Security Analyses of Misbehavior Tracking in Bitcoin Network

Wenjun Fan*, Hsiang-Jen Hong*, Simeon Wuthier*, Xiaobo Zhou*, Yan Bai† and Sang-Yoon Chang*
*Computer Science Department, College of Engineering and Applied Science
University of Colorado Colorado Springs, Colorado Springs, United States, CO 80918
Email: {wfan, hhong, swuthier, xzhou, schang2}@uccs.edu
†School of Engineering and Technology,
University of Washington Tacoma, Tacoma, United States, WA 98402
Email: {yanb}@uw.edu

2021 IEEE International Conference on Blockchain and Cryptocurrency (ICBC) | 978-1-6654-3578-9/20/$31.00 ©2021 IEEE | DOI: 10.1109/ICBC51069.2021.9461126

***Abstract*—Because Bitcoin P2P networking is permissionless by the application requirement, it is vulnerable against networking threats based on identity/credential manipulations such as Sybil and spoofing attacks. The current Bitcoin implementation keeps track of its peer's networking misbehaviors through ban score. In this paper, we investigate the security problems of the ban-score mechanism and discover that the ban score is not only ineffective against the Bitcoin Message-based DoS attacks but also vulnerable to a Defamation attack. In the Defamation attack, the network adversary can exploit the ban-score mechanism to defame innocent peers.**

***Index Terms*—Denial-of-Service Attack, Bitcoin, Ban Score, P2P Networking, Sybil, Spoofing, DoS Attack, Cryptocurrency**

I. Introduction

Bitcoin [1] has drawn great attention of the security community since it secures integrity and non-repudiation of the transactions while supporting permissionless operations for decentralization and anonymity. Bitcoin's peer-to-peer (P2P) networking does not use identity-/credential-based cryptographic protections, all the Bitcoin messages ride on plain-text TCP connections, and thus security threats including denial of service (DoS) are prevalent [2]–[4]. For instance, the real-world DoS attacks on the Bitcoin exchange platforms were studied in [5], [6], and the DoS threat using the Bitcoin Core's vulnerability (CVE-2018-17144) [7] enables the malicious miner to validate a block that contains a transaction attempting to spend same input twice to crash the Bitcoin infrastructure.

The present Bitcoin Core has a ban-score framework/mechanism for resisting against the DoS attack [8]. More specifically, a Bitcoin node can use the ban score to keep track of its peer's misbehaviors by increasing the ban score, and once the ban score reaches the threshold at 100, the peer will get banned for 24 hours. However, we find that the current ban-score mechanism is ineffective and vulnerable. Therefore, we are motivated to investigate the DoS threats on Bitcoin networking nodes to discover the attack vectors that can reveal and exploit the ineffectiveness and vulnerability of the ban-score mechanism.

To this end, first, our *Message-based DoS* reveals that the ban score is ineffective and deficient, although it provides some resistance against Sybil since the attacker requires the bulky handshaking-based re-connection process costing the attacker up to hundreds of packet transmissions, while it still suffers multiple DoS attack vectors. Second, we come up with *Defamation* that aims to exploit the vulnerability of the ban-score mechanism. More specifically, the attacker spoofs the innocent peer to send misbehaving messages to the target node for fooling the target node to ban the innocent peer. Using this attack, the network adversary can easily disconnect the peer connections with the purpose of decreasing the diversity of the peer connections and disturbing the Bitcoin operations. This paper aims to inform the Bitcoin and blockchain R&D communities of the vectors and the severity of the DoS attacks on cryptocurrency P2P networks.

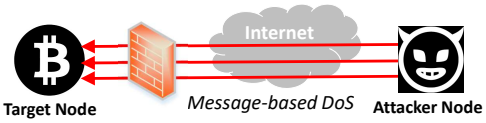

Fig. 1. Thread model of Message-based DoS

II. Ineffectiveness: Message-based DoS can Breach the Ban Score Integrity

A. Threat Model for Ineffectiveness

Figure 1 shows the thread model for our Message-based DoS. The network adversary needs to connect to the public internet and knows the target Bitcoin node's IP address and that should be reachable, which are the prerequisites for taking our attacks. Also, to launch the application-layer Message-based DoS, the attacker node needs to create a Bitcoin session to the target node, which means the attacker node needs to establish a TCP connection with the target node first. Thus, the Message-based DoS attack is a connection-based attack.

