Concordia Institute for Information System Engineering
(CIISE)

Concordia University

INSE 6630 – Recent Developments in Information Systems Security (Bitcoin & Blockchain Technology)

Assignment -1:

Submitted to:

Professor Jeremy Clark

Submitted By:

Nithish Reddy Yalaka - 40164619

(Question)

In recent years, we have seen many attacks against Bitcoin, Ethereum, decentralized finance, NFTs, companies involved with cryptocurrencies, or applications built on top of a blockchain.

Answer:

"Hacker's steal $610m from Poly Network in one day, the biggest heist in DeFi history"

The **PolyNetwork Hack**, one of the biggest cryptocurrency thefts ever targeted on Cross-chain decentralized finance (DeFi) platform Poly Network and allowed an undisclosed attacker to steal the equivalent of a whooping 610 million USD of crypto tokens.

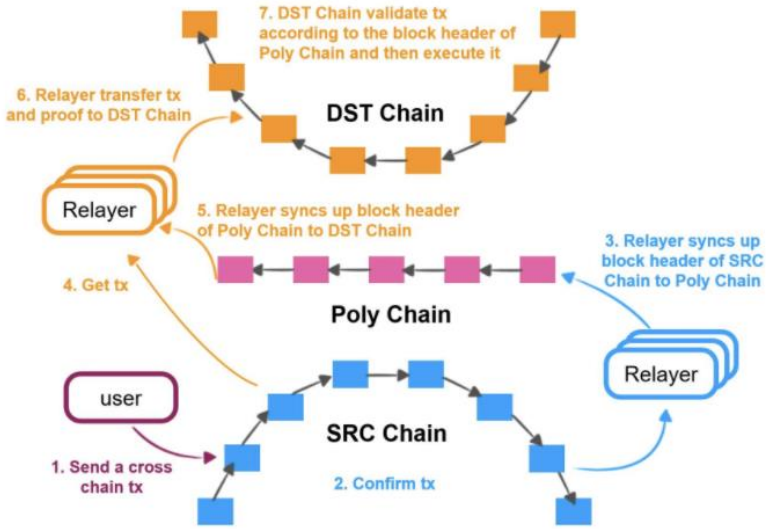
What exactly is a **DeFi**?

Decentralized finance (DeFi) is an emerging financial technology based on secure distributed ledgers similar to those used by cryptocurrencies. The system removes the control banks and institutions have on money, financial products, and financial services.

- DeFi uses the blockchain technology that cryptocurrencies use which is a distributed and secured database or ledger.
- Peer-to-peer (P2P) transactions are one of the core propositions behind DeFi. A P2P DeFi transaction is where two parties agree to exchange cryptocurrency for goods or services with a third party involved.
- DeFi platforms **allow people to lend or borrow funds from others**, speculate on price movements on assets using derivatives, trade cryptocurrencies, insure against risks, and earn interest in savings-like accounts. DeFi uses a layered architecture and highly composable building blocks. [**2**]

What exactly is **Poly Network Platform**?

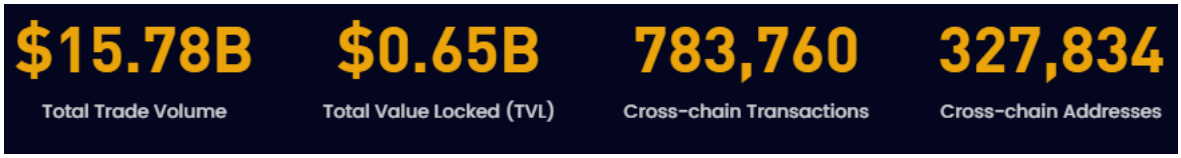
Poly Network is a global cross-chain interoperability protocol for implementing heterogeneous blockchains and building the web3.0 infrastructure, which lets users swap tokens from one digital ledger to another. Poly Network works by facilitating exchange between several blockchains as users trade one cryptocurrency for another, such as trading Bitcoin for Ether. Currently, Poly Network implements interoperability between 11 heterogeneous chains including Bitcoin, Ethereum and so on. Poly Network has also integrated over 15 blockchains, including Ethereum, Polygon, Avalanche, Fantom, BSC, Arbitrum, Optimism, Heco, OEC, Neo, Ontology, Zilliqa, Elrond, xDai, etc. [**4**] [**5**]



Architecture Design of Poly Network

What makes Poly Network one of the finest in the crypto market is its advanced features, including:

1. It's lightweight and loosely coupled architecture
2. It's easy integration with other blockchains
3. It's high speed, low cost, and interoperability
4. It's easy swapping and high security. (Attack happened)
5. It's effective and efficient transfers between Cross-chain asset, and also NFT Cross-chain



The Attack:

Introduction:

Aug 10-2021, Poly Network alerted the world that they have been hacked by "**Mr. White Hat** " and 610 USD million were transferred into his addresses and listed the wallets of the hacker and asked the exchanges to blacklist the stolen assets. IMG-[**2**]

