Security vulnerabilities of Digital Currencies and Countermeasures

[1]Navya Davis, [2] Neethu Prabhakaran,
[1] [2] Assistant Professor, Department of Computer Science, IES College of Engineering, Chittilappilly, Thrissur

Abstract*— Crypto currency commonly defined as digital belongings that use cryptography to secure dealings without the need for a central banking authority is rising in popularity and being widely adopted across the globe. The market for crypto-currencies has been incredibly volatile and these peaks and troughs have made crypto currency value a popular media topic. Hackers, too, have taken notice. In a little under a decade, crypto currency has developed from an obscure experiment to one of the hottest topics in both the technology and finance fields. From the time when the emergence of Bitcoin as the first centralised crypto currency in 2009, the industry has exploded and there are more than 1,500 different currencies now existing. We have seen a new sharp rise in crypto-jacking attacks, exploiting the power of victims' computers to mine crypto-currency and alternative currencies also play a major role in ransom ware attacks, being the payment method of choice. Phishing is a key element in these attacks and businesses need to help their employees to spot phishing attacks. Credential theft is a serious driver of cybercrime today. The world over, different kinds of credentials are used by billions daily to authenticate themselves in their physical and digital lives. From physical keys, through tokens and cards, to digital private keys, session cookies, digital certificates, crypto-currency wallets, login and password combinations, all of these types of credentials are vulnerable to attack. This paper deals with the security vulnerabilities related to crypto currencies and the countermeasures to be taken by block chain to keep it safe.

Index Terms—*crypto, cyber-attacks, penetration,*

I. INTRODUCTION

Crypto currency [2] is an electronic money formed with technology controlling its creation and protecting transactions, while hiding the identities of its users. To prevent scam and manipulation, every user of a crypto currency can concurrently record and authenticate their own dealings and the transactions of everyone else. The digital transaction recordings -"ledger" is publicly available to anyone, so with this public ledger, transactions become efficient, lasting, protected and translucent. The digital transactions have the following possessions as it is Irreversible, Pseudonymous, and Permissionless [3]. Many MNC's decided to implement block chain technologies in their information security solutions as because block chain technologies can be especially useful for securing sensitive records. In addition to securing information, block chain technologies can be used to eliminate the need for using passwords.Blockchain takes responsibility for strong authentication, resolving the single point of attack at the same time. Also, the decentralized network helps us to provide consensus between parties for their identification [4]. In the year of 2010, 2011, 2014, 2016, 2017&2018 are some of the most significant and most devastating crypto currency hacks in history, estimates that cyber criminals have stolen over 980,000 Bitcoins from exchanges since 2011. Today, those stolen coins would be worth more than $6 billion—and that's before you even consider all the other altcoins that have also been victim to hackers [5]. The safety of crypto currencies is one of the main advantages of the block chain technology; but there can be nothing perfect. The safety principle is based on that the contract information is confirmed by other network funders, who are not familiar with each other; it is used by the hackers, to capture the transaction information [6].

II. TECHNICAL APPROACH

A. Types of attack

51% attack, Sybil attack, Double-Spend attack, DDoS attacks are the major types of attacks in digital currencies. A distributed denial-of-service (DDoS) attack is the primary methods of distraction in the modern Internet, by overloading a target with mock traffic. The popularity and importance of crypto currencies makes them a prime target for attack. The most prominent volume of DDoS traffic originated from SSDP amplification attacks, NTP amplification attacks, and application layer attacks. A Sybil attack is an attempt to control a peer network by creating multiple bogus identities. To outside spectators, these bogus identities appear to be sole users. However, unobtrusively, a single entity controls many identities at once, as a result, entity can stimulus the network through additional voting power in a democratic network, or echo chamber messaging in a social network. Selfish mining misuses Bit coin's forks mechanism to derive a selective reward. A fork can arise when at least two cryptographic solutions (blocks) are propagated in a round. This may occur when solutions are concealed almost simultaneously, and take time to promulgate through the Bit coin network. Only one branch of a fork can be valid others are ultimately nullified. In selfish mining, an attacker does not transmit a block immediately, but spawns forks intentionally by propagating a block selectively only when another honest miner creates a block. The attacker can earn a greater compensation by nullifying honest miners' blocks if he has enough computational power. In a Block Withholding (BWH) attack, a miner in a pool submits only PPoWs, but not FPoWs. When an attacker liftoffs a BWH attack against a single pool and conducts honest mining with the rest of her computational power, he earns an extra reward, while the target pool takes a loss. All pools are still vulnerable to this attack because no

