Case Study 2: Report on Binance Hack of October 7, 2022

Team Members

1. **Laasya Vajjala (11848603)**
    a. Introduction and Background Information
    b. Detailed Description of the Hack
    c. Description of the Exploit
    d. Consequences and Impact
2. **Surya Pramod Vadapalli (11861342)**
    a. Analysis of Similar Incidents
    b. Reasons for Targeting Crypto Companies
    c. Countermeasures and Response
    d. Specific Prevention Measures

What is Binance?

Binance is the **world's largest cryptocurrency exchange platform**, facilitating the trading of digital currencies such as **Bitcoin, Ethereum**, **and its own cryptocurrency, Binance Coin (BNB)**. Founded by **Changpeng Zhao in 2017**, Binance quickly rose to prominence by providing a platform for secure, fast, and low-fee trading. Binance also runs the **Binance Smart Chain (BSC)**, **a blockchain platform that enables decentralized finance (DeFi) applications and cross-chain bridges, which connect various blockchain ecosystems.**

Background of security issues

Security in the crypto world has always been a concern, especially due to the decentralized nature of blockchain systems. Cross-chain bridges, which enable the movement of assets across different blockchains, have become significant targets for hackers due to their complex architecture and security vulnerabilities. Vitalik Buterin, Ethereum's founder, has previously expressed concerns about the weaknesses of such systems.

Prior to the October 2022 hack, Binance had experienced multiple security breaches, including a significant hack in 2019 where 7,000 Bitcoins were stolen, costing the company $40 million. Although Binance compensated its customers, the incident highlighted the potential risks in centralized crypto exchanges.

How did the hack happen?

The Binance hack, which occurred on October 7, 2022, targeted the BSC Token Hub, a cross-chain bridge linking the Binance Beacon Chain and the BNB Smart Chain. **The attacker exploited a vulnerability in the bridge's verification system by forging proof for a block**

created two years prior. This allowed the hacker to mint 2 million BNB tokens (approximately $570 million) without stealing existing tokens.

The Binance Bridge vulnerability lay in its failure to completely verify the **Merkle tree, a data structure used in cryptography to secure blockchain data.** The hacker used this flaw to generate forged proofs and mint new BNB tokens directly into their wallet.

What was the root cause?
Introduction to Merkle Trees and Proofs

Merkle trees provide **a way to verify the inclusion of data in a database without disclosing all the data.** This is achieved by **hashing the values in a tree structure where each node is a hash of its children, and the leaf nodes are hashes of the underlying data. The verification process involves comparing a given hash against the root hash of the tree using a set of path nodes—nodes lying on the path from the leaf to the root.**

In a Merkle tree, the data in each node is derived from hashing the concatenated values of its child nodes. For example, if P1 is the parent of nodes P3 and P4, then P1 would be calculated as **P1 = h(P3, P4),** where h is a cryptographic hash function. To verify data in P3, one would hash P3 and use the path nodes P4 and P2 to compute the root hash. **The correctness of this process relies on a consistent ordering of child nodes during concatenation.**

Common ordering in Merkle trees

Typically, the concatenation ordering in Merkle trees involves comparing the hash values of child nodes. **The node with the larger hash value is placed first during concatenation.** For instance, if P3's hash value is greater than P4's, the concatenation would be (P3, P4). **This order is crucial for ensuring the integrity of the root hash.**

IAVL verification
IAVL trees **extend the concept of Merkle trees by introducing additional attributes—left and right attributes—to guide the concatenation of child node hashes.** In an IAVL tree, the right attribute determines the position of a child node during concatenation. For instance, if P4 has a right attribute set to itself, the concatenation for computing P1 would be P1 = H(P3, P4).

The root cause of the exploit lies in the mishandling of these right attributes during the calculation of the root hash. Specifically, the right attribute was not properly considered when computing the root hash, leading to a vulnerability.

How did they exploit it?
The exploit involved manipulating the right attributes in a proof to bypass the root hash verification. The attacker exploited a vulnerability by providing malicious right attributes, which allowed them to pass invalid proofs. This was possible because the proof was **user-controllable, allowing the attacker to introduce malicious data into the tree without invalidating the root hash.**

Emiliano Bonassi's tweet described the exploit's mechanics, where the attacker used proof from an earlier cross-chain transaction and modified it. The process involved unmarshalling the proof, decoding it, and then crafting a new proof with malicious payloads. This new proof was then used to verify against the root hash, producing a valid result despite being malicious.