This attack was reported by the team of poly Network upon the movement of 610 million, and they immediately alerted the world by taking it to twitter. IMG [**1**]

According to the architecture of Poly Network, users can initiate cross-chain transactions on the source chain and once the transaction is confirmed, the source chain Relayer synchronizes the block header information to the Poly Chain, then the Poly Chain synchronizes the block header information to the target chain Relayer, and the target chain Relayer transfers the verification information to the target chain, then executes block header verification on the target chain and executes the user's expected transaction. [**17**]

Circumstances of the incident: According to the architecture, these are circumstances that caused the attack. [**17**]

- The source chain didn't check the initiated cross-chain operation
- The target chain did not check the parsed target call contract and call parameters.
- The owner of the `EthCrossChainData` contract is `EthCrossChainManager`.
- `bytes4(keccak256(abi.encodePacked(_method,"(bytes,bytes,uint64)")))` can be collided by hash.

Technical Details involved in the attack:

Poly Network deploys smart contracts on each blockchain for cross-chain interoperability, among which the `EthCrossChainManager` contract is used to verify the block header synchronized by the Poly Chain to confirm the cross-chain, the authenticity of the information. And the `EthCrossChainData` contract is used to store cross-chain data, and the public key of the relay chain validator (i.e., Keeper) is also stored in this contract. `LockProxy` is used for asset management. [**18**] [**17**] [**19**]

1. The main reason of this attack is that the 'verifyHeaderAndExecuteTx' function of the EthCrossChainManager contract can execute specific cross-chain transactions through the '_executeCrossChainTx' function.
2. Since the owner of the EthCrossChainData contract is the EthCrossChainManager contract, the EthCrossChainManager contract can modify the keeper of the contract by calling the 'putCurEpochConPubKeyBytes' function of the EthCrossChainData contract.

3. The ‘verifyHeaderAndExecuteTx’ function of the EthCrossChainManager contract can perform user-specified cross-chain transactions by calling the _executeCrossChainTx function internally. So, the attacker only needs to pass in the carefully constructed data through the ‘verifyHeaderAndExecuteTx’ function for the ‘_executeCrossChainTx’ function to execute the call to the ‘EthCrossChainData’ contract ‘PutCurEpochConPubKeyBytes’ function to change the keeper role to the address specified attackers.
4. After modifying the address of the keeper role, the hacker can construct a transaction at will and transfer any amount of funds from the contract.

Attack Process:

- The hacker carefully constructs an operation on the source chain to modify the Keeper of the target chain.
- The attacker submitted data in the target chain normally using the official Relayer and replaced the Keeper.
- The attacker uses the replaced Keeper address to sign the operation and submits it to ‘EthCrossChainManager’ for verification.
- The attacker verified whether the Keeper is the address that has been replaced by the attacker. If yes, transfer the asset to the address specified by the attacker.

Impact of the Attack:

- Nearly $610 million has been moved into his addresses by hacker. IMG [**3**]
- Poly Network went on to make various upgrades continously to fix these kinds of bugs.
- After the attack, Poly Network came forward with the roadmap of the next phase to mitigate the damage in future. [**16**]
- The world of DeFi was shocked because of the incident.
- The attacker, “Mr. White Hat” was offered 500K USD as the bounty along with the position of Chief Security Advisor (he evidently refused this). [**20**]

How was the issue addressed?

The issue was addressed by Poly Network team by analyzing the bug and further securing the end-end flow and making several upgrades by addressing the Roadmap. Also, the team constantly made efforts while communicating with the hacker along with getting the help from other exchanges(Tether-USDT froze the attacker’s address with a transaction of 32 million USDT) by freezing the addresses of the attacker. Finally, the attacker returned almost everything he stole from the Poly Network. They offered 500k as the bounty and invited him to be their Chief Security Advisor. IMG[**4**] [**5]**

How could it have been prevented?

- By not having the public functions that can be used with 'onlyOwner' permissions on the contract.
- By not having the 'sigHash' data controlled and input by a user.
- By auditing the code in a timely manner.
- By making the security review by security specialists.

Summary of the Attack:

This attack happened is mainly because the keeper of the 'EthCrossChainData' contract can be modified by the 'EthCrossChainManager' contract, and the 'verifyHeaderAndExecuteTx' function of the EthCrossChainManager contract can execute the data passed in by the user through the '_executeCrossChainTx' function. Therefore, the attacker uses this function to pass in carefully constructed data to modify the address specified by the attacker by the keeper of the EthCrossChainData contract. It is not the case that this event occurred due to the leakage of the keeper's private key. At present, with the efforts of many parties, hackers have returned almost everything that he stole one after another. [**17**]

References:

