Universidad Nacional de San Luis

Detección de vulnerabilidades en especificaciones de contratos inteligentes de la plataforma Ethereum

Mauro C. Argañaraz(1), Mario M. Berón(1), Maria J. Varanda Pereira(2), Pedro R. Henriques(3) & Daniel Riesco(1)
(1)Departamento de Informática - Facultad de Ciencias Física Matemáticas y Naturales
Universidad Nacional de San Luis
(2) Research Centre in Digitalization and Intelligent Robotics (CeDRI) - Instituto Politécnico de Bragança, Portugal
(3)Universidade do Minho - Braga, Portugal
marganaraz@gmail.com(1), {mberon, driesco}@unsl.edu.ar(1), mjoao@ipb.pt(2),
pedrorangelhenriques@gmail.com(3)

OBJETIVO

Construir una herramienta web open source que permita automatizar el proceso de análisis y detección de vulnerabilidades en especificaciones de contratos inteligentes escritas en los lenguajes de programación que soporta la plataforma Ethereum, a través de la ejecución de una serie de reglas predefinidas que utilizan una estructura intermedia que representa el código fuente de un contrato inteligente y en la cual se puedan identificar patrones de seguridad que se almacenan en una base de conocimiento.

CONTEXTO

La presente línea de investigación se enmarca en:

Proyecto de Investigación: **"Ingeniería de Software: Estrategias de Desarrollo, Mantenimiento y Migración de Sistemas en la Nube"**. Facultad de Ciencias Físico Matemáticas y Naturales, Universidad Nacional de San Luis.

Año: **2021**
Director: **Daniel Riesco**
Co-Director: **Roberto Uzal**

RECURSOS HUMANOS

Integrantes: 26
Becarios: 1
Tesis de posgrado en ejecución: 14
Tesis de posgrado aprobadas: 9
Tesis de grado aprobadas: 3

LINEA DE INVESTIGACION

Plantear una estrategia para la detección de vulnerabilidades. Por un lado, utiliza un enfoque de verificación con las siguientes características

- **Lenguaje destino**: lenguajes de alto nivel de la plataforma Ethereum (se selecciona Solidity como caso de estudio)
- **Método de análisis**: estático
- **Garantías**: búsqueda de bugs
- **Grado de automatización**: verificación automatizada

Por el lado de los enfoques de diseño, se toman como base los patrones de seguridad para lenguajes existentes y la idea de construir una representación intermedia para analizar los aspectos de seguridad.

1. **El proyecto open source OpenBalthazar consiste en una herramienta web de análisis estático para los contratos inteligentes de la plataforma Ethereum implementada con Microsoft .NET Core.**

2. **Está implementado Solidity y se inició el desarrollo de las reglas de Vyper, si bien es una herramienta extensible y se pueden incorporar nuevos lenguajes como Bamboo.**

3. **Se utiliza la librería ANTLR 4 y las gramáticas de Solidity y Vyper para generar el AST. Este árbol se puede enriquecer con información adicional utilizando algoritmos y técnicas de procesamiento de lenguajes. Las reglas de verificación construidas utilizan un repositorio de patrones que definen los criterios en términos del árbol.**

COMO SEGUIMOS

Realizar un seguimiento de nuevas amenazas, vulnerabilidades y ciberataques en materia de despliegue y ejecución de contratos inteligentes.

- Generalización para otras plataformas que soporten contratos inteligentes.
- Obtención de código fuente a partir de bytecode EVM para aplicar el análisis.
- Análisis de seguridad que surjan de la interoperabilidad con otras blockchain.

 RedUNCI - UNdeC. ISBN 978-987-24611-4-0