Ethereum responds to eclipse attacks described by research trio

March 5 2018, by Nancy Owano

AI will serve to develop a network control system that not only detects and reacts to problems but can also predict and avoid them. Credit: CC0 Public Domain

In a nutshell, three researchers have described in a paper "Low-Resource Eclipse Attacks on Ethereum's Peer-to-Peer Network" that it is possible to carry out an eclipse attack on the Ethereum network. As important, maintainers of the Ethereum network got on the case and issued an

update.

What is an "eclipse" attack? Amy Castor, who follows Bitcoin and Ethereum, walked readers in *Bitcoin Magazine* through this type of attack.

"An eclipse attack is a network-level attack on a blockchain, where an attacker essentially takes control of the peer-to-peer network, obscuring a node's view of the blockchain."

Catalin Cimpanu, security news editor for *Bleeping Computer*: "Eclipse attacks are network-level attacks carried out by other nodes by hoarding and monopolizing the victim's peer-to-peer connection slots, keeping the node in an isolated network."

Meanwhile, here are some definitions of Ethereum. It is an open software platform based on blockchain technology.

It is also described as "a decentralized platform that runs smart contracts: applications that run exactly as programmed without any possibility of downtime, censorship, fraud or third-party interference."

The network of nodes serves as the backbone of the Ether cryptocurrency, said *Bleeping Computer*, and the myriad of smart contracts that support many other digital currencies and ICOs.

Castor said their discovery was communicated to Ethereum: "The researchers submitted their finding via Ethereum's bug bounty program, a program that rewards individuals for submitting bugs."

The three disclosed the attacks to Ethereum in January and Ethereum developers issued a patch—Geth v1.8.1—as the network fix.

The paper's authors have affiliations that include Boston University and University of Pittsburgh. The paper was posted online March 1, where authors Yuval Marcus, Ethan Heilman and Sharon Goldberg described the attacks.

Goldberg spoke with *Bitcoin Magazine*, and she said working with Ethereum developers to fix the vulnerability was a smooth process. "It was a very functional, easy disclosure," she said.

The authors in their paper thanked Felix Lange and Martin Holst Swende from the Ethereum Foundation (oversees the development of Ethereum) for their "productive collaboration" on the development of patches.

In an email to *Bitcoin Magazine*, Swende, security lead at Ethereum Foundation, said the Geth patch had modifications to the peer-to-peer layer and did not affect consensus-critical code. Users need not be concerned because "an eclipse-attack is a targeted attack against a specific victim," he wrote, adding, "Nevertheless, we recommend all users to upgrade to 1.8.1."

So how was the Ethereum attack possible?

Castor weighed in on a protocol: "Ethereum was actually easier to attack mainly because while Bitcoin relies on an unstructured network where nodes form random connections with each other, Ethereum relies on a structured network based on a protocol called Kademlia, which is designed to allow nodes to connect to other nodes more efficiently."

The authors stated that the eclipse-attack vulnerabilities result from Ethereum's adoption of the Kademlia peer-to-peer protocol.

In the paper, the authors said Ethereum inherits most of the complicated artifacts of the Kademlia protocol yet rarely uses the key property for

which Kademlia was designed.

Solution: Raise the bar for attackers. (As Cimpanu said, however, "The countermeasures don't fully prevent eclipse attacks, but merely raise the number of malicious nodes needed to carry out such an attack from two to thousands.)

"We have suggested a set of countermeasures that eliminates some artifacts of the Kademlia protocol," they wrote. The authors' countermeasures force them "to control thousands of IP addresses (rather than just two) in order to successfully launch attacks."

Many of their counter-measures have already been adopted in geth v1.8.0, said the authors, and these harden Ethereum against the eclipse attacks discussed in the paper.

More information: Low-Resource Eclipse Attacks on Ethereum's Peer-to-Peer Network, (PDF)

Abstract
We present eclipse attacks on Ethereum nodes that exploit the peer-to-peer network used for neighbor discovery. Our attacks can be launched using only two hosts, each with a single IP address. Our eclipse attacker monopolizes all of the victim's incoming and outgoing connections, thus isolating the victim from the rest of its peers in the network. The attacker can then filter the victim's view of the blockchain, or co-opt the victim's computing power as part of more sophisticated attacks. We argue that these eclipse-attack vulnerabilities result from Ethereum's adoption of the Kademlia peer-to-peer protocol, and present countermeasures that both harden the network against eclipse attacks and cause it to behave differently from the traditional Kademlia protocol. Several of our countermeasures have been incorporated in the Ethereum geth 1.8 client released on February 14, 2018.