Proof of Concept

To validate the exploit, the attacker crafted a malicious payload and tested it using the IAVL library. The procedure included:

- Crafting the payload with specific parameters (e.g., token address, amount).
- Modifying the proof by adding new leaves and empty inner nodes.
- Hashing the malicious payload and integrating it into the proof.
- Verifying the new proof against the root hash.
- The successful execution of the PoC indicated that both the legitimate and malicious proofs produced the same root hash and no errors during verification, confirming the validity of the exploit.

This oversight allowed attackers to generate and verify malicious proofs by manipulating the proof structure, ultimately leading to the exploitation of the system. They then began distributing the funds across liquidity pools and different blockchains, including Ethereum, Polygon, Avalanche, and others, to convert the stolen tokens into various assets.

Who was involved?

The hacker responsible, referred to as the "BNB bridge exploiter," remains unidentified. Their method involved registering as a relayer for the Binance Bridge and manipulating verification proofs to exploit the bridge's security vulnerabilities. While no specific individuals or groups have been officially linked to the attack, the sophistication of the breach suggests that the attacker may have had advanced knowledge of blockchain systems and bridge vulnerabilities.

Consequences

The hack resulted in the loss of $570 million worth of BNB tokens. The incident caused the price of BNB to drop by 3.7%. While Binance paused the network to prevent further movement of funds, the hacker quickly moved a portion of the stolen assets into liquidity pools and decentralized exchanges.

Fortunately, swift action from Binance and other cryptocurrency entities, such as Tether and Circle, led to the freezing of approximately $33.5 million of the stolen funds. Despite these efforts, around $45 million remained in censorship-resistant assets on the Ethereum blockchain(Binance Blockchain Hit …).

Losses & is it the first one?

This is not the first significant hack Binance has faced. As mentioned earlier, Binance

experienced a major breach in 2019, where 7,000 Bitcoins were stolen. Although Binance compensated users in both cases, the recurring nature of these incidents demonstrates the ongoing challenges crypto platforms face in securing their systems.

In addition to Binance, other crypto bridges like Nomad, Wormhole, and Ronin have also been targeted in recent years, highlighting a trend where cross-chain bridges are frequently exploited for their vulnerabilities. The Nomad Bridge lost $191 million in August 2022, and the Wormhole Bridge suffered a $320 million hack in February 2022(Binance Blockchain Hit …).

How and why are crypto companies targeted?

Crypto companies are targeted because of the large sums of money they manage, the decentralized nature of their systems, and the innovative yet often untested technology they rely on. Cross-chain bridges, in particular, are frequently targeted because they hold significant amounts of cryptocurrency tokens and rely on complex architectures that can be difficult to secure.

Bridges lock assets on one chain while issuing an equivalent amount on another. The central storage of these locked assets becomes a prime target for exploitation, as seen in the Binance case. Additionally, decentralized finance (DeFi) protocols, which operate without centralized authority, often have slower response times to security incidents, making them even more attractive to attackers.

Countermeasures

In response to the hack, Binance took immediate actions, including:

Suspending the Binance Smart Chain (BSC) to prevent the hacker from moving additional funds.
Freezing funds with the cooperation of other blockchain entities, notably Tether and Circle, which froze $33.5 million in illicit assets.

Governance votes: Binance proposed on-chain governance votes to decide whether to offer a 10% bounty for finding the hacker and setting up a bug bounty program to reward individuals who report vulnerabilities.

What measures were taken?

Binance's response to the attack was decisive. By pausing the BSC network, they were able to limit the hacker's ability to distribute the stolen funds further. Additionally, the freezing of assets on multiple blockchains prevented a significant portion of the funds from being converted or moved(Binance Blockchain Hit …).

Lessons learned & future prevention

If you were an administrator or system designer, there are several lessons to be learned from this breach:

Stronger Verification Mechanisms: The key vulnerability in this hack was the incomplete

verification of the Merkle tree. Ensuring complete validation of cryptographic proofs across all nodes in the network is essential.

Layered Security for Bridges: Cross-chain bridges require robust security protocols. Implementing multiple layers of security checks for asset transfers can prevent similar exploits.

Improved Monitoring Systems: Real-time monitoring and automated responses to unusual activity can help mitigate the impact of an attack. Early detection is crucial in reducing the damage.

Bug Bounty Programs: Offering substantial rewards for identifying vulnerabilities can encourage white-hat hackers to find and report issues before they are exploited by malicious actors.

Specific measures for prevention

Regular Security Audits: Frequent code audits, particularly of critical infrastructure such as cross-chain bridges, can help identify vulnerabilities before they are exploited.

