블록체인 관련 보안약점 연구

A Research on Security Weaknesses Related to Blockchain

저자 (Authors)
이종모, 김태훈, 윤동준, 한경숙
Jong-Mo Lee, Tae-Hoon Kim, Dong-Jun Yoon, Kyung-Sook Han

출처 (Source)
한국컴퓨터정보학회 학술발표논문집 28(2), 2020.7, 449-450 (2 pages)
Proceedings of the Korean Society of Computer Information Conference 28(2), 2020.7, 449-450 (2 pages)

발행처 (Publisher)
한국컴퓨터정보학회
The Korean Society Of Computer And Information

URL
http://www.dbpia.co.kr/journal/articleDetail?nodeId=NODE09415072

APA Style
이종모, 김태훈, 윤동준, 한경숙 (2020). 블록체인 관련 보안약점 연구. 한국컴퓨터정보학회 학술발표논문집 , 28(2), 449-450.

블록체인 관련 보안약점 연구

이종모[O], 김태훈[*], 윤동준[*], 한경숙[*]
[*]한국산업기술대학교 컴퓨터공학부,
[*]한국산업기술대학교 컴퓨터공학부
e-mail: {zotnlnn, dkrmrm878, dbsehdwns1, khan}@kpu.ac.kr[O*]

A Research on Security Weaknesses Related to Blockchain

Jong-Mo Lee[*], Tae-Hoon Kim[*], Dong-Jun Yoon[*], Kyung-Sook Han[*]
[O]Dept. of Computer Engineering, Korea Polytechnic University,
[*]Dept. of Computer Engineering, Korea Polytechnic University

● 요 약 ●

최근 블록체인이 많은 분야에서 활용되고 있다. 본 연구에서는 블록체인과 관련된 개발 도구에 포함된 보안약점을 분석하고 그 보안약점을 진단하기 위한 정보를 기반으로 분류한다. 또한 일부 보안약점의 예를 통하여 진단하기 위한 알고리즘을 llvm의 Clang 도구에 적용하기 위한 방법을 연구한다. 이를 통하여 블록체인과 관련된 보안약점을 분류하고 그에 대한 진단 방법을 연구하였다. 향후 기존 정적 분석 도구를 확장함으로써 진단 성능을 높일 수 있을 것이며, 줄리엣 코드와 같은 벤치마크 테스트를 통해 그 결과를 비교해볼 수 있을 것이다.

키워드: 보안약점 (Weakness), 진단 방법 (Diagnostic Method), 블록체인(Blockchain)

I. Introduction

최근 블록체인이 많은 분야에서 활용되고 있다. 블록체인은 중앙화 되어 있던 것을 분산화 하는 것을 목표로 한다.[1] 블록체인은 기본적으로 구성 노드들의 검증 과정을 통하여 변조를 막는 것을 목적으로 하고 있다. 그러나 블록체인 개발에 사용되는 도구들에도 보안약점이 포함되어 있어 그 약점이 공격의 대상이 될 경우 완벽하게 변조를 막는다고 보장할 수 없다. 본 연구에서는 블록체인과 관련된 몇 개의 개발 플랫폼을 정적 분석 도구로 분석함으로써 포함된 보안약점을 추출한다. 또한 그 보안약점을 진단하기 위한 정보를 컴파일러 단계에서 얻을 수 있는 정보를 기반으로 분류하고 이에 따라 보안 약점을 분류한다. 일부 보안약점의 예를 통하여 보안약점을 진단하기 위한 알고리즘을 연구하고 이를 llvm[2]의 Clang 정적 분석 도구에 적용하기 위한 방법을 연구한다.

II. Preliminaries

1. Blockchain

블록체인은 거래 내역을 블록으로 연결하고 분산된 블록을 체인으로 연결함으로써 데이터를 분산 처리하는 기술이다.[1] 본 연구에서는 블록체인 관련 도구 중 보유한 정적분석 도구로 분석 가능한 Trust Wallet Core[3]와 Hyperledger Fabric SDK[4]를 대상으로 보안약점을 분석 하였다. 그 결과는 Table 1. 과 같다.

Table 1. Weaknesses in Platforms for Blockchain

Trust Wallet Core	Hyperledger Fabric
CWE-191, CWE-390, CWE-401, CWE-415, CWE-468, CWE-562, CWE-570, CWE-571, CWE-676, CWE-754, CWE-767	CWE-22, CWE-99, CWE-209, CWE-390, CWE-397, CWE-476, CWE-495, CWE-496, CWE-571, CWE-597, CWE-754, CWE-1071

2. LLVM (Low-Level Virtual Machine)

llvm은 2000년에 시작된 오픈소스 컴파일러 프로젝트로, 재사용 가능한 모듈식 컴파일러 및 툴 체인 기술 모음이다.[2] 이 중 Clang[5]은 C 관련 언어를 위한 프론트엔드로, llvm을 백엔드로 하며, Clang 프론트엔드와 Clang 정적분석기로 구성되어 있다.