efficient and cheap defense has emerged, despite of ongoing exploration. When two pools attack each other, both will take a loss in equilibrium. Currently, pools implicitly agree not to launch BWH attacks against each other because it would harm everyone. FAW attack, which combines a BWH attack with intentional forks. FAW attack is always profitable regardless of an attacker's computational power or network connection state. The FAW attack delivers superior rewards compared to the BWH attack.

B. Attack Models

An attacker can be an unaccompanied miner, or the manager of a closed or open mining pool. Second, the attacker can launch Sybil attacks i.e., the attacker can generate an arbitrary number of identities and join multiple open pools with different IDs and Bitcoin accounts. However, the attacker cannot join closed pools since those require private information. Third, the computational power of an attacker is finite, and he can distribute it into any fraction for both blameless mining and penetration mining. If a mugger is the manager of an open pool, his penetration mining power should be loyal mining power. Finally, the rushing enemy can plant many Sybil nodes in the Bitcoin network, which can simply listen to the propagation of valid blocks and propagate the attacker's block preferentially when the attacker's block and another block are released simultaneously. By this means, the attacker can track the propagation of other blocks and propagate his own as fast as possible using Sybil nodes, these nodes require very little computational power because their role is only to listen and propagate a block; thus planting Sybil nodes involves negligible computation cost for the mugger. One target pool considering an attacker, who targets one open pool, the FAW attack proceeds as follows, first, an attacker conducts both blameless and penetration mining by distributing her computational power to join the target pool. If the attacker finds an FPoW through blameless mining, he transmits it and earns a authentic profit. However, if the attacker finds an FPoW in the target pool, he does not submit it immediately. There are three possible paths the mugger can take. 1) When he notices that other miners, not participating in the target pool, propagate a valid block, he immediately submits his FPoW to the manager of the target pool, who propagates his FPoW to other Bitcoin nodes, generating a fork in the Bitcoin network. 2) When an honest miner in the target pool finds an FPoW, the attacker discards her FPoW. 3) When he finds another FPoW through innocent mining, he discards the FPoW generated by penetration mining.

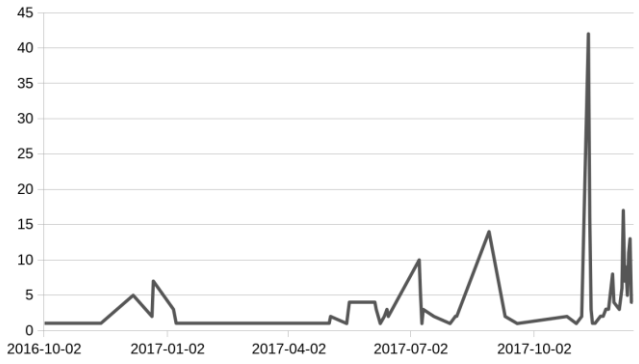

Fig .1

Fig 1, Graph showing the number of potential application layer attacks targeting popular crypto currency web properties through mid-December 2017.