Multi-Signature Wallets: Requiring multiple parties to approve transactions, especially when moving large amounts of funds, can provide an additional layer of security.

Government Regulations: Governments can enforce regulations that require cryptocurrency exchanges and platforms to adhere to strict security standards. Implementing mandatory security frameworks and holding companies accountable for breaches can deter attacks.

Data Storage Methodology: Storing sensitive data in decentralized databases with end-to-end encryption can protect against tampering. Additionally, using secure, verifiable hash functions can prevent malicious manipulation of blockchain records.

Tools and storage methodologies

Secure Multi-Party Computation (SMPC): This can help ensure that sensitive cryptographic operations, like verifying proofs, are done securely without revealing private keys.

Decentralized Identity (DID) Frameworks: Implementing DID frameworks ensures that identities and credentials used within the system remain secure.

Blockchain Analytics Tools: Tools like Chainalysis and Elliptic can help monitor transactions and detect suspicious activity, providing early warning of potential breaches.

In conclusion, the Binance hack was a significant event that exposed vulnerabilities in cross-chain bridges. While Binance responded effectively to mitigate losses, the attack underscores the need for enhanced security protocols and better regulatory oversight in the cryptocurrency industry.

References

1. Binance Blockchain Hit by $570 Million Hack, Exposing Crypto Vulnerabilities.

2. $570M Binance Hack: What Happened & Who Is Responsible?

3. Attack mints $569 million-worth of BNB tokens in BSC bridge exploit.

4. **Immunefi. (2022, October 7). Hack Analysis: Binance Bridge October 2022. Medium.**

5. Security News This Week: Binance Hackers Minted $569M in Crypto—Then It Got Complicated

6. Inside story: We go deep in the Binance Hacker story. [CoinDesk].

7. Binance Bridge hacked for $100M ….Chain halted. (2023) [CryptosRUs].

Image 1 - https://www.reuters.com/technology/binance-billionaire-zhao-crypto-king-who-wants-world-2023-03-28/

Image 2 - https://www.cybavo.com/blog/cybavo-announces-binance-smart-chain-bsc-support/

Script for presentation:

Laasya


BINANCE
Binance Hack of October 7, 2022
Laasya Vajjala, Surya Pramod Vadapalli

Slide 1: Title Slide

Good [morning/afternoon], everyone. Today, we're going to discuss the Binance Hack that occurred on October 7, 2022. My name is [Presenter's Name], and I'll be walking you through the event, the vulnerabilities that led to the breach. This hack **exposed vulnerabilities** in the **infrastructure of Binance** and raised concerns about the **security of cross-chain bridges in the cryptocurrency ecosystem**.

Slide 2: What is Binance?

World's largest cryptocurrency exchange platform,
Bitcoin, Ethereum, **and its own cryptocurrency, Binance Coin (BNB)**.
Changpeng Zhao in 2017,
Binance Smart Chain (BSC), **a blockchain platform that enables decentralized finance (DeFi) applications and cross-chain bridges, which connect various blockchain ecosystems.**

Slide 3: Background on Cross-Chain Bridges

Security concern in crypto- due to its decentralized nature of blockchain systems
Cross chain bridges -movement of assets = targets
BSC Token hub and Merkle tree verification = focus
How it works?

The attacker exploited a vulnerability in the bridge's verification system by forging proof for a block created two years prior. This allowed the hacker to mint 2 million BNB tokens (approximately $570 million) without stealing existing tokens.

Slide 5: The Root Cause: Merkle Tree Verification Failure

Merkle tree, a data structure used in cryptography to secure blockchain data.
Merkle trees provide **a way to verify the data in a database without disclosing all the data.**
The Merkle proof functionality uses a precompiled iavlMerkleProofValidate contract that is written in Go.
The contract uses methods from the Cosmos cross-chain framework to implement the Merkle proof functionality.

hashing the values in a tree structure where each node is a hash of its children, and the leaf

nodes are hashes of the underlying data. The verification process involves comparing a given hash against the root hash of the tree using a set of path nodes—nodes lying on the path from the leaf to the root.
P1 = h(P3, P4),
The correctness of this process relies on a consistent ordering of child nodes during concatenation.
The node with the larger hash value is placed first during concatenation.
This order is crucial for ensuring the integrity of the root hash.

Slide 6: IAVL Verification Issue

IAVL - Immutable AVL Tree, Adlesen-Velsky and Landes
IAVL trees **extend the concept of Merkle trees by introducing additional attributes—left and right attributes—to guide the concatenation of child node hashes.**
The exploit involved manipulating the right attributes in a proof to bypass the root hash verification. The attacker exploited a vulnerability by providing malicious right attributes, which allowed them to pass invalid proofs.
Proof was user-controllable, allowing the attacker to introduce malicious data into the tree without invalidating the root hash.