III. Weakness Analysis and Diagnosis

1. Classification of Weaknesses

대상 블록체인 개발 도구에서 추출된 보안약점 분석을 위하여 CWE[6] 사이트의 정보를 활용하였다. 보안약점 진단을 위하여 필요한 정보를 기반으로 하여 어휘를 포함한 구문, 제어와 데이터의 흐름 정보, 값 분석과 타입 등 기타 심화 정보로 구분하였다. 이는 컴파일러의 각 단계에서 추출할 수 있는 정보를 기반으로 한 것이다.[7]

보안약점에 대한 진단 방법을 기반으로 분류한 결과는 Table.2와 같다.

Table 2. Classification of Weaknesses

Syntax Analysis	Flow Analysis	Value Analysis	Type and Etc.
CWE-22, 209, 390, 397	CWE-191, 401, 415, 468, 476, 496, 562, 568, 754	CWE-570, 571	CWE-470, 491, 586, 597, 676, 767, 1071

2. Extension of Clang Static Analyzer

본 연구에서는 블록체인 관련 일부 보안약점에 대하여 진단을 위한 알고리즘을 개발하였다. 이를 Clang 정적 분석기에 적용하여 분석기를 확장하기 위해 Clang 정적 분석기와 llvm에서 필요한 라이브러리를 분석하였다. 예를 들어, CWE-571 “Expression is Always True” 보안약점의 경우, 다음과 같이 진단 단계를 구현할 수 있다.

1) 분기 조건에 대하여 진단하므로 BranchCondition에 대한 콜백 함수 구현
2) getSVal() 함수를 이용하여 가치객체 값 추출
3) isTainted() 함수를 이용하여 가치객체 값이 외부 입력이나 다른 변수에 의한 오염이 있는지 확인. 오염이 있는 경우 리턴
4) UndefinedVal 타입으로 변환하여 외부 입력에 의존하는지 확인. 외부 입력에 의존하는 경우 리턴
5) ConcreteInt 타입으로 변환하여 고정 값을 가지는지 확인. 그렇지 않은 경우 리턴
6) 고정 값을 가지면서 true인 경우 보안약점 검출

이 예시와 같이, 보안약점을 분석하기 위하여 필요한 정보를 분석하고, 이를 표현하기 위해 필요한 llvm과 Clang의 라이브러리를 추출한다. 이러한 과정을 통하여 Clang 정적 분석기에서 진단하지 않는 보안약점에 대하여 분석 기능을 확장할 수 있다.

IV. Conclusions

본 연구에서는 블록체인과 관련된 다양한 개발 도구 중 C/C++, 자바 언어로 구현되어 있는 도구를 대상으로 보안약점을 분석하였다. 또한 이러한 보안약점을 진단하기 위한 정보를 기반으로 보안약점을 분류하였다. 이는 컴파일러 구현의 각 단계에서 얻을 수 있는 정보를 활용하기 위한 준비 단계라고 할 수 있다. 또한 기존의 확장 가능한 정적 분석 도구에서 이러한 정보를 추출하기 위한 라이브러리를 추출하여 적용함으로써 정적 분석 도구의 진단 능력을 확장할 수 있을 것이다. 이러한 정보를 기반으로 블록체인 관련 보안약점에 대한 진단 알고리즘을 개발하였다.

향후 이러한 진단 알고리즘을 구현하기 위한 라이브러리를 좀 더 정교하게 분석하고 활용하여 기존 도구를 확장할 수 있을 것이다. 기존 정적 분석 도구를 확장함으로써 진단을 원하는 대상 보안약점에 대한 진단 성능을 높일 수 있을 것으로 기대한다. 도구 확장에 대한 성능 향상 결과는 줄리엣 코드[8]와 같은 벤치마크 테스트를 통해 비교해볼 수 있을 것이다.

ACKNOWLEDGEMENT

This work was supported by the National Research Foundation of Korea (NRF) grant funded by Korea government (MSIT) (No. 2019R1H1A2080156)

REFERENCES

[1] Sungmook Park, “Blockchain you can see”, Information Publishing Group, pp. 22-48, 2018
[2] LLVM, *http://llvm.org/*
[3] Trustwalletcore, *https://github.com/trustwallet*
[4] Hyperledger Fabric, *https://www.hyperledger.org/use /fabric*
[5] Clang, *http://clang.llvm.org/*
[6] CWE, Common Weakness Enumeration, h*ttps://cwe.mitre.org/*
[7] Kyungsook Han, Damho Lee, Changwoo Pyo, Classification of Diagnostic Information and Analysis Methods for Weaknesses in C/C++ Programs, Journal of The Korea Society of Computer and Information Vol. 22 No. 3, pp. 81-88. March 2017.
[8] Juliet test-suite, https://samate.nist.gov/SRD/testsuite.php/