DA-1 Summer / CSE1006 Blockchain & Cryptocurrency Technologies

by Sharadindu Adhikari, 19BCE2105

In this assignment, about blockchain security attacks, I'm going to group the different types into 4 categories :-

Type-1 : Peer-to-peer Network-based Attacks.

(1) Eclipse Attack : A node will depend on "x" number of nodes selected using a Peer selection strategy to have its view of the distributed ledger. But if an attacker can manage to make the node to choose all the "x" number of nodes from his malicious nodes alone, then he can eclipse the original ledger's view and prevent his own manipulated ledger to the node.

(2) Sybil attack : While the Eclipse attack is about eclipsing a user's view of the true ledger, the Sybil attack targets the whole network. In a Sybil attack, an attacker will flood the network with large number of nodes with pseudonymous identity and try to influence the network. These nodes, though appearing like unrelated individuals, are operated by a single operator at the back. In this case the objective is not to target one user, but a number of nodes or network as whole, and generate a fork in the ledger if possible, allowing the attacker to make double spending and other attacks.

Type-2: Consensus Mechanism and Mining-based Attacks

① **Selfish mining attack**: Many blockchains consider the longest chain to be the true latest version of the ledger. So a selfish miner can try to keep building blocks in stealth mode on top of the existing chain, and when he can build a lead of greater than two or more blocks than the current chain in the network, he can publish his private fork, which will be accepted as a new truth as it is the longest chain. He can do transactions in the public network just before publishing his long stealth chain to reverse the transaction he just did. This effectively provides a small window for the attacker to do double spending based on this ability to build a stealth chain by building sufficient block lead (Finney attack).

② **Mining Malware**: Malware uses the computing power of unsuspecting victims' computer to mine cryptocurrencies for hackers. China reported that over a million computers were infected by this malware and helped attackers mine more than 26 million tokens of various cryptocurrencies.

③ **51% attack**: This attack is possible when a miner or a group of miners controls 51% or more of the mining power of the blockchain network. Though it is very difficult to happen for large networks, the possibility of a 51% attack is higher in small networks.

Once a group has majority control over tramactions on a blockchain network, it can prevent specific tramaction or even reverse old tramactions.

④ Timejack Attack : Nodes in certain blockchain networks like Bitcoin depend on internal timing derived from median time reported by its peer nodes. For example, we depend on our friends to know the time. Let us say an attacker manages to put a lot of malicious people in our friend's list, then he can manipulate our time. The first step to this attack can be an Eclipse attack on the target node. Once this attack is complete on a target node, then the target node will not accept blocks from the actual network as the timestamp of the blocks will not be in line with its timestamp. This provides an opportunity for the attackers to be double spending or do tramactions with the targeted node as these tramactions can't be submitted to the actual blockchain network.

⑤ Finney attack : If I can mine a block with one of my tramactions in it and keep it in stealth, there is an opportunity for me to double spend the money. If a merchant accepts the unconfirmed tramaction, I can transfer him this earlier transacted currency. Next I publish the earlier mined block, which was kept in stealth, before my new tramaction is confirmed on the network.

(6) Race Attack: This attack is minor variation of the Finney attack. The difference is that the attacker need not pre-mine the block with his transaction, which he intends to double spend. During the attack, the attacker submits an unconfirmed transaction to a merchant (vilim) and simultaneously does another transaction which he broadcasts to the network. It is easier for the attack to launch the attack if he is directly connected to the merchant's node. This would give the merchant an illusion that his transaction is the first, but that is never submitted to the blockchain network by the attacker.

(7) Type-3: Smart Contract-based Attacks

(1) The DAO attack: The biggest exploitation in the history of cryptocurrencies is "the DAO" attack. Decentralised Autonomous Organization was an ambitious feature of Ethereum. A company called Slock started crowdfunding for a project called 'the DAO'. The crowdfunding got an overwhelming response, collecting 12.7 million ether, valued at $150M then ($2B today). But an attacker identified a vulnerability in the code, where by, a recursive withdraw function could be executed without checking the settlement of the current function/transaction. So the attacker started the attack by contributing a small amount and requesting withdrawal with a recursive function. This allowed him to pull out almost $70M out of the crowdfund.

After this, the events took an interesting turn. The Ethereum Foundation threatened the attacker to stop the attack and freeze the account. The attacker responded saying that he was playing as per the agreed upon contract and an intervention through a soft or hard fork will be a breach of contract, which he can take to court. But he stopped the attack. Later the Ethereum Foundation went with a hard fork to recover the money, though this decision raised many concerns of autonomy of smart contracts. This hard fork resulted in two Ethereum currencies — Ethereum & Ethereum classic and a lot of controversy.

(ii) Type-4 : Wallet-based Attack

(1) Parity Multisig Wallet Attack : This was the case of a vulnerability with the parity client wallet hacked by an attacker resulting in holding up of 500,000 Ether ($77M today). Wallet contracts are additional logic than can be built on user wallets for regular automated payments. To reduce the gas or transaction fees, the parity Multisig wallet functionality (Multisig wallet is like a joint account in bank with multiple owners) used a centralized Library contract. But they left some critical functions open, resulting in a vulnerability, which was exploited by the

attacker. The attacker added his account as owner in the library contract, so for all wallets implemented after a particular date, the attacker became a joint owner. Then he triggered a kill function, which froze the currencies in the wallet. He basically locked $155M as of that day, forever in cryptographically inaccessible wallets.