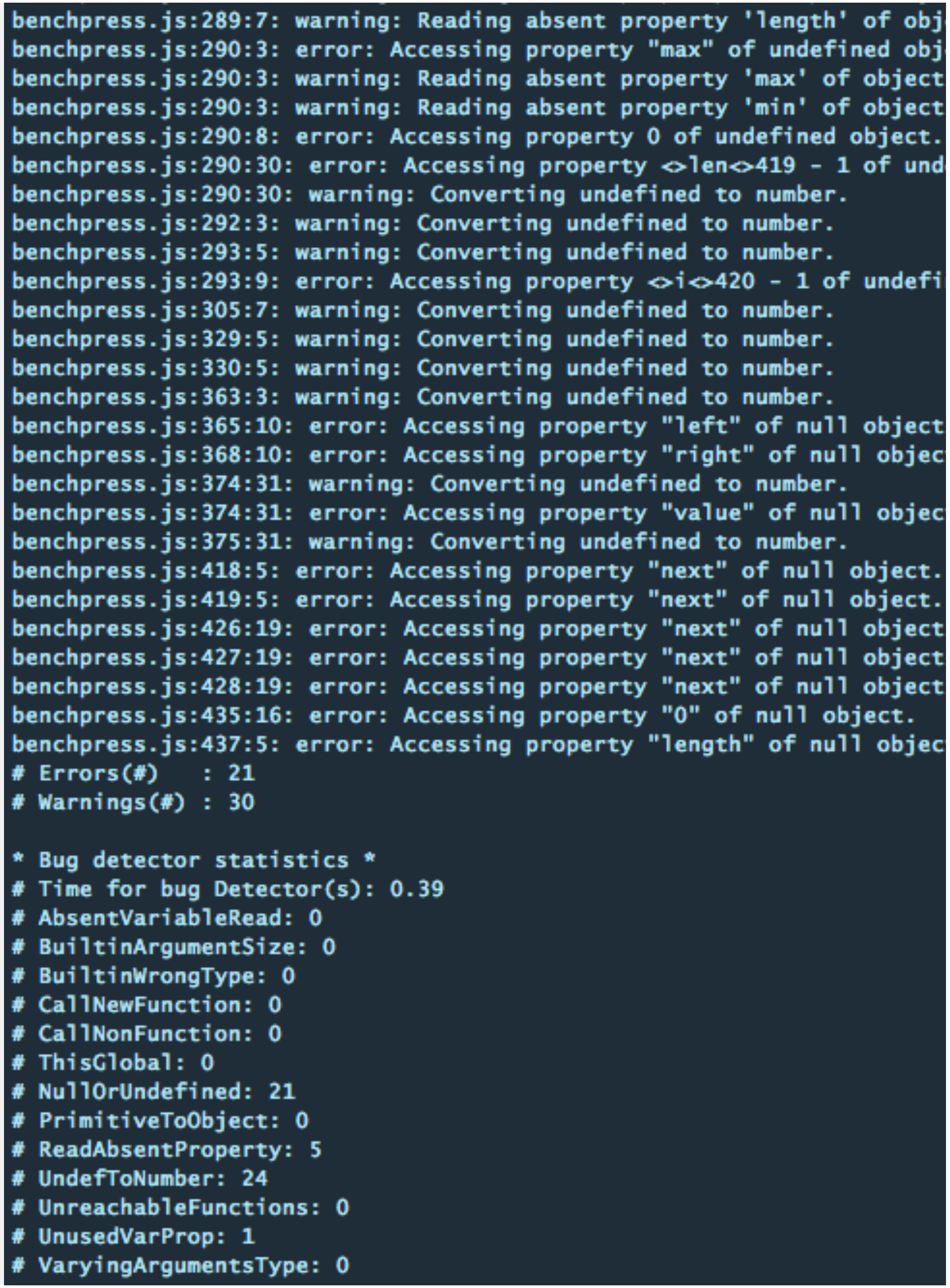
| | |
|---|---|
| CallNewFunction | 함수가 Constructor와 함수로써 모두 사용될 때 |
| GlobalThis | This 값이 global 객체를 가져올 때 (보안취약) |
| PrimitiveToObject | primitive type을 object로 변환하려 할 때 |
| ReadAbsentProperty | 읽어들인 프로퍼티가 absent 일 때 |
| UndefToNumber | Undefined를 number로 변환하려 할 때 (NaN 발생) |
| UnreachableFunctions | 함수가 함수콜 또는 constructor로써 사용되지 않을 때 |
| … | … |

# Testing

V8, SunSpider benchmark

False alarms found !

Soundness vs true alarms



```
benchpress.js:289:7: warning: Reading absent property 'length' of obj
benchpress.js:290:3: error: Accessing property "max" of undefined obj
benchpress.js:290:3: warning: Reading absent property 'max' of object
benchpress.js:290:3: warning: Reading absent property 'min' of object
benchpress.js:290:8: error: Accessing property 0 of undefined object.
benchpress.js:290:30: error: Accessing property <>len<>419 - 1 of und
benchpress.js:290:30: warning: Converting undefined to number.
benchpress.js:292:3: warning: Converting undefined to number.
benchpress.js:293:5: warning: Converting undefined to number.
benchpress.js:293:9: error: Accessing property <>i<>420 - 1 of undefi
benchpress.js:305:7: warning: Converting undefined to number.
benchpress.js:329:5: warning: Converting undefined to number.
benchpress.js:330:5: warning: Converting undefined to number.
benchpress.js:363:3: warning: Converting undefined to number.
benchpress.js:365:10: error: Accessing property "left" of null object
benchpress.js:368:10: error: Accessing property "right" of null objec
benchpress.js:374:31: warning: Converting undefined to number.
benchpress.js:374:31: error: Accessing property "value" of null objec
benchpress.js:375:31: warning: Converting undefined to number.
benchpress.js:418:5: error: Accessing property "next" of null object.
benchpress.js:419:5: error: Accessing property "next" of null object.
benchpress.js:426:19: error: Accessing property "next" of null object
benchpress.js:427:19: error: Accessing property "next" of null object
benchpress.js:428:19: error: Accessing property "next" of null object
benchpress.js:435:16: error: Accessing property "0" of null object.
benchpress.js:437:5: error: Accessing property "length" of null objec
# Errors(#)   : 21
# Warnings(#) : 30

* Bug detector statistics *
# Time for bug Detector(s): 0.39
# AbsentVariableRead: 0
# BuiltinArgumentSize: 0
# BuiltinWrongType: 0
# CallNewFunction: 0
# CallNonFunction: 0
# ThisGlobal: 0
# NullOrUndefined: 21
# PrimitiveToObject: 0
# ReadAbsentProperty: 5
# UndefToNumber: 24
# UnreachableFunctions: 0
# UnusedVarProp: 1
# VaryingArgumentsType: 0
```

# 앞으로는?

Error

BinaryOperator
throwTypeErrorConstructor
throwTypeErrorIfWrongKindofThis
builtinObjectTypeConversion
…

& Warning

alwaysTrueConditionalBranch
UnreachableCode
newUsedVariable
shadowingFunOrParam
…

1 더 많은 버그를 잡자!

2 정확하게 버그를 잡자!

False alarm 제거

3 빠르게 버그를 잡자!

dense 분석 → sparse 분석

# 감사합니다

질문 있으신가요?

끝