



School: Campus:

Academic Year: Subject Name: Subject Code:

Semester: Program: Branch: Specialization:

Date:

Applied and Action Learning

(Learning by Doing and Discovery)

Name of the Experiment : Security First – Understanding Blockchain Attacks

Objective/Aim:

To understand how validators are selected in the Proof of Stake (PoS) consensus mechanism and how staking influences block creation.

Apparatus/Software Used:

- Laptop
- Microsoft word

Websites:

- BlockApps
- NordLayer
- Apriorit
- LevelBlue
- WeSecureApp

Theory/Concept:

Layer-based Vulnerabilities

- Attackers manipulated the Border Gateway Protocol (BGP) routing on the internet to redirect mining pool traffic. This allowed them to steal mining rewards and disrupt the network. For instance, the 2014 BGP hijack resulted in \$83,000 in stolen cryptocurrency, and in 2022, a BGP hijack on Celer Bridge led to \$235,000 in losses. **Example:** BGP Hijacking (Network Layer)

Consensus Attack Theory

- In this variant of double-spending, the attacker privately mined a block, created two transactions (of different amounts), pushed one to an exchange, and later released the other to the main network. The attack leveraged control over multiple nodes and manipulated the system's consensus process to trick exchanges and steal funds. **Example:** Vector76 Attack (Consensus Layer)

Smart Contract Exploits

- In 2016, attackers exploited a reentrancy bug in the DAO smart contract, recursively calling the withdrawal function before the balance was updated and siphoning over \$50 million in ETH. **Example:** DAO Hack (Contract Layer)

Network-based Attacks

- By rerouting internet traffic, an attacker captured the communication between blockchain nodes, redirecting or partitioning parts of the network, and exploiting this for malicious intent. **Example:** BGP Hijacking (again)

Taxonomy of Attacks

- Researchers have systematically classified attacks by blockchain layers (data, network, consensus, contract, application) and by attacker motivation, strategy, and victim type. For instance, the DAO Hack is categorized as a contract-layer exploit driven by financial motivation, while the Vector76 attack belongs to the consensus/network layer with goals of double-spending. **Example:** Classification and Frameworks

Procedure:

Step 1: Define Scope

Select The DAO hack, a real-world exploit of an Ethereum-based smart contract through a reentrancy vulnerability.

Step 2: Data Collection

- Gather primary code samples (Solidity code of DAO).
- Review blockchain transaction logs for the period of attack.
- Collect post-mortem reports and developer notes.

Step 3: Attack Analysis

- The hacker used a smart contract that interacted with the DAO's withdrawal function.
- By recursively calling the withdraw() function within a fallback function before the contract updated balances, the attacker repeatedly withdrew funds, draining over \$50M in ETH.

Step 4: Technical Breakdown

1. Attacker deposits ETH into DAO contract.
2. Attacker triggers withdrawal from the DAO.
3. The fallback function of attack contract is called before balance is updated.
4. Fallback re-enters DAO withdraw, repeating the process.
5. Funds are drained until contract depleted, only then updating attacker's balance.

Step 5: Validation

- Analyze blockchain for recursive withdrawal patterns.
- Compare balance updates and event logs against contract source code.

Step 6: Outcome and Prevention

- Losses: \$50M+ in ETH.
- Countermeasures: Practices such as updating balances before transfers, code audits, and formal testing of contract logic were implemented after the hack.

Observation Table:

Attack Name	Date	Type	Affected System	Methodology	Impact	Prevention
DAO Attack	2016-06-17	Smart Contract	Ethereum	Reentrancy bug	\$50 million	Hard fork, audits
Poly Hack	2021-08-10	Cross-chain	Poly Network	Contract exploit	\$611 million	Communication, design review
ETC 51% Att.	2020-08	Majority control	Ethereum Classic	Double spending	\$9 million	PoS consensus, delay txns
Finney Att.	Variable	Double Spending	Bitcoin	Hidden block, delay	Transaction loss	Multiple confs

ASSESSMENT

Rubrics	Full Mark	Marks Obtained	Remarks
Concept	10		
Planning and Execution/ Practical Simulation/ Programming	10		
Result and Interpretation	10		
Record of Applied and Action Learning	10		
Viva	10		
Total	50		

Signature of the Student:

Name :
Regn.No.

Signature of the Faculty: