Slither: A Static Analysis Framework For Smart Contracts

"EthCC 2019"

이수연

목차

1. introduce
2. realted works
3. Slither
4. SlithIR
5. evaluation and comparison to state of the art tools
6. conclusions and future work

introduction

➡이상적으로는 Etherum 스마트 계약을 위한 정적 분석 프레임워크는 다음과 같은 특성을 가져야 함

correct level of abstraction

- 프레임워크가 너무 추상적 – common usage pattern을 포착하는 정확한 semantics를 도입하기 어려움
- 프레임워크가 특정 이슈의 검출에만 초점을 맞추면 새로운 검출기나 분석을 추가하기 어려움

robustness

- 실제 코드를 crash 없이 구문 분석해야 함

performance

- 대규모 계약에서도 분석이 빠르고, IDE와 같은 개발 도구에 쉽게 합쳐질 수 있어야함

1. introduction

accuracy

- 낮은 false positive rate을 유지하면서 대부분의 잠재적 문제를 찾아내야 함

- false positive 수가 매우 많을 경우, 결과를 무시하고 직접 검사해야 할 수도 있음

batteries included

- 유용한 일반적인 분석들과 검출기들이 포함되어야 함

1. introduction

Slither

- 오픈소스 정적 분석 프레임워크
- solidity 코드에 대한 정적 분석을 쉽게 하도록 설계된 자체 중간 언어인 SlithIR을 사용
- 정보를 추출하고 구체화하기 위해 dataflow 및 taint tracking과 같은 널리 사용되는 프로그램 분석 기법을 적용
- 보안 중심의 프레임워크지만 스마트 계약에 대한 사용자의 이해도를 높이고 코드 리뷰를 지원하며 누락된 최적화를 탐지하는 데도 사용
- 모두 오픈 소스여서 다른 사람들이 결과를 검증하고 개선 가능

기여
- Slither, 즉 Solidity 계약 정적 분석을 위한 프레임워크를 제시
- Slither의 중간 표현 및 분석기 설계를 자세히 설명
- 대규모 contract 환경에서 performance, robustness, accuracy을 평가하고 비교

1) Securify

- SRI Systems Lab(ETH Zurich)에서 개발
- 오픈소스
- Java와 stratified Datalog를 사용하여 구현
- 바이트코드 수준에서 작동
  - EVM 바이트코드를 파싱하고 분해
  - 정적 분석을 사용하여 결과 코드를 semantic facts로 변환
  - common issue 를 탐지하기 위해 미리 정의된 패턴 목록과 fact를 일치시킴

2) SmartCheck

- SmartDec에서 개발한 정적 분석 툴
- solidity 소스 코드에서 XML 기반 IR로 직접 변환하여 작동
- IR과 XPath 패턴과 비교하여 potential security, functional, operational, development issue를 식별한다.

3) Solhint

- ProtoFire에서 개발한 solidity 코드 linting을 위한 도구
- 보안과 style guide 검증을 모두 제공하는 것이 목표
- 오픈소스이며 NodeJS 와 Solidity parser로 구현
- 다른 주목할 만한 static analysis framework로는 Vandal 과 EtherTrust가 있음

4)GASPER & GasReduce

- 정적 분석을 사용하여 contract에서 잠재적 최적화를 탐지
  - GASPER : high level 단계 (예: 데드 코드)
  - GasReduce : 바이트코드 instruction pattern수준

- 둘 다 dead code와 loop 최적화에 초점

- Slither의 최적화 패턴과는 좀 다른 접근방법

Dynamic analysis

symbolic execution, taint tracking 및 fuzzing을 활용하여 취약점을 발견

Oyente
- Ethereum 스마트 계약에서 보안 문제를 분석하고 탐지하기 위한 최초의 툴 중 하나
- 멜론포트가 개발
- 코드는 오픈소스임

Manticore
- Ethereum 스마트 계약 및 바이너리 분석을 위한 오픈소스 symbolic execution 도구
- Bits의 Trail of Bits 가 개발

Echidna
- Bits의 Trail of Bits 가 개발
- Ethereum 스마트 계약을 fuzzing하기 위한 property-based 테스트 툴

2. 관련 연구 – Dynamic Analysis

Mythril Classic

- ConsenSys가 만든 Ethereum 스마트 계약을 위한 오픈 소스 보안 분석 툴

- 다양한 보안 취약점을 탐지하기 위해 concolic 분석, taint 분석, control flow checking을 사용

TeEther

- Krupp과 Rossow가 제작

- Ethereum 스마트 계약의 특정 유형의 취약점에 대한 자동 exploit 생성 도구

- 소스 코드는 이 글을 쓸 당시에는 제공되지 않았지만, 저자들은 Usenix 2018에서 발표 90일 만에 오픈 소스 도구를 만들겠다고 했음