**Lecture 5-1 Notes**

**Vulnerabilities on Blockchain**

**Slide 3**

* Cybercriminals have already managed to misuse blockchains to perform malicious actions.
* Ransomware attacks like WannaCry and Petya wouldn’t have been so massive if attackers hadn’t received their rewards in cryptocurrencies.
* Currently, It looks like hackers consider exploiting blockchain security vulnerabilities as their main source of revenue.
* Ex: In March 2019, white hat hackers found 43 bugs in various blockchain and cryptocurrency platforms in just 30 days. They even found vulnerabilities in such famous platforms as Coinbase, EOS, and Tezos.
* However, weak spots are often challenging to detect, since they can be hidden in unobvious places. For instance, the Parity multisig wallet was hacked by breaking a library that had a withdraw function in it. The attacker managed to initialize the library itself as a wallet and claim owner rights to it. As a result, 573 wallets were affected, $30 million worth of crypto was stolen, and another $180 million rescued by a white hat hacker group was later returned to the rightful owners.

**Slide 4**

* By attacking such huge networks as Bitcoin and Ethereum, cybercriminals show that they’re clever enough to disprove the myth of blockchain security. Let’s consider the five most common blockchain attack vectors:
  + **Blockchain Network**
  + **User wallets**
  + **Smart Contract**
  + **Transaction Verification Mechanism**
  + **Mining pool**

**Slide 5**

Identified 65 real-world cybersecurity incidents occurred between 2011 and first half-year 2019 that have adversely impacted blockchain systems. The blockchain cybersecurity vulnerabilities are divided into five categories

* + Clients’ Vulnerabilities
  + Consensus Mechanisms Vulnerabilities
  + Mining Pool Vulnerabilities
  + Network Vulnerabilities
  + Smart Contract Vulnerabilities

**Slide 6**

**1. Blockchain network attacks**

A blockchain network includes nodes that create and run transactions and provide other services. For instance, the Bitcoin network is formed by nodes that send and receive transactions and miners that add approved transactions to blocks. Cybercriminals look for network vulnerabilities and exploit them with the following types of attacks.

**Slide 7**

**Distributed denial of service**

* Distributed denial of service (DDoS) attacks are hard to execute on a blockchain network, but they’re possible.
* When attacking a blockchain network using DDoS, hackers intend to bring down a server by consuming all its processing resources with numerous requests.
* DDoS attackers aim to disconnect a network’s mining pools, e-wallets, crypto exchanges, and other financial services. A blockchain can also be hacked with DDoS at its application layer using DDoS botnets.
* In 2017, Bitfinex suffered from a massive DDoS attack. It was especially inconvenient for the IOTA Foundation, which had launched their IOTA token on the platform the day before Bitfinex informed users about the attack. Three years later, in February 2020, Bitfinex experienced another DDoS attack just a day after the OKEx cryptocurrency exchange noticed a similar attack.

**Slide 9**

**Transaction malleability attacks**

* A transaction malleability attack is intended to trick the victim into paying twice. In the Bitcoin network, every transaction has a hash that’s a transaction ID.
* If attackers manage to alter a transaction’s ID, they can try to broadcast the transaction with a changed hash to the network and have it confirmed before the original transaction.
* If this succeeds, the sender will believe the initial transaction has failed, while the funds will still be withdrawn from the sender’s account.
* And if the sender repeats the transaction, the same amount will be debited twice. This hack is successful once the two transactions are confirmed by miners.
* Mt. Gox, a Bitcoin exchange, went bankrupt as the result of a malleability attack in 2014. However, Bitcoin seems to have solved this issue by introducing the Segregated Witness (SegWit) process, which separates signature data from Bitcoin transactions and replaces it with a non-malleable hash commitment to each signature.

**Slide 10**

**Timejacking**

* Timejacking exploits a theoretical vulnerability in Bitcoin timestamp handling.
* During a timejacking attack, a hacker alters the network time counter of the node and forces the node to accept an alternative blockchain.
* This can be achieved when a malicious user adds multiple fake peers to the network with inaccurate timestamps.
* However, a timejacking attack can be prevented by restricting acceptance time ranges or using the node’s system time.

**Slide 11**

**Routing attacks**

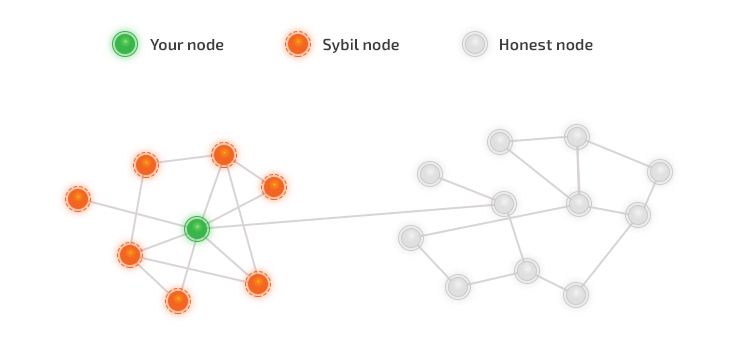
A routing attack can impact both individual nodes and the whole network. The idea of this hack is to tamper with transactions before pushing them to peers. It’s nearly impossible for other nodes to detect this tampering, as the hacker divides the network into partitions that are unable to communicate with each other. Routing attacks actually consist of two separate attacks:

1. A partition attack, which divides the network nodes into separate groups
2. A delay attack, which tampers with propagating messages and sends them to the network

**Slide 12**

**Sybil attacks**

A Sybil attack is arranged by assigning several identifiers to the same node. Blockchain networks have no trusted nodes, and every request is sent to a number of nodes.