B. Attack Vectors

*1) **Nullifying ban score by using messages never getting banned**:* In fact, not every Bitcoin message type is equipped with ban score, and only 11 out of 26 message types possess corresponding ban-score rules [9]. Thus, the adversary can use those no-ban-score messages (e.g. Bitcoin `PING` message) to launch Message-based DoS to attack the target node.

978-1-6654-3578-9/21/$31.00 ©2021 IEEE

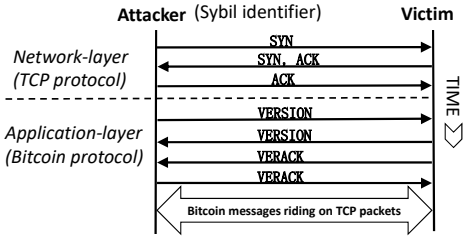

Fig. 2. Sybil identifier to establish Bitcoin connections

*2) **Forgoing ban score by constructing bogus messages**:* We discover that the adversary can use the messages having ban score to attack the target node as long as the adversary can construct the bogus message payload which can bypass the corresponding ban-score-based checking. For instance, despite the `BLOCK` message does have ban-score rule protection, an adversary can still construct bogus payload with invalid Proof-of-Work (PoW) hash value while with incorrect checksum, and send it to the target node. The target node will process the message and drop it when it finds the message's checksum incorrect, but that happened before the ban-score-based checking, whereby the adversary's connection will not get banned.

*3) **Defeating ban-score mechanism by creating serial and multiple Sybil connections**:* Furthermore, the adversary can generate serial and multiple Sybil identifiers to connect to the target node and transmit misbehaving messages to it. More specifically, in the context of permissionless Bitcoin P2P networking, one entity/node can have multiple identifiers. With that, an attacker node is able to use multiple identifiers to establish Bitcoin connections to the target node. Figure 2 illustrates how Sybil identifier works for this attack vector. The attacker node (*A*) using Sybil socket pairs (picking an unused `[IP:Port]`) initiates the TCP three-way handshake to the victim node (*V*), i.e., the target node, listening on port 8333. If the Sybil attacker *A* succeeds, it can exchange Bitcoin messages with *V* directly. Thereafter, *A* can transmit misbehaving messages to *V* for DoS attack. When a prior identifier gets banned, the attacker node can use another un-banned identifier (e.g., another port with the same IP address) to create the next connection in serial to keep sending misbehaving messages to attack the target node.

III. Vulnerability: Ban Score Enables Defamation on Innocent Peer

A. Threat Model for Vulnerability

Figure 3 presents the threat model of Defamation. It is apparent that there are two victims involved in this attack, i.e., the target node and the innocent peer. Thus, the attacker should first know the IP addresses of both of them. Second, the attacker is assumed to have the spoofing capability to impersonate the innocent peer to connect to the target node. Also, the attacker should be able to craft misbehaving Bitcoin messages to trigger the ban score increasing.

B. Attack Vectors

*1) **Pre-connection Defamation**:* In this case, the attacker only needs to know the existence of the innocent peer identifier j and the target node identifier i, and only to preemptively

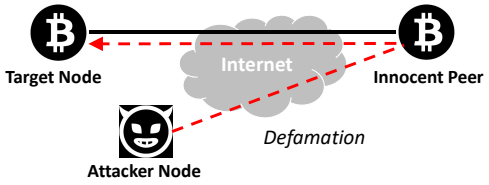

Fig. 3. Thread model of Defamation

Algorithm 1 Post-connection Defamation

Require: A can sniff i's inbound peer connection from j
Ensure: j gets banned by i
1: A gets 4-tuple [i's IP, i's port, j's IP, j's port]
2: **while** A performs real-time eavesdropping **do**
3: A learns the current TCP `seqnum` and `acknum`
4: A craft misbehaving message with the packet header using the 4-tuple and the expected `seqnum` and `acknum`
5: A inject the misbehaving message to i
6: i increase ban score against j
7: **end while**

make j get banned by i, even before j attempts to connect to i. In other words, the attacker node uses j spoofing the innocent peer to connect to the target node and transmit misbehaving messages to i. Hence, this attack will work if it occurs before j connects to i, and there is no TCP connection between the original innocent peer and the target node. Thus, the attacker node only needs to perform IP spoofing rather than real-time eavesdropping and TCP data injection.

