김영웅 박재선

지도교수 오희국

Symbolic execution을 활용한

다중 스마트컨트랙트 간 취약점 탐지 도구 디벨롭

개요

목표

* 활동 내역을 없애고 개요랑 목표를   
  다른 박스로 만들어서  
  취약점 탐지 절차를 더 크게 만드는 방법도 있음.

프로젝트 설명

Html5 ?

python

Solidity

Flask

Etherscan

mythril

Blockchain tracer

개발 언어 및 환경

스마트 컨트랙트 배포 전 취약점 탐지 도구를 이용하면 해킹 사례 예방 가능.

기대 효과

취약점 탐지 절차

개발 진행 그래프

타임라인

간트차트

활동 내역

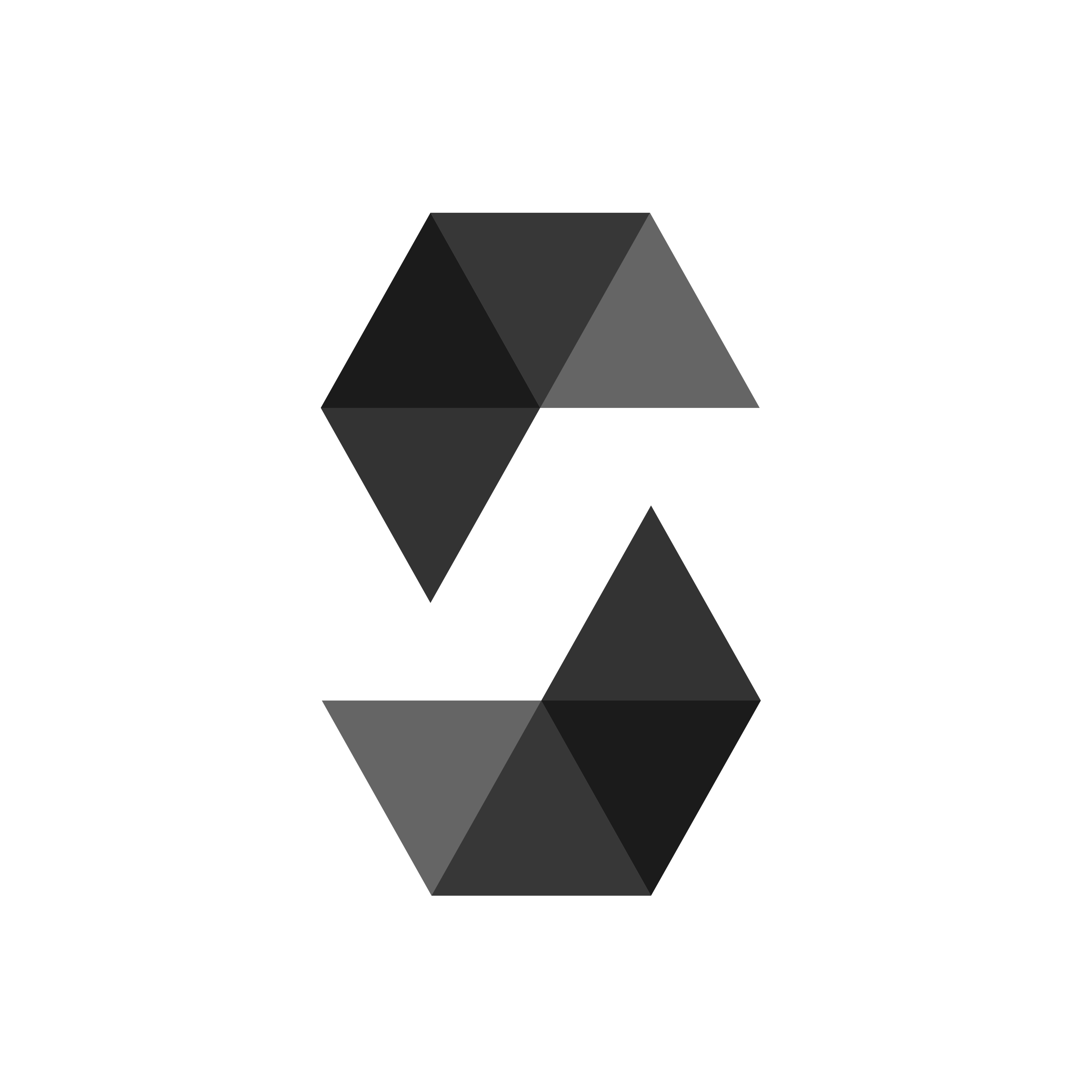
가상의 ethereum 환경을 만들어서

실제 트랜잭션이 동작하는 대로 global state 변화.

