Eclipse attacks on Bitcoin's peer-to-peer network

Review

Name: Ashwath Venkataraman UFID: 5198-9461

An **Eclipse attack** aims to take control of a victim node by monopolizing incoming and outgoing connections to and from it. The adversary on having control over a specific number of IP addresses, can soon exploit it by taking over its mining power, computational resources and consensus mechanism. The paper gives a detailed idea about the quantification of resources that are needed for the eclipse attack. The eclipse attack as a consequence can lead to several other attacks like selfish mining, 0-confirmation and n-confirmation double spend and splitting of mining power.

Peers in a Bitcoin network exchange information through TCP connections and are identified by their respective IP addresses. In a typical Bitcoin network, a node can allow up to **117 incoming connections and 8 outgoing connections**. IP addresses that are public are stored in a peer's '**tried**' (that consists of 64 buckets of addresses for successful connections) and '**new**' (that contains 256 buckets for connections not yet initiated) tables. An eclipse involves the adversary filling the tried table with malicious nodes and overwriting addresses in the new table with 'trash' addresses. On restart the victim connects with the attacking node with high probability and slowly occupies the tried table (with attack nodes) with no connections from the 'trash' new table. Each step in the attack – population of tried table, writing '**trash**' addresses in the new table, restart of victim node, selecting incoming and outgoing connections are each quantified with probability measurements and mathematical modeling.

Two types of attack variants are discussed in the paper; A **botnet attack** in which a distinct group of addresses of the adversary, with enough diversity attack the node and research showed that no more than 6000 groups are enough to attack; **infrastructure attack** in which the adversary holds sets of addresses in the same group. It is equivalent to a model comprising the nation-wide ISPs. It is shown in the paper that the botnet attack is far superior to infrastructure attack with a success rate far higher.

Countermeasures are deployed for these eclipse attacks and its proven success of preserving Bitcoin's protocol is appreciative, since it has been employed in the real protocol itself. Measures discussed are deterministic random eviction, in which the bitcoin eviction protocol is changed by addresses hashing to a single slot in a bucket, random selection in which address from the tried and new tables are selected in random, which reduces attack to some extent and is remedied more by the test before eviction scheme. Other measures proposed are more buckets, feeler connections, anchor connections, diversification of incoming connections and anomaly detection (detecting short TCP connections, large ADDR messages and trash addresses).

Comments, Views and Suggestions

The paper gives a very clear picture on what an Eclipse attack is, it's consequences in both theoretical and mathematical fashion. Its proven success is very apparent since the counter-measures discussed are implemented in the real Bitcoin protocol itself.

The paper gives a detailed analysis about the attack, but could have given a bit more detail about the capabilities of the attacker himself. In order to pull of an Eclipse attack, attacker needs to be computationally very powerful and this is very costly, which in most cases might be considered impractical. Adversarial capabilities could be outlined more so it could be easier to relate especially with the case of an infrastructure attack that involves a nation-wide attack model.

The notion of "network congestion" could be incorporated since the protocol involves connections over TCP between the peers. The peer message packets, may experience queuing delays during message transmission, establishing incoming and outgoing connections by the adversary may not work out at all times. On the downside this could lead to an entirely different type of attack.

The paper could give a bit more detail about attacks on private IPs, since the paper itself states that outgoing connections (which consist of private IPs) could be to eclipsed public IP nodes.

A suggested countermeasure would be to hide IP addresses by means of masking/hiding IP addresses (say by using VPN connections) or mixing IPs (interchanging IP addresses at a subnet level).