학부생 연구기회 프로그램 (UROP) 공고

◆ 담당교수 : 전병곤	◆ 연구실명 : 소프트웨어 플랫폼 연구실
◆ UROP 연구 과제명 : 퍼즈 테스팅으로 이더리움(Ethereum) 버그 찾기	
◆ 모집대상 : 이더리움과 테스팅에 관심이 많은 학생	
◆ 모집기간 : ~ 2020년 6월 말	

연구 배경

- 이더리움 블록체인의 불역성(Immutability)를 유지하기 위해서는, 모든 이더리움 클라이언트들 코드는 항상 합의를 해야 한다
- 새로운 이더리움 기능을 구현하는 과정에서, 두 가지 이더리움 클라이언트 Parity(Rust)와 geth(Go)가 구현상 버그로 인하여 특정 트랜젝션이 발생하였을 때 합의를 하지 못하는 문제들이 발생하였다
- 예를 들어서, 2016년 11월 EIP-161 (Ethereum Improvement Proposal) 구현 과정에서 Parity와 geth 사이에 network split이 발생하였고, split 이후 geth에서 이루어진 트렌젝션들이 무효화 되는 문제가 발생하였다

연구 내용

- 이더리움 합의 버그를 퍼즈 테스팅으로 찾아서, 버그 발생을 방지한다
- Parity와 geth를 연동하여 개발한 libfuzzer를 개선한다 (해당 libfuzzer 는 parity/geth에 동일한 트랜젝션을 실행한 뒤, 결과값을 비교한다)
  - Exec/s 향상: 합의와 관련없는 코드를 제거한다
  - Coverage 향상: libfuzzer의 알고리즘을 개선한다 (EIP 스펙 활용 등)
- 퍼즈 테스팅을 통해 버그를 찾는 속도가 개선되었는지 확인하고, 기존에 알려지지 않은 새로운 버그를 찾을 수 있는지 확인한다

사전 지식 및 요건

- Linux 사용 경험, Rust 또는 Go 코드를 읽고 작성할 수 있어야 함
- 블록체인과 이더리움에 대한 기초 지식
- [선택] 이더리움 클라이언트(스마트 컨트랙트 등) 사용 경험
- [선택] AFL/libFuzzer 등 퍼즈 테스팅 프레임워크 사용 경험

서울대학교 컴퓨터공학부
Seoul National University
Dept. of Computer Science and Engineering

소프트웨어 플랫폼 연구실
Seoul National University
Software Platform Lab

문의 양영석(johnyangk@gmail.com)