*2) **Post-connection Defamation**:* In this case, the target node i and the innocent peer j have already established a TCP connection, where assuming j is an inbound peer of i. To defame j, the attacker A needs to perform not only spoofing but also sniffing and learning the real-time TCP connection state in order to inject data into the connection. In other words, A should be capable of spoofing j and inject misbehaving messages to i to make i to ban j. The attack procedures can be described by Algorithm 1.

IV. Conclusion

Although Bitcoin uses ban-score-based misbehavior tracking to secure networking, we discover that the current ban-score-based protection is ineffective and vulnerable. This ban-score-based protection can be nullified or bypassed, which means an adversary can still use the ban-score protected messages to attack the victim, by crafting bogus messages. Even worse, the ban-score mechanism has a severe side-effect, which enables an attacker to defame the innocent and benign Bitcoin peers due to the ease of launching connection identifier spoofing attack in the permissionless P2P networking context. We reveal and prototype a variety of DoS attack vectors against the current ban-score mechanism. Our ongoing and future work aims to secure the blockchain networking, e.g., anomaly detection [10], and we call for greater R&D from others in the cybersecurity community to design and build security mechanisms to replace the ban-score mechanism.

Acknowledgment

This paper was supported by Colorado State Bill 18-086 and the National Science Foundation under Grants 1922410 and 1921576.

REFERENCES

[1] S. Nakamoto *et al.*, "Bitcoin: A peer-to-peer electronic cash system," 2008.

[2] J. Bonneau, A. Miller, J. Clark, A. Narayanan, J. A. Kroll, and E. W. Felten, "Sok: Research perspectives and challenges for bitcoin and cryptocurrencies," in *2015 IEEE Symposium on Security and Privacy*, 2015, pp. 104–121.

[3] A. Biryukov and I. Pustogarov, "Bitcoin over tor isn't a good idea," in *2015 IEEE Symposium on Security and Privacy*, 2015, pp. 122–134.

[4] M. Conti, E. Sandeep Kumar, C. Lal, and S. Ruj, "A survey on security and privacy issues of bitcoin," *IEEE Communications Surveys Tutorials*, vol. 20, no. 4, pp. 3416–3452, 2018.

[5] M. Vasek, M. Thornton, and T. Moore, "Empirical analysis of denial-of-service attacks in the bitcoin ecosystem," in *Financial Cryptography and Data Security*, R. Böhme, M. Brenner, T. Moore, and M. Smith, Eds. Berlin, Heidelberg: Springer Berlin Heidelberg, 2014, pp. 57–71.

[6] A. Feder, N. Gandal, J. T. Hamrick, and T. Moore, "The impact of DDoS and other security shocks on Bitcoin currency exchanges: evidence from Mt. Gox," *Journal of Cybersecurity*, vol. 3, no. 2, pp. 137–144, 01 2018.

[7] BitcoinCore, "CVE-2018-17144 Full Disclosure," https://bitcoincore.org/en/2018/09/20/notice/, 2018, online; accessed 31 October 2019.

[8] Gavin Anderson, "Denial-of-service prevention," https://github.com/bitcoin/bitcoin/pull/517, 2011, online; accessed 31 October 2019.

[9] BitcoinProject, "The set of 26 bitcoin message types," 2020. [Online]. Available: https://developer.bitcoin.org/reference/p2p_networking.html

[10] J. Kim, M. Nakashima, W. Fan, S. Wuthier, X. Zhou, I. Kim, and S.-Y. Chang, "Anomaly detection based on traffic monitoring for secure blockchain networking," in *IEEE International Conference on Blockchain and Cryptocurrency (ICBC)*, 2021.