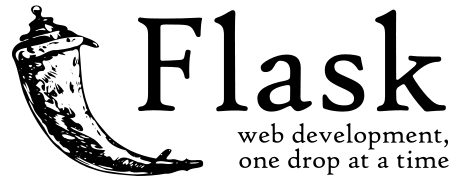
이 과정에서 취약점이 탐지될 수 있는 포인트 검출.

아무래도 정확도나 여러 케이스에서 탐지가 가능한 것을  
보여주는 게 효과적일 것 같긴한데 그러면 이 섹션을 두 파트로  
나누어서 한쪽은 취약점 탐지 절차. 한쪽은 실험결과 쪽으로.

왼쪽 한계, 개선점 오른쪽 취약점 탐지 절차.

로고이(가) 표시된 사진

자동 생성된 설명로고이(가) 표시된 사진

자동 생성된 설명로고이(가) 표시된 사진

자동 생성된 설명

향상된 스마트 컨트랙트 취약성 탐지

Mythril을 개선하면 스마트 계약의 취약성을 보다 정확하게 탐지하여 잠재적인 보안 위협을 식별하는 데 있어 도구의 효과를 높일 수 있습니다. 향상된 기능을 통해 특정 취약성을 더 잘 탐지하거나 Mythril의 출력에서 잘못된 긍정을 줄이는 방법을 시연할 수 있습니다.

사용 편의성 향상

향상된 기능으로 Mythril이 사용자에게 더욱 친숙해진 경우, 이 기능이 전반적인 사용자 환경을 어떻게 개선했는지 보여줄 수 있습니다. 향상된 기능을 통해 도구를 설정 및 실행하고, 출력을 해석하거나, 추가 정보 또는 리소스에 액세스하는 것이 얼마나 쉬워졌는지를 보여줄 수 있습니다.

Ethereum network의 광범위한 영향.

구체적인 개선 사항에 따라 프로젝트가 스마트 계약 개발 생태계에 더 광범위한 영향을 미칠 수 있습니다. 예를 들어, 특정 유형의 취약성을 식별하기 위한 새로운 기술을 개발한 경우 업계 전체의 보안 관행이 개선될 수 있습니다. 개선사항이 가져올 수 있는 잠재적인 광범위한 영향을 보여줄 수 있습니다.

개발 언어 및 환경

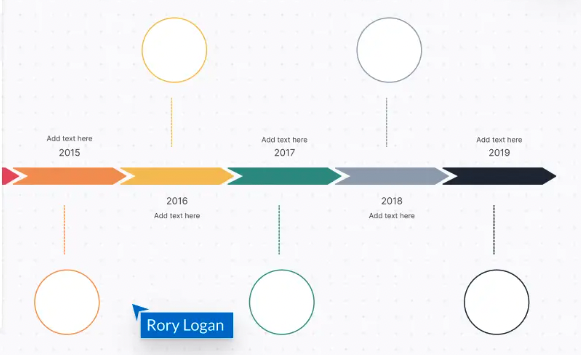
지도교수 오희국

Symbolic execution을 활용한

다중 스마트컨트랙트 간 취약점 탐지 도구 디벨롭

활동 내역

<https://app.creately.com/d/nJaK5vWTpI5/edit>



취약점 탐지 절차

.

기대 효과

프로젝트 설명

**개요**

블록체인의 안전성은 충분히 검증되었지만 스마트 컨트랙트의 취약점이 여러 발견되고 해킹사례가 꾸준하게 발생하고 있다.   
사용자들이 신뢰할 수 있는 스마트 컨트랙트를 개발자는 개발해야한다.

**목표**

스마트 컨트랙트에 대해서 발생할 수 있는 취약점을 조사 및 분석하고 발생할 수 있는 새로운 취약점을 개발하고 발전하도록 함.