Root Cause:

The Problem:

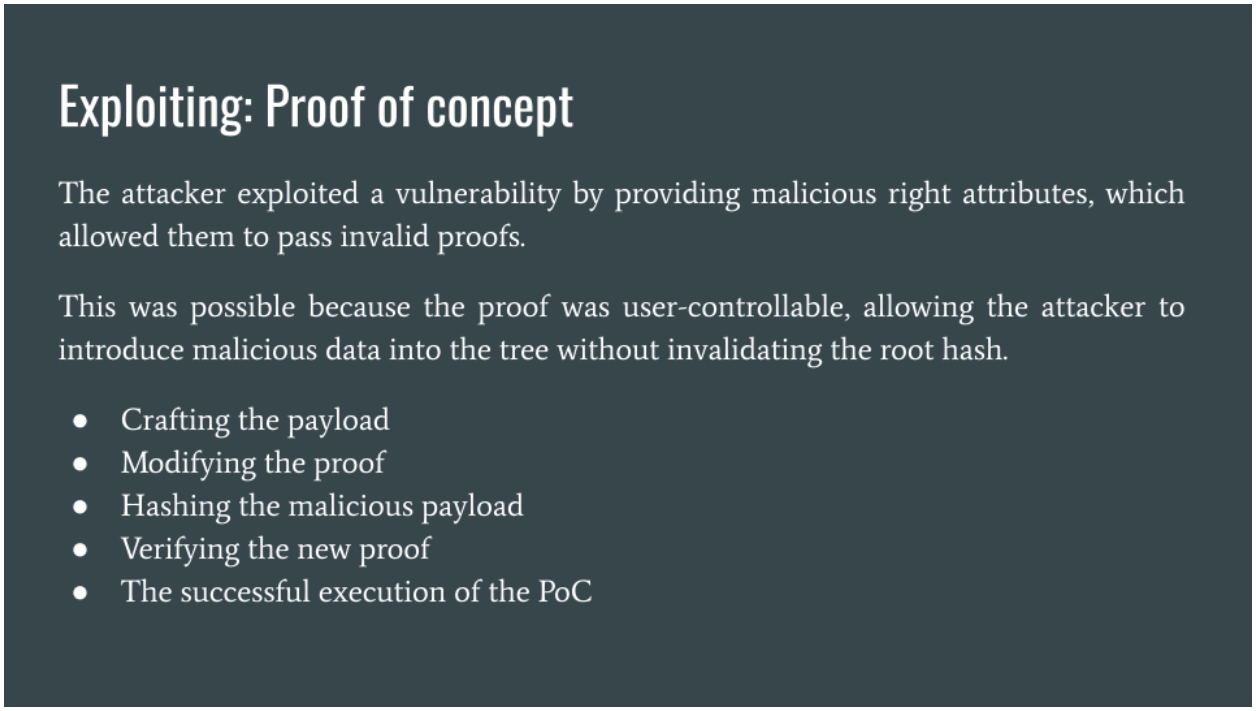
The code only considered one child node (left or right) when calculating the hash for intermediate nodes.

An attacker could exploit this by adding a new leaf node (right child) while keeping the original left child and creating an empty intermediate node.

This manipulation wouldn't change the root hash, allowing the attacker to forge a proof for the new data.

This vulnerability could be used to inject fake data into the system without compromising the root hash.

Surya



Slide 7: Proof of Concept (PoC) Exploitation

After understanding the vulnerability, the attacker crafted a Proof of Concept, or PoC, to demonstrate and exploit the flaw. They did this by crafting malicious payloads, modifying the proof, and successfully hashing it so that the system believed the forged data was valid. The forged proof was then passed through the BSC Token Hub's verification process.

Since the verification process was flawed, the attacker was able to inject fake data without compromising the root hash, thereby minting millions of BNB tokens.

The attacker moved the stolen funds into multiple blockchain ecosystems, including Ethereum, Polygon, Avalanche, Fantom, Optimism, and Arbitrum, in an effort to escape detection and conversion freezes.

