Blockchain Secrets Unmasked: Was this accidental?

I never believed people they said technology disruption could be attacked prone, but by analyzing the facts discovered made me realized its truth. The Security Vulnerability uncovered was like venom from a snake bite. In the rat race we often forget the basics and that leads to disaster. The views expressed in this article are to bring attention of Blockchain Community to build the bullet-proof 'proof-of-concept' technology of the future.

"Don't let fear or insecurity stop you from trying and new things. Believe, work, transform and be kind to others—even if you hate them."—Stacy L

Story Begins…

At 1.30 pm, Mark was playing with his laptop. The keyboard said "Little Slower"… He whispered "Shut up" wait for a movement. I am working on something important.

What happened?

There was a wealthy princess named Bitcoin. She owned a Kingdom of Blockchain. Miners work day and night to mine the treasure called Bitcoin (A digital crypto- Currency). The power of the kingdom was the mining nodes that used the powerful tool (computation power). They spread across the kingdom in a 'decentralized' fashion. Their work was to mine Bitcoin and Mann the security of the kingdom. They used an unbreakable secret known as Hash (the one way function that is reversed to get the original text or value). Record keepers are muscular, tall and heavy built Marshall artistic who preserves the hash and verify the entry and exit of every hash. Integrity is checked and informed to secret agents who update the miners. The Security of was full proof as no one was that powerful to break into it.

Suddenly there was an intruder. What? How did he get in? The Queen was Annoyed. She cancelled the contract with the contractors and court marshaled the Guards.

How can a fake entry be allowed? How can a security be breached?

Here is where Mark comes in…

He created the couple of random transactions and signed using a wrong private key (secret key). Then posted the transaction on Blockchain.info (records all transactions on Blockchain). Wola! Access Granted. In-fact, the website committee and accepted the fake transaction.

The problem was due to ‘zero-confirmation-api (ZCA)’. The transaction includes a script string—a cryptographic proof that you are authorized to spend Cryptocurrency. The wrong key used will list the transactions into a pool of unconfirmed transaction. The system can be tricked that you have an intruder and funds stolen or the other way round that you have received the payment.

The transaction will never get confirmed, but bugs like this could be disastrous. Image someone gave a confirmation of 300 Bitcoin transferred and the other party was tricked to believe it was true. The Cross Site Scripting Error can be exploited by the hackers to gain access of your wallet and root domain server of your domain. This was clear when a security researcher discovered this bug on Blockchain.info

The Systems need to be patched and the codes must be error free to stop attacks on Blockchain based project and networks.

Blockchain technology has enormous potential to bring technology revolution and change the way banking and transaction happening across the globe, data being stored, security being maintained, records were authenticated and much more. Blockchain reduces the transaction cost, increases the privacy, efficiency and impound the seal of trust. One must also keep in mind that a lot of re-engineering is happening in background to disrupt this technology. We need a common community of Block chain enthusiast, researchers, developers, security researchers and intelligence network to build an open culture for sharing threat intelligence and security risk uncovered also means to fix it.

"The pool is more powerful than one."

Blockchain Secrets Blockchain Technology Cybersecurity

1

Prakash Prasad
Author | Blockchain Researcher |