Tema: Building a Database for Evaluating Smart Cintract Vulnerability Detection Tools

Andando em Círculos? TCC da USP aponta possíveis problemas com a forma com que ferramentas de detecção de vulnerabilidades em contratos inteligentes são validadas

04 de dezembro de 2023

A segunda maior rede blockchain de cunho financeiro, o Ethereum, foi pioneira na utilização de contratos inteligentes em blockchain. Estes pequenos códigos implementam funcionalidades como carteiras de ativos digitais, tokens e *crowdfundings*. Com o aumento do volume de fundos que circulam por estes contratos inteligentes, uma série de ataques à contratos na rede do Ethereum começou a ocorrer utilizando-se de uma série de vulnerabilidades a época ainda desconhecidas presentes em diversos destes contratos. A mais famosa, ocorrida em 2016, desviou o equivalente a US$320.000.000,00 e foi apelidada de "TheDAO".

Em vista destes ataques uma serie de ferramentas foi desenvolvida a fim de detectar vulnerabilidades em contratos inteligentes da rede Ethereum. Entretanto, um projeto de TCC da USP apontou um possível problema com a forma com que estas ferramentas estavam sendo validadas. Basicamente, uma nova ferramenta desenvolvida era testada utilizando-se uma base de contratos inteligentes extraídos da rede do Ethereum e varridos com outras ferramentas de detecção de vulnerabilidades já presentes na literatura ou analisadas manualmente. A ferramenta desenvolvida então varria esta base e os resultados eram comparados.

Um projeto de TCC da USP apontou que esta forma de validação não é ideal pois se baseia muito fortemente em outras ferramentas de detecção de vulnerabilidades que, na maioria dos casos, foi validada da mesma forma. Além disso, uma análise manual se mostra muito ineficiente e suscetível a erro pois muitas das bases de contratos inteligentes utilizadas na validação de ferramentas de detecção de vulnerabilidades são compostas por centenas ou até mesmo milhares de contratos inteligentes. Assim, mesmo que estas técnicas de validação tenham o seu mérito, é possível que o avanço do estado da arte nesta área esteja avançando muito lentamente.

O TCC ainda propõe uma solução para este problema baseada em apontamentos feitos por pesquisadores na literatura acadêmica que já começavam a desconfiar que a validação das ferramentas de detecção de vulnerabilidades em contratos inteligentes na rede do Ethereum pouco contribuía para o avanço do estado da arte. Basicamente, é apresentada uma base de mais de 50 contratos inteligentes curtos implementados manualmente que foram rotulados ao longo de seu desenvolvimento. Cada um destes contratos inteligentes implementa algum caso de uso real de contratos inteligentes na rede do Ethereum em que uma de dez vulnerabilidades estudadas pelo aluno poderiam comprometer de alguma forma o funcionamento deste contrato ou desviar fundos.

Uma vez apresentado o TCC esta base de dados foi aberta para amplo uso por desenvolvedores de ferramentas de detecção de vulnerabilidades no Ethereum bem como para contribuições feitas por estudantes, pesquisadores, desenvolvedores e entusiastas. Entretanto, o aluno afirma que embora um passo importante para que futuras ferramentas de detecção de vulnerabilidades sejam validades de forma mais robusta, esta base de dados apenas ainda não configura o cenário ideal de validação. Além disso, o aluno se diz engajado em continuar este desenvolvimento de uma forma de validação melhor e mais completa em uma possível pós-graduação.

Integrantes: Ryan Weege Achjian

Professor(a) Orientador(a): Marcos Antônio Simplício Júnior
Co-orientador(a):