Slide 8: Involvement of ‘BNB Bridge Exploiter’

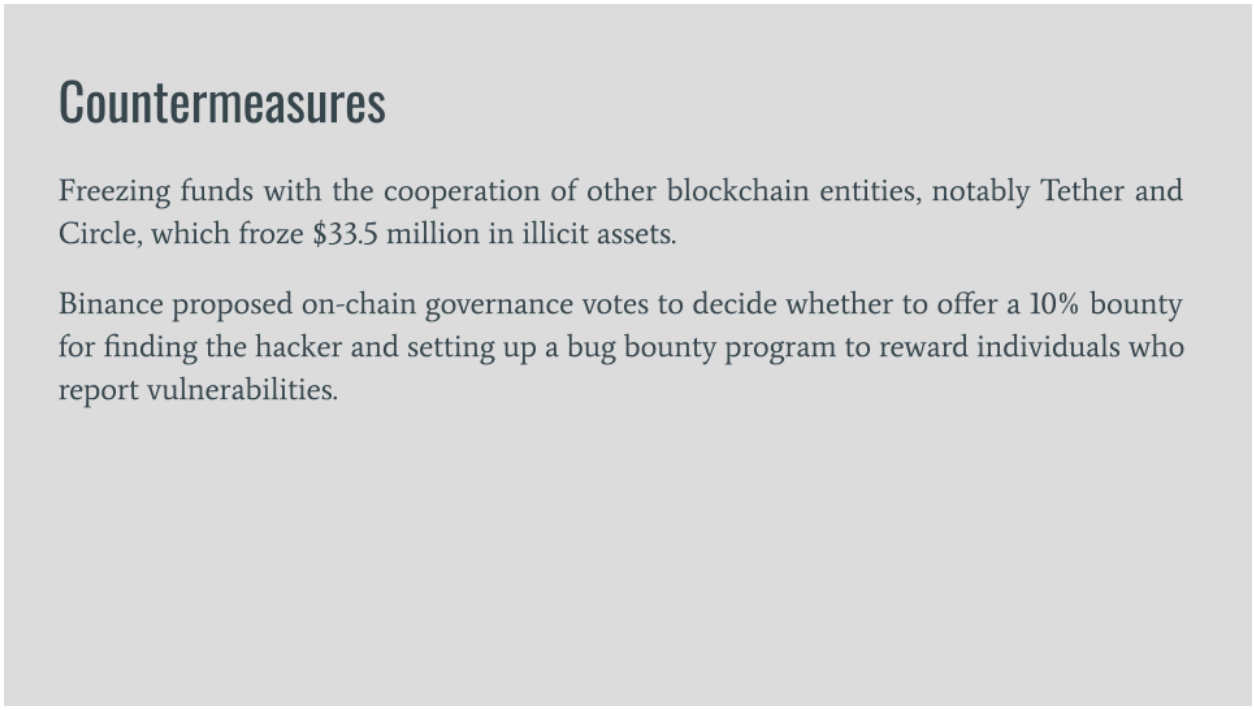
The attacker, dubbed the 'BNB bridge exploiter,' was able to register as a relayer within Binance’s network. This meant they could introduce malicious verification proofs and manipulate the bridge’s security vulnerabilities to their advantage.

This registration as a relayer was key in allowing the attacker to carry out their plan undetected until it was too late.

Slide 8: Impact on Binance and the Cryptocurrency Market

Presenter: "The immediate financial impact of the hack was felt across the Binance ecosystem. The price of Binance's native token, BNB, dropped by around 3.7% following the news. However, this wasn't the first time Binance had faced such a challenge. Back in 2019, Binance was the victim of another significant hack in which over 7,000 Bitcoins were stolen. That attack cost Binance nearly $40 million."

"Cross-chain bridges, like the one exploited in this hack, have increasingly become targets for hackers. For example, the Nomad bridge lost $191 million in a hack in August 2022, and other high-profile breaches have included the Wormhole bridge, Poly Network, and the Ronin bridge."



Slide 10: Countermeasures Taken

Presenter: "Binance, along with other blockchain entities, took swift countermeasures. For example, companies like Tether and Circle froze $33.5 million worth of stolen assets. Binance also proposed on-chain governance votes to decide on offering a 10% bounty to find the hacker and launching a bug bounty program to reward individuals who report vulnerabilities."

"These steps are vital to rebuilding trust within the Binance ecosystem and the broader crypto community."

Slide 7: Binance's Response to the Hack

Presenter: "Once Binance realized what was happening, they responded quickly by suspending the entire BNB Smart Chain to prevent further movement of the stolen funds. This drastic step allowed them to freeze a large portion of the illicit gains. Binance worked closely with other major players in the cryptocurrency space, such as Tether and Circle, which froze $33.5 million worth of assets from the hacker."

