실제 개발 환경에 적용해 본 concolic testing

발표자: 김윤호
Provable Software Lab, KAIST

세 줄 요약

- 2명(교수1, 대학원생1) 이 약 **0.5MM** 동안
- **Concolic testing** 기법을 적용해서
- S사의 **모바일 소프트웨어 버그 여러 개**를 찾을 수 있었다.

세 줄 요약

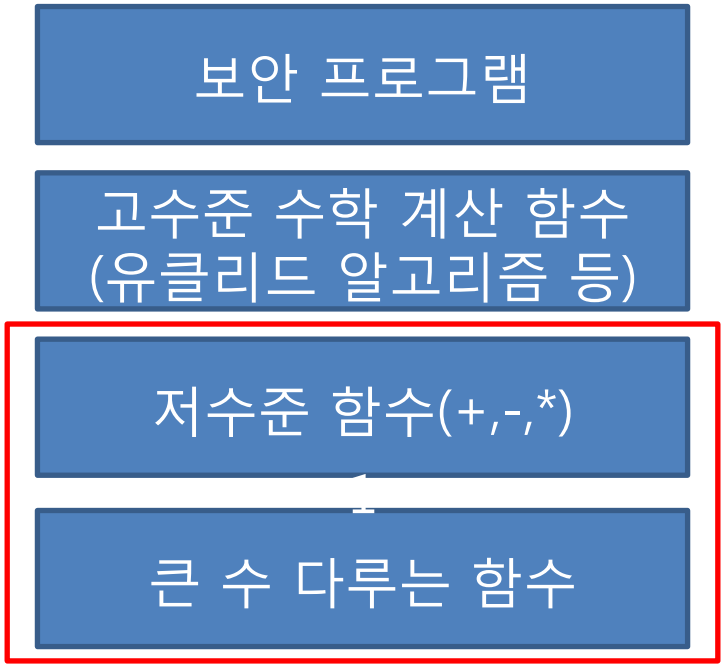
- 2명(교수1, 대학원생1) 이 약 **0.5MM** 동안

Concoclic testing
꽤 쓸 만 하다!

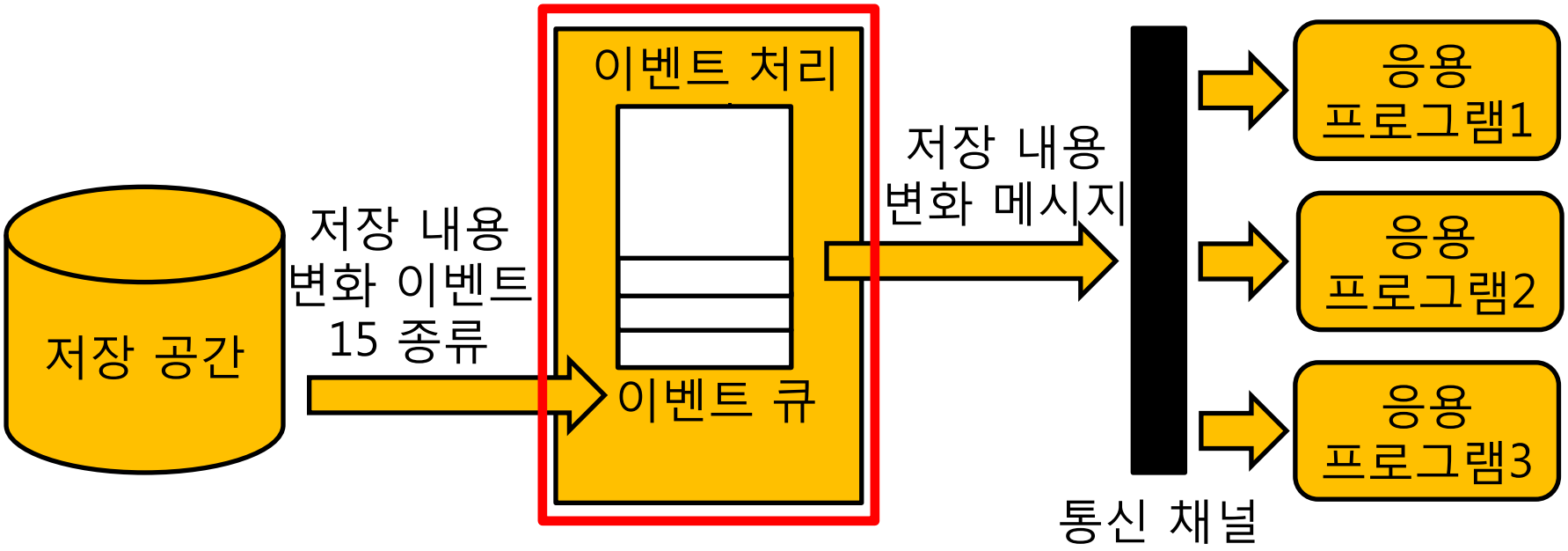
찾을 수 있었다.

적용 대상 – 보안 프로그램 A

- 복잡한 보안 프로그램
  - 약 2,000 줄의 C 프로그램
- 잘 나눠진 계층 구조
- 고수준의 정확도가 요구되는 핵심 프로그램
- 기본적인 수학적 관계 명세
  - (a+b) mod m == (b+a) mod m
- 결과를 저장할 큰 수 객체의 **메모리 침범 오류** 발견



적용 대상 – 이벤트 처리 프로그램 B



- 저장 공간 변화에서 생기는 이벤트 처리기
  - 약 23,000 줄의 C 코드

- **무한 루프 버그** 를 유발하는 이벤트 발견
  - 발생 빈도: “글쎄요.. 이게 필요하긴 한데.. 본적은 잘..”

배운 점

- Concolic testing 의 효과를 극대화하려면
  - **명확한 요구사항 명세**가 있어야 하고
  - 검사 대상 **프로그램에 대한 깊은 이해**가 있어야 하며
  - 검사 대상 프로그램이 **모듈 구조**로 잘 짜여 있어야 한다

- 아주 기본적인 명세도 쓸만하다.
  - '(a+b) mod m 랑 (b+a) mod m 는 항상 같아야 한다' 같은 기본적인 명세로 메모리 침범 오류 발견

- 널리 적용하려면 배포하기 좋은 도구가 필수적이다