*Figure 1. Sybil attack*

* During a Sybil attack, a hacker takes control of multiple nodes in the network. Then the victim is surrounded by fake nodes that close up all their transactions.
* Finally, the victim becomes open to double-spending attacks.
* A Sybil attack is quite difficult to detect and prevent, but the following measures can be effective: increasing the cost of creating a new identity, requiring some type of trust for joining the network, or determining user power based on reputation.

**Slide 14**

**Eclipse attacks**

* An eclipse attack requires a hacker to control a large number of IP addresses or to have a distributed botnet.
* Then the attacker overwrites the addresses in the “tried” table of the victim node and waits until the victim node is restarted.
* After restarting, all outgoing connections of the victim node will be redirected to the IP addresses controlled by the attacker.
* This makes the victim unable to obtain transactions they’re interested in.
* Researchers from Boston University initiated an eclipse attack on the Ethereum network and managed to do it using just one or two machines.

**Slide 15**

**Long range attacks on proof of stake networks**

Long range attacks target networks that use the proof of stake (PoS) consensus algorithm, in which users can mine or validate block transactions according to how many coins they hold.

These attacks can be categorized into three types:

1. Simple — A naive implementation of the proof of stake protocol, when nodes don’t check block timestamps
2. Posterior corruption — An attempt to mint more blocks than the main chain in a given time frame
3. Stake bleeding — Copying a transaction from the honestly maintained blockchain to a private blockchain maintained by the attacker

When conducting a long-range attack, a hacker uses a purchased or stolen private key of a sizable token balance that has already been used for validating in the past. Then, the hacker can generate an alternative history of the blockchain and increase rewards based on PoS validation.

## Slide 16

## User wallet attacks

Actually, blockchains and cybersecurity go together like salt and pepper until people interact with them. It may sound surprising, but blockchain users pose the greatest security threat. People tend to overestimate the security of the blockchain and overlook its weaknesses. User wallet credentials are the main target for cybercriminals.

To obtain wallet credentials, hackers try to use both traditional methods like phishing and dictionary attacks and new sophisticated methods like finding weaknesses in cryptographic algorithms. Here’s an overview of the most common ways of attacking user wallets.

### Phishing

In 2018, there was an attack on IOTA wallets initiated with iotaseed.io (now offline), a fake online seed generator. Hackers conducted a phishing campaign with this service and collected logs with secret seeds. As a result, in January 2018, hackers successfully stole more than $4 million worth of IOTA from victims’ wallets.

### Dictionary attacks

During these attacks, a hacker attempts to break a victim’s cryptographic hash and [salt](https://en.wikipedia.org/wiki/Salt_(cryptography)) by trying hash values of common passwords like password1. By translating clear text passwords to cryptographic hashes, attackers can find wallet credentials.

### Vulnerable signatures

Blockchain networks use various cryptographic algorithms to create user signatures, but they may also have vulnerabilities. For example, Bitcoin uses the ECDSA cryptographic algorithm to automatically generate unique private keys. However, it appears that ECDSA has insufficient entropy, which can result in the same random value in more than one signature. IOTA also faced cryptographic problems with its old Curl hash function.

### Flawed key generation

Exploiting vulnerabilities in key generation, the hacker known as Johoe got access to private keys provided by Blockchain.info in December 2014. The attack happened as the result of a mistake that appeared during a code update that resulted in poor randomness of inputs for generating public user keys. Though this vulnerability was quickly mitigated, the flaw is still possible with the ECDSA algorithm.

### Attacks on cold wallets

Hardware wallets, or cold wallets, can also be hacked. For instance, researchers initiated an Evil Maid attack by exploiting bugs in the Nano S Ledger wallet. As a result of this hack, researchers obtained the private keys as well as the PINs, recovery seeds, and passphrases of victims.

One of the latest cold wallet attacks happened in 2019, when the [UPbit](https://www.hackread.com/upbit-cryptocurrency-exchange-hacked-ether-stolen/" \t "_blank) cryptocurrency exchange was transferring funds to a cold wallet. This is a common way to freeze crypto when you’re expecting a cyberattack. The hackers managed to steal 342,000 ETH, apparently because they knew the timing of the transaction.

### Attacks on hot wallets

Hot wallets are internet-connected apps for storing private cryptographic keys. Though owners of cryptocurrency exchanges claim they keep their user data in wallets disconnected from the web, a $500 million attack on Coincheck in 2018 proved this isn’t always true.

In June 2019, an attack on GateHub resulted in unauthorized access to dozens of native XRP wallets and the theft of crypto assets. Singapore-based crypto exchange Bitrue also experienced a hot wallet attack at almost the same time due to a system vulnerability. As a result, hackers managed to steal funds worth over $4.5 million in XRP and $237,500 in ADA.