"In total, over $350 million worth of stolen assets were rendered inaccessible to the hacker due to a combination of asset freezes and network shutdowns. Although the initial amount stolen was significant, Binance's swift response limited the damage."

Slide 11: Not Binance's First Hack

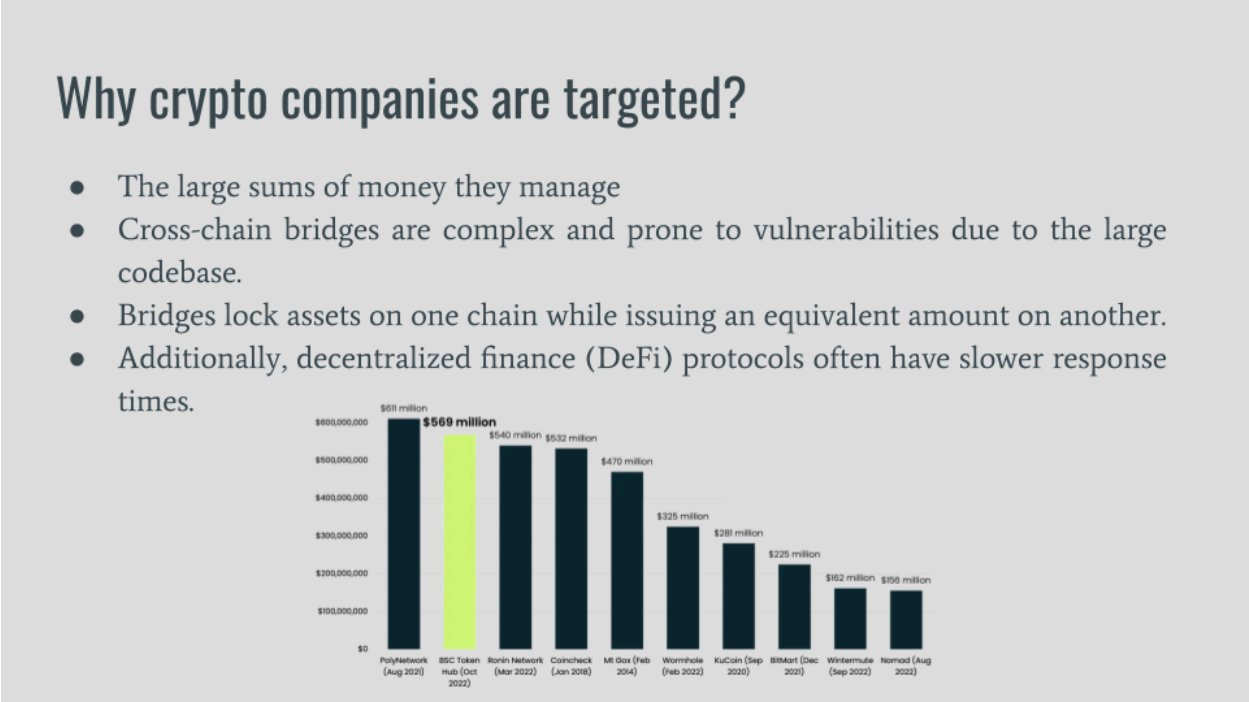
Presenter: "It's important to note that this was not the first major hack Binance had faced. In 2019, the platform lost 7,000 Bitcoins in another high-profile breach. However, Binance has always made it a priority to compensate its users for any losses suffered during these incidents."

"Additionally, cross-chain bridges, like the one exploited here, have often been the target of hackers. Nomad Bridge lost $191 million, and Wormhole Bridge lost $320 million, both in 2022. These attacks reveal the significant security risks inherent in cross-chain bridges."

Slide 9: Actions Binance Proposed

Presenter: "Following the attack, Binance proposed several actions to prevent future incidents. One of the primary proposals was to hold an on-chain governance vote to decide whether to offer a 10% bounty for finding the hacker and returning the stolen funds. This bounty would provide a strong incentive for hackers to either return the funds or help identify vulnerabilities in the system."

"In addition, Binance is considering launching a bug bounty program with rewards of up to $1 million for individuals who report serious bugs in the Binance network. This could go a long way toward making their systems more secure in the future."



