Prof. Laurent Vanbever
Networked Systems Group

On-Path attackers against Bitcoin

Semester/Master thesis proposal

Bitcoin is notorious for its centralization [1], which is said to become even more pronounced [2]. This combined with the fact that Bitcoin messages are unencrypted and lack any integrity guarantees, allow certain ASes to intercept and act upon a large volume of traffic. For instance in our previous work [1], we had shown that on-path attackers can tamper with messages and eclipse nodes for even 20 minutes while staying undetected. Later, authors in [3] showed that an AS-level, on-path adversary can increase the amount of Bitcoin traffic she intercepts, by persuading a victim client to connect to peers, the paths to whom traverse the adversary's network. To do so, the AS-level adversary uses IP spoofing. While effective these attacks do not reveal the full attack surface. For example, an AS-level adversary could also *(i)* affect the structure of the Bitcoin graph; *(ii)* censor transactions; *(iii)* de-anonymize users; and *(iv)* mess with a client's system clock. Next, we discuss each of the potential threats.

Modify the Bitcoin Graph Structure: An AS-level adversary could influence the delay properties of the Bitcoin peer-to-peer graph by influencing the peer selection. Intuitively, a loosely connected graph, would result in an increased orphan rate. To do so, an on-path adversary could abuse two mechanisms used by Bitcoin: (i) the peer advertisement; (ii) the banning mechanism. Concretely, by changing the content of address advertisements, an adversary can flood the address pool of victim nodes with malicious ones. Similarly, by tampering with multiple Bitcoin messages an AS-level adversary can trigger the banning mechanism, essentially causing useful connections to be torn down for many hours.

Censoring Transactions: An AS-level adversary can tamper with inventory messages to delay or prevent certain transactions from being included in the Blockchain. This is an effective DoS attack against targeted organizations which will not be able to timely secure their operations.

De-anonymizing: ISPs might not be willing to risk their reputation to act on traffic, still they might be willing to keep metadata of seen transaction allowing them to map Bitcoin addresses to IPs.

Time Jacking: AS-level attackers can also modify Bitcoin messages in order to advertise the wrong time. By doing so she can alter a target's network time counter and deceive it into accepting an alternate blockchain. Indeed, all participating nodes in the Bitcoin network maintain a time counter representing network time. The value of the counter is based on the median time of a node's peers. If the median time differs by more than 70 minutes the system time, the network time counter reverts to system time.

Milestones The required work can be split roughly into the following milestones:

1. Thoroughly look at all the operations performed by a Bitcoin client, and elaborate on two-three vulnerabilities (possibly among the proposed ones).
2. Implement and test the attacks against actual Bitcoin clients.
3. Simulate the routing graph of the Bitcoin network to quantify the potential impact of the attacks.

Requirements

- Some familiarity with the Bitcoin system.
- Skills in programming (preferably C++) and data analysis.

Contact

- Maria Apostolaki, apmaria@ethz.ch
- Prof. Dr. Laurent Vanbever, lvanbever@ethz.ch

References

[1] M. Apostolaki, A. Zohar, and L. Vanbever. Hijacking bitcoin: Routing attacks on cryptocurrencies. In *2017 IEEE Symposium on Security and Privacy (SP)*, pages 375–392. IEEE, 2017.

[2] M. Saad, V. Cook, L. Nguyen, M. T. Thai, and A. Mohaisen. Partitioning attacks on bitcoin: Colliding space, time and logic. Technical report, Tech. Rep, 2019.

[3] M. Tran, I. Choi, G. J. Moon, A. V. Vu, and M. S. Kang. A stealthier partitioning attack against bitcoin peer-to-peer network. 2020.