PLRG
Programming Language Research Group

실제 자바스크립트 웹 어플리케이션에서 정적으로 결함을 검출하는 프레임워크

박 창 희

공동 연구 : 원순철, 진준호, 류석영 교수님, 최재준(S-Core)

카이스트 프로그래밍 언어 연구실

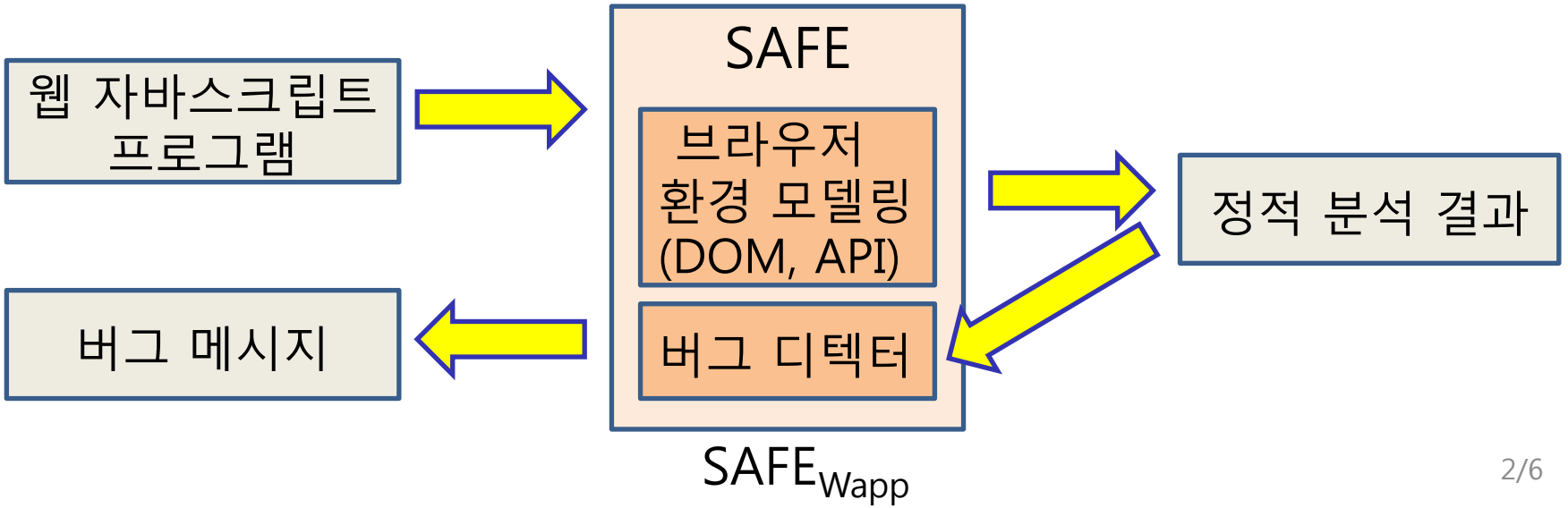
2014년 1월 14일

큰 그림

PLRG
Programming Language Research Group

- SAFE : 오픈 소스 자바스크립트 정적 분석기

- $SAFE_{Wapp}$: SAFE 확장



$SAFE_{Wapp}$ 프레임워크 특징 (1/2)

PLRG
Programming Language Research Group

- 브라우저 환경 모델링
  - 기존 연구들: W3C DOM 문서 모델링
    - 방대하지만 완전하지 않음 (incomplete)
    - 브라우저의 비 표준(non-standard) API들은 모델링 할 수 없음
  - $SAFE_{Wapp}$: 실제로 많이 쓰이는 오브젝트나 API 모델링
    - 가장 방문자 수가 많은 9,465개 웹사이트에 존재하는 자바스크립트 코드 조사

종 류	1개 이상 사이트에서 발견	10개 이상 사이트에서 발견	100개 이상 사이트에서 발견	1,000개 이상 사이트에서 발견
Field	1,721	951	327	150
API	267	160	98	50
합 계	1,988	1,111	425	200

모델링 완료

$SAFE_{Wapp}$ 프레임워크 특징 (2/2)

PLRG
Programming Language Research Group

- 버그 탐지 능력
  - ➢ 기존 연구 TAJS
    - 버그에 대한 명확한 정의 부재
    - 13개 버그 탐지
  - ➢ $SAFE_{Wapp}$
    - 버그 정의 : ECMAScript 스펙에 정의된 run-time exception을 일으키는 프로그램 에러
    - ECMAScript 스펙에 정의된 모든 **155개** 에러를 찾아내고 그 중 **129개**의 에러를 검출할 수 있는 첫 번째 프레임워크

	Range Error	Reference Error	SyntaxError	TypeError	URIError	합 계
ECMAScript	7	31	31	98	12	155
버그디텍터	7	31	31	72	12	129
탐지율	100%	100%	100%	73.4%	100%	83.2%

실제 웹사이트에서 버그 탐지

PLRG
Programming Language Research Group

- 4개 웹사이트의 메인 웹 페이지에서 버그 탐지 결과

website	LOC	Time (sec)	CallNon Function	Absent Read	Conditional Branch	Function ArgSize	Shadowing	Primitive ToObject	Total
wikipedia.org	177	32.88	0	4	9	1	0	0	14(W)
odnoklassniki.ru	226	22.94	0	1	12	3	1	0	17(W)
soso.com	2413	27.52	0	9	20	18	2	1	50(W)
directrev.com	4549	42.03	1	4	37	7	36	0	1(E)/84(W)

DirectRev

```
$('ul.accordion').accordion( ... );
```

jQuery user interface

jQuery UI 라이브러리 import 하지 않음
⇒ CallNonFunction 에러

결 론

PLRG
Programming Language Research Group

- $SAFE_{Wapp}$: 자바스크립트 웹 어플리케이션의 정적 버그 탐지를 지원하는 오픈 소스 프레임워크
  - ➢ 9,465개 웹사이트 대상으로 한 실험 자료에 근거한 브라우저 환경 모델링
  - ➢ ECMAScript에 기술된 모든 155개 에러 중 129개의 에러 탐지 가능
- 15일 포스터 발표

A Framework for Static Bug Detection in JavaScript Web Applications in the Wild