Slide 12: Why Crypto Companies Are Targeted

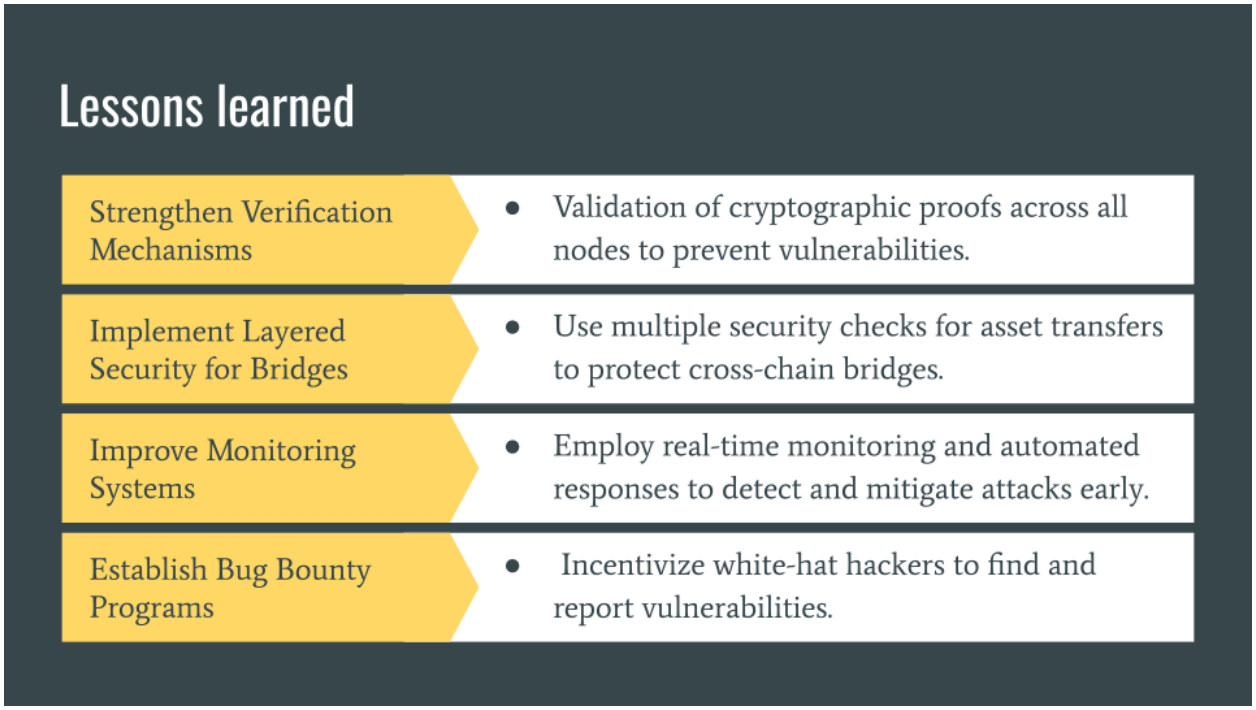
Presenter: "Why are cryptocurrency companies like Binance so frequently targeted? The main reason is the enormous sums of money that flow through these platforms. Cross-chain bridges are especially attractive targets because of their complexity and potential vulnerabilities. Bridges lock assets on one chain while issuing an equivalent amount on another, creating points of weakness."

"Moreover, decentralized finance (DeFi) protocols often have slower response times, making them easier targets for exploitation."

Slide 10: Broader Implications for Cross-Chain Bridges

Presenter: "This attack is part of a larger trend of breaches targeting cross-chain bridges. These bridges have become frequent targets for ultra-high value hacks due to the large sums of money they hold and their relative complexity compared to base-layer blockchain networks. Because cross-chain bridges hold enormous amounts of cryptocurrency tokens, they represent a significant point of vulnerability."

"Not only Binance, but the entire crypto ecosystem, must rethink how cross-chain bridges are designed and secured. There are inherent risks in decentralization, especially when there are delays in responding to attacks like this one. As more bridges connect disparate blockchain networks, the challenge of securing them will only grow."



Slide 13: Lessons Learned

Presenter: "Let's now focus on the lessons we can take away from this attack. First, it's clear that we need to strengthen verification mechanisms. Ensuring the validation of cryptographic proofs across all nodes is crucial to preventing vulnerabilities like the one we saw here."

"Next, we need to implement layered security for cross-chain bridges. This means adding multiple security checks for asset transfers, which could have prevented this exploit. Additionally, improved monitoring systems that allow for real-time alerts and automated responses can help catch and mitigate attacks as they happen."

