자동테스팅 도구 SymCC의 성능과 사용성 개선

2023년 가을학기
캡스톤 축제
[캡스톤 디자인1]

참여기업: V+Lab
지도교수님: 홍 신 교수님
팀원: 함상훈, 한나린, 이진주, 하정원

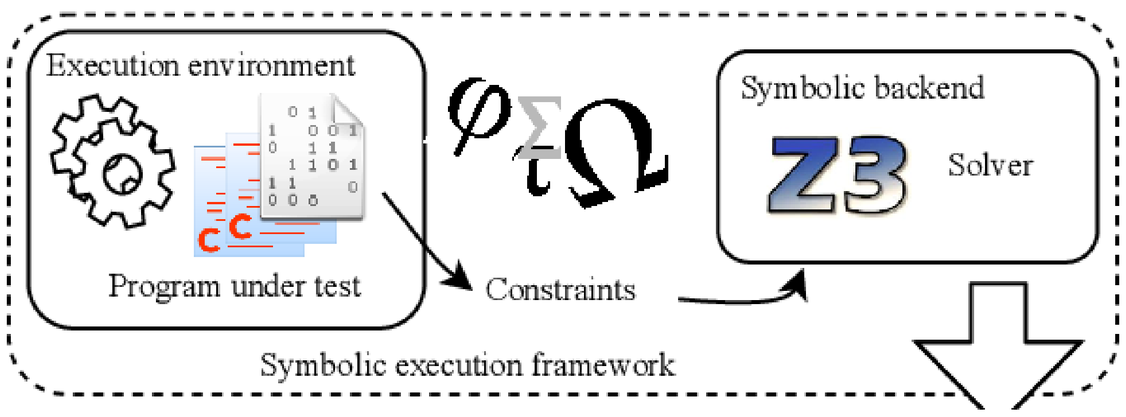
I. 문제 배경

1. 연구 배경

SymCC는 동적 심볼릭 실행을 통해 프로그램을 대상으로 테스트 입력을 자동으로 생성하는 Whitebox Testing 도구로 C, C++, Rust, Object-C 등 다양한 시스템 프로그램에 적용이 가능한 오픈소스 테스팅 엔진이다.

2. 과제의 필요성

SMT 기반 분석을 통해 랜덤 테스팅으로 도달이 어려운 복잡한 실행 경로에 대한 테스트 생성이 가능하고, 기존 동적 심볼릭 테스팅 도구가 최근 C 코드 지원이 어려운 것과 달리, SymCC는 LLVM 프레임워크 기반으로 다양한 C 계열 프로그램에 적용이 가능하다.



II. 문제 정의

Problem Statement

SymCC의 탐색 휴리스틱과 사용자 인터페이스를 개선함으로써 실제 C/C++ 프로그램 테스팅에서 활용성을 개선하고자 한다.

Constraints

- Concolic Testing 알고리즘의 명시적인 개선이 이루어져야 한다.
- SymCC 실행 과정을 모니터링하고 성능 Bottleneck을 식별할 수 있는 새로운 UI 디자인을 제공해야 한다.
- Testing의 결과는 사용자에게 직관적으로 보여져져야 한다.

Objectives

- 기존의 동적 심볼릭 테스팅 연구에서 제안된 다양한 탐색 휴리스틱을 SymCC 기반으로 구현하여 SymCC의 성능을 향상한다.
- SymCC의 다양한 파라미터를 쉽게 튜팅할 수 있는 인터페이스, SymCC 성능 문제가 발생하는 코드 영역을 비쥬얼하게 파악할 수 있는 인터페이스, SymCC를 위한 테스트 드라이버를 쉽게 작성할 수 있는 인터페이스 등 사용성을 개선한다.

III. 배경 연구

1. System Programming

- C언어를 통해 Fuzzing 학습 전 선행되어야 할 기초적인 System Programming 지식에 대해 복습했다.
- File I/O, Socket Programming, Multi-Process, Multi-Thread 등의 분야를 집중 학습했다.

2. Introduction to Software Testing

- Software Testing은 SW 개발 과정에서 중요한 단계로, 현재 많은 부분이 자동화되어 있는 상태이다. Software Quality가 낮을 경우 발생할 수 있는 사회적/경제적 손실을 Testing을 통해 방지할 수 있다는 점에서 Testing의 중요성을 확인할 수 있다.
- Program Fault의 종류와 Fault to Failure의 필요충분 조건인 Execution-Infection-Propagation(PIE)를 적용/분석했다.

3. Structural Coverage Measurement

- Gcov는 GCC Tool의 일종으로, 이를 통해 프로그램의 Line coverage와 Branch coverage를 측정할 수 있다.
- Clang의 Source-based coverage는 Compiler의 Front-end level에서 coverage를 구하는 Tool이다.

IV. 접근 방법 및 초기 결과

Key Approach

Symbolic Execution 기술에 대한 스터디, SymCC 프레임워크 분석, SymCC 인터페이스 개선을 차례대로 진행한다.

System Design (conceptually)

1. Symbolic Execution 기술에 대한 스터디
   - 소프트웨어 테스팅 개념과 동적 분석 기술 스터디
   - 동적 분석을 위한 LLVM 프레임워크 스터디
   - Dynamic Symbolic Execution 기술 스터디
2. SymCC 프레임워크 분석
   - 코드 Instrumentation 분석
   - 현재 탐색 알고리즘 성능 평가
   - 새운 탐 알고리즘 구현
3. SymCC 인터페이스 개선
   - SymCC 테스팅 과정 리포트 기능 개발
   - SymCC 성능 문제 프로파일링 기능 개발
   - 테스트 드라이버 작성 인터페이스 개발
   - 사용성 평가