1200 - Porosity: A Decompiler For Blockchain-Based Smart Contracts Bytecode

Thursday at 12:00 in 101 Track
45 minutes | Demo, Tool
Matt Suiche*Founder, Comae Technologies*

Ethereum is gaining a significant popularity in the blockchain community, mainly due to fact that it is design in a way that enables developers to write decentralized applications (Dapps) and smart-contract using blockchain technology.

Ethereum blockchain is a consensus-based globally executed virtual machine, also referred as Ethereum Virtual Machine (EVM) by implemented its own micro-kernel supporting a handful number of instructions, its own stack, memory and storage. This enables the radical new concept of distributed applications.

Contracts live on the blockchain in an Ethereum-specific binary format (EVM bytecode). However, contracts are typically written in some high-level language such as Solidity and then compiled into byte code to be uploaded on the blockchain. Solidity is a contract-oriented, high-level language whose syntax is similar to that of JavaScript.
This new paradigm of applications opens the door to many possibilities and opportunities. Blockchain is often referred as secure by design, but now that blockchains can embed applications this raise multiple questions regarding architecture, design, attack vectors and patch deployments.

As we, reverse engineers, know having access to source code is often a luxury. Hence, the need for an open-source tool like Porosity: decompiler for EVM bytecode into readable Solidity-syntax contracts - to enable static and dynamic analysis of compiled contracts.
Matt Suiche
Matt Suiche is recognized as one of the world's leading authorities on memory forensics and application virtualization.

He is the founder of the United Arab Emirates based cyber-security start-up Comae Technologies. Prior to founding Comae, he was the co-founder & Chief Scientist of the application virtualization start-up CloudVolumes which was acquired by VMware in 2014. He also worked as a researcher for the Netherlands Forensic Institute.

His most notable research contributions enabled the community to perform memory-based

forensics for Mac OS X memory snapshots but also Windows hibernation files.
Since 2009, Matt has been recognized as a Microsoft Most Valuable Professional in Enterprise Security due to his various contributions to the community.

@msuiche

#defcon25/by_track/101/thursday #defcon25/By_Day/_thursday