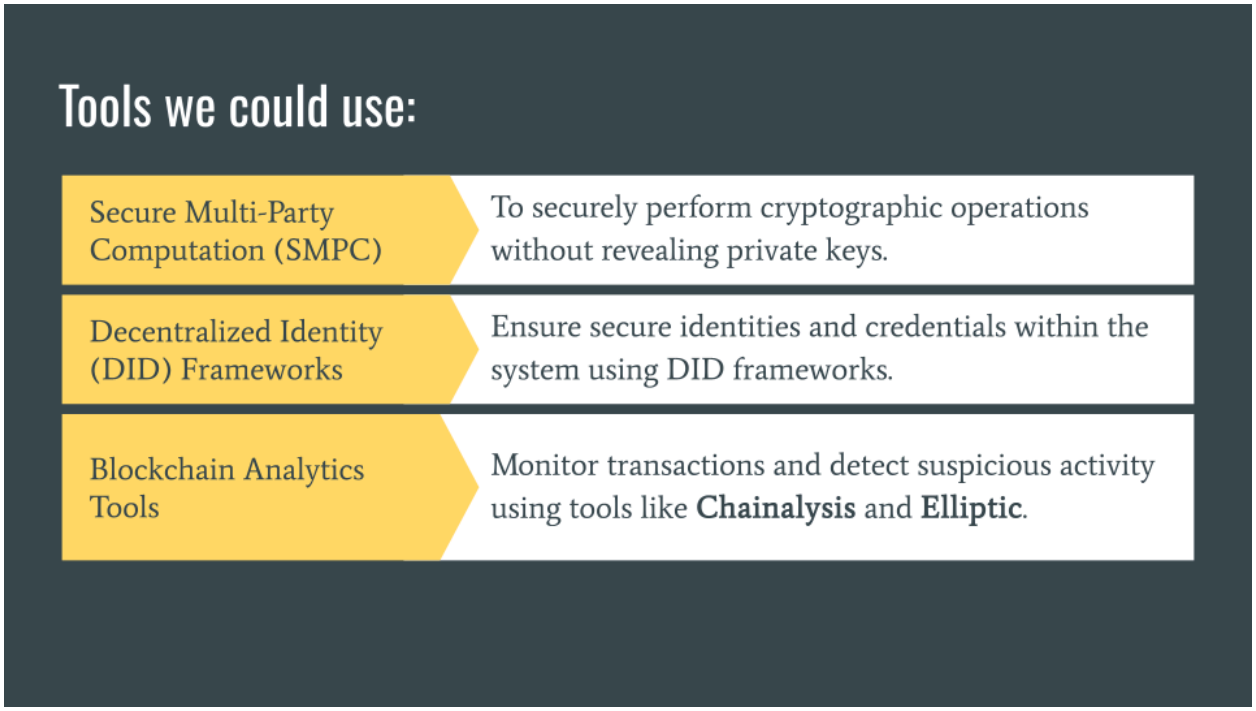
"Lastly, we need to establish robust bug bounty programs. By incentivizing white-hat hackers to find and report vulnerabilities, crypto companies can stay one step ahead of malicious actors."

Slide 11: Lessons Learned

Presenter: "What are the key takeaways from this event? First and foremost, it's crucial that cross-chain bridges are subjected to stronger security measures. Verification mechanisms need to be enhanced to ensure that any data passed through these bridges is fully validated. Had the Binance Smart Chain fully verified the Merkle tree in this case, the hacker might not have been able to forge their proofs."

"Secondly, faster incident response times are necessary. In a decentralized environment like Binance, there can be a delay in halting malicious activity, which gives hackers time to transfer and obscure their stolen funds."

"Lastly, collaboration across the cryptocurrency space is critical. Binance's ability to work with other companies, like Tether and Circle, to freeze assets played a crucial role in minimizing the damage."



Slide 14: Tools We Could Use

Presenter: "There are several tools that could help bolster security in the future. Secure Multi-Party Computation (SMPC) can securely perform cryptographic operations without revealing private keys. Decentralized Identity (DID) frameworks can ensure the secure management of identities and credentials within the system."

"Finally, blockchain analytics tools like Chainalysis and Elliptic can be used to monitor transactions and detect suspicious activity before it leads to large-scale breaches."

Slide 15: Thank You

Presenter: "That concludes our presentation on the Binance Hack of October 7, 2022. Thank you for your attention, and I'd be happy to take any questions you may have."

Slide 12: Closing Remarks

Presenter: "To wrap up, the Binance Hack of October 2022 serves as a stark reminder that no system is invulnerable, no matter how large or established it may be. As the cryptocurrency space continues to grow, security must remain a top priority for all participants, from exchanges to decentralized finance protocols."

"Binance's quick response to this incident was commendable, but the event also highlights the importance of ongoing vigilance, stronger verification protocols, and a collective effort to safeguard assets in the increasingly interconnected world of blockchain technology."

"Thank you for your attention, and I'd be happy to take any questions you may have."