한양대학교 컴퓨터공학과

Programming Language bAsed Software Security and Engineering

PLASSE RESEARCH

테스트 코드 돌연변이를 이용하여 정적분석도구 허위경보 줄이기

프로그래밍언어연구실 박현우, 도경구

RESAEC center 12th
Research On Software Analysis for Error-free Computing
소프트웨어 무결점 연구센터 NRF ERC

정적분석도구의 허위경보

오탐 : 소스코드가 보안에 취약하지 않아도 취약점을 탐지하는 현상
미탐 : 소스코드가 보안에 취약해도 취약점을 탐지하지 못하는 현상

1. [연구내용 및 방법]

정적분석도구 구현 방법

분석 알고리즘 → 분석도구 구현 → 분석도구 테스트 → 분석 결과

테스트 코드의 종류와 문제점

테스트 코드 종류	문제점
오픈소스 / MITRE / CERT / CWE / CVE	오직 제공되는 예제 코드의 취약점만 분석
분석도구 개발자 작성	분석 알고리즘에 종속적이고 단순

CERT가 제공하는 예제코드의 문제점

FLP30-C. Do not use floating-point variables as loop counters

```
for (float x = 0.1; x <= 1.0; x += 0.1 ){

     /* Loop may iterate 9 or 10 times */
}

 for (int count =1; count <= 10; count +=1 ){

     /* Loop iterates exactly 10 times */
}
```

뮤테이션 테스팅

목적 - 작성된 테스트 케이스 품질 평가와 향상
- 소스코드를 변형시켜 특정 오류 지점 검출

프로그램 테스트 → 돌연변이 생성 → 돌연변이 테스트 → 돌연변이 생존 여부 → 테스트 케이스 추가

돌연변이 생성 예제

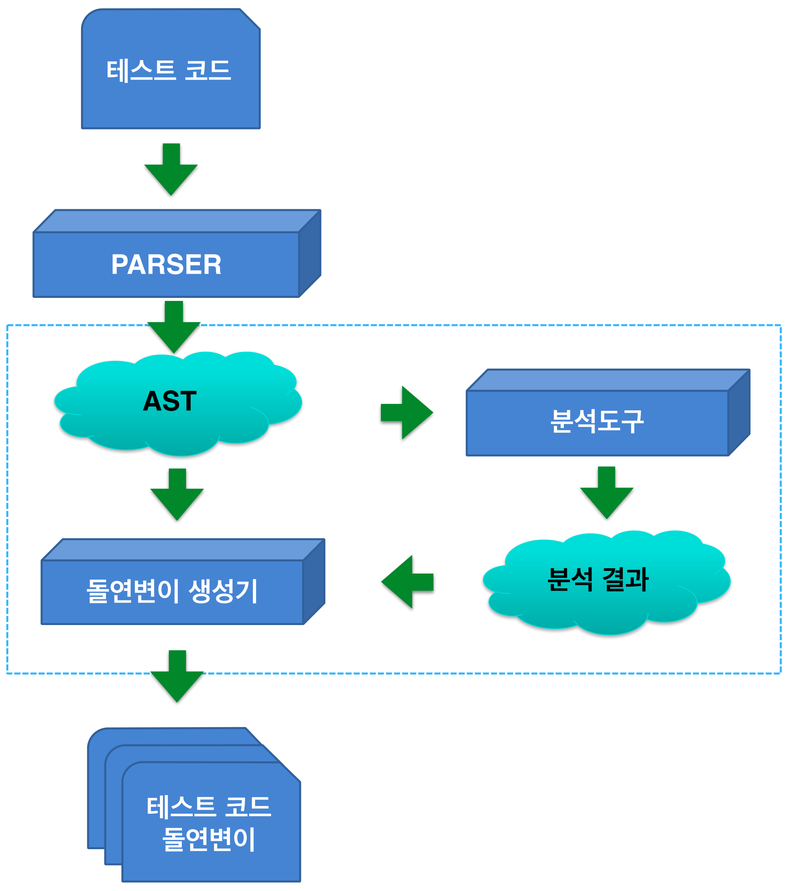
```
public String getSomething(int someParameter) {
    if (someParameter > 0) {
      return "foo";
    } else {
      return "bar";
    }
}
```

```
public String getSomething(int someParameter)
{
    if (someParameter < 0) {
      return "foo";
    } else {
      return "bar";
    }
}
```

뮤턴트 생성기법 종류

Operator	Description
ABS	Absolute value insertion
AOR	Arithmetic operator replacement
LOR	Logical operator replacement
ROR	Relational operator replacement
UOI	Unary operator insertion
UOD	Unary operator deletion
COR	Conditional operator replacement
SOR	Shift operator replacement
ASR	Assignment operator replacement
SVR	Scala variable replacement

테스트 코드 돌연변이 생성 방법



2. [기대효과]

- 분석결과를 이용하여 적합하고 다양한 테스트 코드 자동 생성
- 정적분석도구 분석 능력 향상
- 정적분석도구 개발단계에서 미탐과 오탐을 줄여 시간과 노력 비용 감소

테스트 코드 돌연변이 생성 예제

```
for (float x = 0.1; x <= 1.0; x += 0.1 ){

     /* Loop may iterate 9 or 10 times */
}
```

기존 테스트 코드

```
for (float x = 0.1; x <= 1.0; x += 0.1 ){

     /* Loop may iterate 9 or 10 times */
}

for (double x = 0.1; x <= 1.0; x += 0.1 ){

     /* Loop may iterate 9 or 10 times */
}

for (int x = 0.1; x <= 1.0; x += 0.1 ){

     /* Loop may iterate 9 or 10 times */
}
. . . . . .
```

테스트 코드 돌연변이