김영웅 박재선

**프로젝트 설명**

개요: QYResearch에서 21년 10월에 발표한 스마트 컨트랙트 시장 규모 현황 예측을 살펴보면, 20년의 스마트 컨트랙트 시장 규모는 2억 1,158만 달러이고 시장은 꾸준히 커져가며 27년에는 11억 5,785만 달러에 달할 것으로 예측하고 있다. 스마트 컨트랙트에서 사용하는 기술, 블록체인의 안전성은 충분히 검증되었지만 스마트 컨트랙트의 취약점이 여러 발견되고 해킹사례가 꾸준하게 발생하고 있다. 16년 The DAO 해킹, 21년 Alpha Finance Lab 해킹, 22년 Flash Loan 해킹 등 스마트 컨트랙트는 암호화폐를 직접적으로 다루는 프로그램이므로 피해자에게 직접적인 경제적인 타격을 입힌다. 따라서 사용자들이 신뢰할 수 있는 스마트 컨트랙트를 개발자는 개발해야한다.

목표: 먼저 실제 사건을 분석하여 스마트 컨트랙트의 취약점을 탐구하여 어떻게 탐지할 지 연구한 후 구조를 설계한다. 또 오픈소스 Mythril(smart contract 취약점 탐지 도구)를 기반으로 symbolic execution을 이용하여 탐지 못하는 취약점에 대해 true negative를 높이고, 27%의 취약점 탐지 정확도를 높이는 방향으로 개선한다. Mythril은 스마트 컨트랙트 개발 언어인 Solidity를 사용하므로 Solidity의 bytecode를 이해하고 이더리움 네트워크의 환경(트랜잭션, global state, environment, world state, memory등)을 학습하여 가상 환경에서 이더리움 네트워크를 구성할 수 있도록한다. 또 터미널 환경에서 스마트 컨트랙트의 취약점을 탐지하기에는 ui 요소와 접근성이 좋지 않으므로 클라이언트와 서버가 서로 통신할 수 있는, 간단한 스마트컨트랙트의 취약점과 바이트 코드의 설명이 들어 있는 웹 서비스를 만든다.

**활동내역**

Title을 먼저 구상하고, 날짜를 매칭하는 형식으로

주제선정, 솔리디티 언어 학습. Symbolic execution 학습. Concolic execution 학습. 해킹 사례 분석, mythril 구조 분석, Ethereum 네트워크 학습. Solidity bytecode 학습. 가상환경 개발. 취약점 탐지 모듈 개발. 취약점 탐지 모듈 개선. 웹 사이트 제작.

2022.11 – 주제선정, 솔리디티 언어 학습

2022.12 – 정적분석 기술 학습(symbolic, concolic, cfg)

2023.01 – Ethereum 네트워크 학습(block, transaction, smart contract, blockchain, globalstate, worldstate…)

2023.02 – 실제 사례 분석(The DAO, Flash loan)

2023.03 – mythril 구조 분석

2023.04 – 가상환경 개발, 취약점 탐지 모듈 개바

2023.05 – 취약점 탐지 모듈 개선, 웹 서비스 제작

**취약점 탐지 절차**

**기대효과**

향상된 스마트 컨트랙트 취약성 탐지

Mythril을 개선하면 스마트 계약의 취약성을 보다 정확하게 탐지하여 잠재적인 보안 위협을 식별하는 데 있어 도구의 효과를 높일 수 있습니다. 향상된 기능을 통해 특정 취약성을 더 잘 탐지하거나 Mythril의 출력에서 잘못된 긍정을 줄이는 방법을 시연할 수 있습니다.

사용 편의성 향상

향상된 기능으로 Mythril이 사용자에게 더욱 친숙해진 경우, 이 기능이 전반적인 사용자 환경을 어떻게 개선했는지 보여줄 수 있습니다. 향상된 기능을 통해 도구를 설정 및 실행하고, 출력을 해석하거나, 추가 정보 또는 리소스에 액세스하는 것이 얼마나 쉬워졌는지를 보여줄 수 있습니다.

Ethereum network의 광범위한 영향.

구체적인 개선 사항에 따라 프로젝트가 스마트 계약 개발 생태계에 더 광범위한 영향을 미칠 수 있습니다. 예를 들어, 특정 유형의 취약성을 식별하기 위한 새로운 기술을 개발한 경우 업계 전체의 보안 관행이 개선될 수 있습니다. 개선사항이 가져올 수 있는 잠재적인 광범위한 영향을 보여줄 수 있습니다.

경제적 이득.

스마트 컨트랙트 시장