1. News about the Hack:https://www.cnbc.com/2021/08/11/cryptocurrency-theft-hackers-steal-600-million-in-poly-network-hack.html
2. Understanding DeFi-1:https://en.wikipedia.org/wiki/Decentralized_finance
3. Understanding DeFi-2:https://www.investopedia.com/decentralized-finance-defi-5113835
4. https://en.wikipedia.org/wiki/Poly_Network_exploit
5. Poly Network Website: https://poly.network/
6. Poly Network Twitter: https://twitter.com/PolyNetwork2
7. Technical Explanation About The Exploit: https://research.kudelskisecurity.com...
8. Poly Network Exploiter Ethereum Wallet: https://etherscan.io/address/0xc8a65f...
9. Poly Network Exploiter BSC (Binance) Wallet: https://bscscan.com/address/0x0D6e286...
10. Poly Network Exploiter Polygon Wallet: https://polygonscan.com/address/0x5dc...
11. USDT Warning Message In Transaction: https://etherscan.io/tx/0xae2442c5b57...
12. Message To The Attacker: https://etherscan.io/tx/0xbedeb9f2153...
13. Reply From The Attacker: https://etherscan.io/tx/0xea8ffdabd3d...
14. Hacker Starting To Return Funds: https://www.coindesk.com/poly-network...
15. Hacker Continues To Return Funds: https://www.coindesk.com/poly-network...
16. RoadMap of next phase: https://medium.com/poly-network/poly-network-roadmap-for-the-next-phase-9f84c03c2e53
17. The Analysis of the Attack: https://slowmist.medium.com/the-analysis-and-q-a-of-poly-network-being-hacked-8112a35beb39
18. GitHub Code of Poly network: https://github.com/polynetwork/eth-contracts/blob/master/contracts/core/cross_chain_manager/logic/EthCrossChainManager.sol#L91
19. Root Cause: https://slowmist.medium.com/the-root-cause-of-poly-network-being-hacked-ec2ee1b0c68f
20. Offer for attacker: https://twitter.com/PolyNetwork2/status/1427574236483231749
21. Ploy Network twitter account: https://twitter.com/PolyNetwork2

Appendix:

Image-1: Poly Network informing they've been hacked and asking the exchanges to block the hackers' addresses.

Image-2: Poly Network team asking the hacker to return the stolen money,

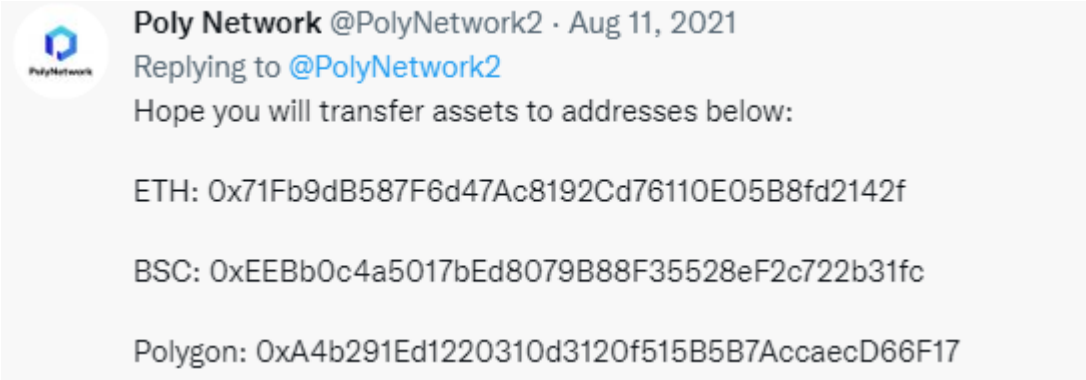


Image-3: Addresses involved in the attack

	Chain	Address
Hacker address	BSC	**Address 1** 0x0d6e286a7cfd25e0c01fee9756765d8033b32c71
	Polygon	**Address 2** 0x5dc3603c9d42ff184153a8a9094a73d461663214
	Ethereum	**Address 3** 0xc8a65fadf0e0ddaf421f28feab69bf6e2e589963
Suspected hacker address	Ethereum	**Address 4** 0xaaf5feaa9e5694b2b293e67558e2da8ea4b1fb13

Image-4: Stolen money was recovered

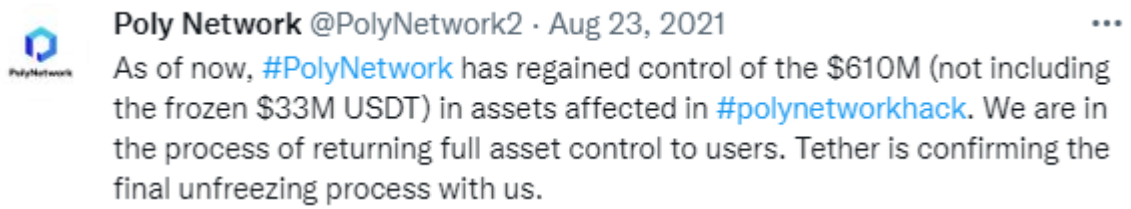


Image5: Poly Network team offered a bounty and job to the hacker