arbitrary./execution

Hacking Smart Contracts With Mainnet Forking

Darian Chan

darian@arbitraryexecution.com

arbitraryexecution.com

Mainnet Forking

What is It

- Copying the state of the blockchain into your local environment
- Includes all balances and smart contracts
- You can execute transactions locally to interact with mainnet-deployed smart contracts

Mainnet Forking

Hardhat

- We’ll be using Hardhat to fork mainnet Ethereum
- Hardhat is a development environment that lets you compile, deploy, test and debug your Ethereum software
- Allows you to fork any EVM compatible blockchain, but we will be focusing on Ethereum for today

Mainnet Forking

Use cases

- Locally simulate how your transaction affects the state of the blockchain
- Testing and debugging smart contracts before live deployment on mainnet
- Allows hackers to simulate hacks on real smart contracts before they actually perform the hack

Parity Multisig Hack

Background

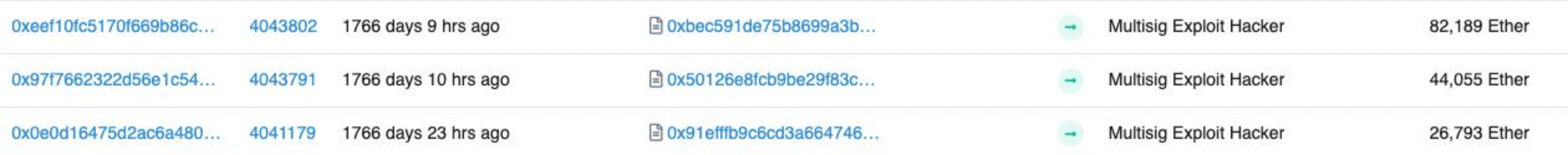
- A vulnerability was found on the Parity Multisig Wallet version 1.5+
- There was an unprotected `initialize` function in the smart contract that allowed the hacker to take control of the smart contract and become the owner
-
  ```
  function initWallet(address[] _owners, uint _required, uint _daylimit)
  ```
- Hacker stole 153,000 ETH on July 19th, 2017
- Valued around $30 Million at the time (closer to $300 Million today)

Parity Multisig Hack

Transactions

- Happened over the course of 3 separate transactions
- Hacker was then able to call the `execute` function to drain the funds

-
  ```
  function execute(address _to, uint256 _value, bytes callData _data)
  ```
- tx: 0xeef10fc5170f669b86c4cd0444882a96087221325f8bf2f55d6188633aa7be7c
- This was the largest transaction out of the 3 and the one we'll replicate



0xeef10fc5170f669b86c…	4043802	1766 days 9 hrs ago	0xbec591de75b8699a3b…	→	Multisig Exploit Hacker	82,189 Ether
0x97f7662322d56e1c54…	4043791	1766 days 10 hrs ago	0x50126e8fcb9be29f83c…	→	Multisig Exploit Hacker	44,055 Ether
0x0e0d16475d2ac6a480…	4041179	1766 days 23 hrs ago	0x91efffb9c6cd3a664746…	→	Multisig Exploit Hacker	26,793 Ether

CTF Challenge

Overview

- Quick reminder that we are hosting a free CTF challenge for everyone
- Claim your free POAP with the handout that you received earlier *(will need our POAP to play the CTF)*
- Have metamask installed on your phone or use Punkwallet.io *(come see me after this presentation if you need help setting that up)*
- Visit our website for more instructions: *https://www.arbitraryexecution.com/otccon*

./ae

Demo Time!