FARIZ IKHSAN
1103170287

Stubborn Mining: Generalizing Selfish Mining and Combining with an Eclipse Attack (Summarize)

Selfish mining, originally discovered by Eyal et al. is a well-known attack where a selfish miner, under certain conditions, can gain a disproportionate share of reward by deviating from the honest behavior.

Since cryptocurrencies carry monetary value, they nat urally become a valuable target of attacks. Intuitively, for a secure-by-design cryptocurrency, an attacker controlling α fraction of the network's computational resource should be able to obtain only α fraction of the mining reward. However, a malicious attacker can employ various types of attacks to gain an unfair share of the mining reward. We refer to such attacks generically as *mining attacks*. Among the most well-known are "selfish-mining"-style attacks that exploit weaknesses in the distributed consensus protocol and network-level attacks that seek to create network partitions between mining powers, referred to as the "eclipse attack".

Selfish mining is not optimal for a large parameter space. We introduce a new family of alternative "stubborn min ing" strategies that generalize and outperform the selfish mining attack. For a large fraction of the interesting pa rameter space, our new strategies significantly increase the attacker's revenue. Depending on the environment param eters, stubborn mining strategies can beat selfish mining by up to 25% (even without leveraging any network-level attacks). Depending on the parameters, and at the price during the time of writing, this can translates to $73K additional gains per day in comparison with the selfish miner.

Depending on the environment param eters, stubborn mining strategies can beat selfish mining by up to 25% (even without leveraging any network-level attacks). Depending on the parameters, and at the price during the time of writing, this can translates to $73K additional gains per day in comparison with the selfish miner. In one of our mining strategies, called trail-stubbornness, the attacker keeps mining on her private fork even if the public fork is ahead, thus violating the longest-chain rule. This surprisingly benefits the attacker since if she happens to overtake the public later, she will have wasted more of the public's mining power. We show that in some cases, a trail-stubborn strategy can result in 13% gains in comparison with a non-trail-stubborn counterpart.

Detecting and inferring attacks. Eclipse attacks and stubborn mining can likely be detected if they occur in practice. One way is by observing the stale block rate – a stale block is one that has valid transactions and proof-of-work, but is ultimately excluded from the main chain.

Eclipse attacks can benefit the victim. As it turns out, the "victim" of an eclipse attack can sometimes even profit from the attack, even when the attacker uses the optimal strategy. This implies that users in some cases may have little incentive to detect or defend against eclipse attacks. For example, suppose Lucy has an accurate belief about the attacker's hashpower and the network propagation parameter.