Partitioning Attacks on Bitcoin: Colliding Space, Time, and Logic
Review
Name: Ashwath Venkataraman

Bitcoin is a type of cryptocurrency, a decentralized form of currency, which can be sent from one user to another user without the need for third-party intermediaries in a peer-to-peer blockchain network. The network contains nodes connected to each other via their IP addresses and information throughout the network is exchanged by using a simple broadcast protocol. Essentially information exchanged are the transactions, addresses and blocks. Specific type of nodes, called miners create blocks containing the hashed transaction information, add it to the blockchain and distribute it across to the other nodes for validation.

There are four types of partitioning attacks that can be launched on the Bitcoin network: **Spatial Partitioning, Temporal Partitioning, Spatio-Temporal Partitioning and Logical Partitioning.**

Spatial Partitioning is a type of attack in which the adversary tries to isolate the set of nodes, restrict access to the nodes in the network and launch a BGP hijacking attack. The attack is based on the number of ASes (Autonomous Systems) and the number of nodes hosted by an AS. Nodes concentrated within few ASes, are more centralized and more vulnerable to a BGP attack. Data analysis in the paper shows that more than 30% of the Bitcoin traffic is hosted by 8 organizations and ASes, making an attack even more effective. Mining pools consists of miners who send their proof of work (PoW) to a Stratum server. Organizations hosting more that 50% of mining power make attacks easier. Spatial partitioning causes double spending, eclipse attacks, the 51% attack and mining pools with lower hash rates can block rewards, in turn compromising the network.

Temporal Partitioning involves isolation of nodes whose blockchain are not properly updated with respect to the current state of the network. This gives the adversary a chance to attack outdated nodes, take control of them, isolate them, disrupt communication, in turn creating forks in the network. Data analysis from the paper takes snapshots at various intervals and reports that consensus pruning is not uniform across the network and attacker can find a time window to isolate a group of nodes. Thus this attack is represented as an optimization model to find the majority of nodes that is not updated, within a given time constraint. Information propagation in a Bitcoin network takes exponential delay, and gives the adversary the required time to connect with the victim nodes. Temporal partition causes significant loss to stakeholders, transaction invalidations and the entire network is disrupted.

Spatio-temporal partitioning attack makes use of the both temporal attack - for blocks behind the main chain, and spatial attack - isolate the nodes and launch a spatial attack by BGP hijacking. Attack of this type depends on the miner, a cloud servicer type of adversary with both routing and mining capabilities can launch a spatio-temporal attack. A cloud service provider typically attacks synced nodes by BGP hijacking, find a time to attack between lagged and synced nodes to launch a temporal attack. A cascading attack is possible that can compromise the entire network.

Logical partitioning involves modification of the Bitcoin core protocol software by malicious peers. Bitcoin network is public to any client and as such, it is easy for the attacker to gain the

confidence of full nodes by providing attractive capabilities. An example is Falcon (not malicious) that demonstrates how independent software could gain general acceptance. In a similar way an adversary can attack cooperating peers and in turn control a significant portion of the network, taking advantage of incentives, stealing Bitcoin wallets, isolate nodes and create chances for several other network attacks.

Several **countermeasures** to hinder the adversaries are discussed as well. To lower the chances of a spatial attack, stratum servers and node exchanges should be spread across multiple ASes. A simple and an effective scheme called BlockAware is proposed to counter temporal partitioning. In this scheme, the timestamp of the latest block and the current block is compared. If it crosses 10 minutes which is the block time in Bitcoin, it is indicated that the latest block has not yet been received. Using this information, nodes can query for latest blocks quicker. Bitcoin is an open and a public protocol. It is decentralized in nature and violating that would violate the very aspect of the protocol itself. Thus vulnerability to a logical attack is something that is not looked upon much.

Comments, Views and Suggestions

This paper pretty much covers all the domains an adversary can take advantage of, to attack a Bitcoin network in a very simple, yet elegant manner. The various other types of attacks that occur in Bitcoin like routing attacks (spatio-temporal), selfish mining (temporal), block withholding (temporal), timejacking (temporal) etc. essentially fall into one of the four types of partitioning attacks as well.

However the paper could provide a little bit more substantial evidence in the case of a temporal attack where a false block is mined. Mining a block requires huge resources and it is not really practical for an attacker to possess such a big amount of power required to mine a block before other original nodes in the network. The adversarial capabilities could be explored a bit more to validate this.

In the spatial partitioning scheme, a suggested countermeasure could be to employ a type of a “dumb” server analogy, where a number of dumb server nodes could be deployed along with the original nodes in the network within an AS. An adversary attacking the AS based on the prefix to capture a victim node with the same prefix address could latch on to this fault tolerant dumb node. This is a simple high level scheme, which is to develop a fault tolerant AS, however this occurs at the expense of extra costs. This is also analogous to a bogus route purging scheme and can reduce the chance of an attack to some extent.

Another suggested countermeasure could be to employ better security mechanisms in general within an AS like provisioning extra bandwidth, so that one can accommodate unexpected or a sudden surge of traffic across a network coming from an attacker. This is a type of prevention mechanism for a DDoS (Distributed Denial of Service) attack, that could give us some time to act before our resources are gotten rid of completely. Also since more bandwidth is provisioned, it takes less time for block propagation. This is a suggested countermeasure for a temporal partitioning attack. Through this, the possible block time could also be reduced to be less than 10