In a web-based crypto-mining attack, the victim's browser is used to mine crypto currencies once the victim visits an infected web site. Conventional web-based crypto-mining attacks are largely dependent on watering hole attacks. In this scenario, the attacker identifies a busy web server with high volumes of web traffic and exploits it to install crypto-mining JavaScript code as a servlet. Once the victim visits the compromised server, the crypto-mining JavaScript code runs in the client's browser and starts to mine crypto currencies. This attack scenario was observed on reputed e-commerce platforms such as ShowTime, YouTube and even on The Pirate Bay. Browser-based crypto-mining has of late drastically risen as evidenced by web search interests from major search engines. The attacker breaches the security of the core components of web technology. Upon breaching the security state of these components, he is able to mine crypto currency from the victim. Because mining of a crypto currency is processor-specific, the attacker mines, which is mineable on general-purpose CPUs. Each breach is defined either as a breach of confidentiality, integrity or availability. The attacker first identifies target hosts which could reside in a WLAN or LAN, because the attack is of the MITM class, the attacker likewise identifies the network's gateway through which all traffic leaves the subnet. Having the IP address of the default gateway and a list of targeted hosts, he executes IP address spoofing via ARP poisoning. This is the first stage of the attack designated as the reconnaissance phase in the attack model

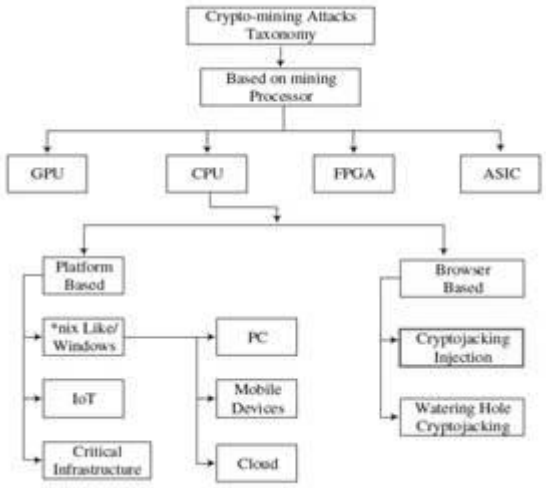

Fig .2 Taxonomy of crypto-mining attacks

C. Comprehensive measurement for Privacy

To protect privacy, the block chain needs to following requirements, a) the links between transactions should invisible or discoverable, b) the content of transactions is only known to their participants. However, in the case of a public setting, everyone can have access to the block chain with no restrictions, the privacy requirements should be considered on the following two factors: a) Identity Privacy: means intractability between the transaction scripts and the real identities of their participants, as well as the contract relationships between users. Even if users apply pseudonyms when stand-in in the block chain, only provide limited identity privacy. By monitoring the unencrypted network and traversal through the public block chain, some behavioral analysis strategies may reveal some information about who is using blockchain.b) Transaction Privacy, means that the contract contents can only be accessed by specified users, and kept unknown to the public block chain network. Transaction privacy is desired in many block chain-based applications where users may request for increased levels of privacy and

avoid revealing their sensitive information to any curious block chain entities. A homomorphic cryptosystem (HC) supports a cryptographic methodology that satisfies homomorphism so as to preserve arithmetic operations carried out on cipher texts. Homomorphic cryptography performs as black box, when given '*n'* cipher texts and operations; it outputs the encrypted result of the same operations on the corresponding original data.

Phishing will continue to be the primary method to deliver malware of all types. Employee training won't help with auto-executing crypto jacking from visiting legitimate websites. Crypto jacking scripts are often delivered through web ads, installing an ad blocker can be an effective means of stopping them. Use endpoint protection that is capable of detecting known crypto miners. Many of the endpoint protection/antivirus software vendors have added crypto miner detection to their products. Keep web filtering tools up to date.

Short-term measures

Increase the diversity of node connections the more connected an AS level is, the harder it is to attack it. Observe that even single-homed Bit coin nodes could benefit from extra connectivity by using one or more VPN services through encrypted tunnels so that Bit coin traffic to and from the node go through multiple and distinct ASes. Attackers that wish to deny connectivity through the tunnel would need to either know both associated IP addresses or, alternatively, disrupt all encrypted traffic to and from nodes— making the attack highly noticeable. By monitoring the RTT towards its peers, a node could detect sudden changes and establish extra random connections as a protection mechanism. While inferring the topology, many pools were using gateways in the same AS. Hosting these gateways in different ASes would make them even more robust to routing attacks.

Longer-term measures

Using a Message Authentication Code (MAC) to validate that the content of each message has not been changed would make delay attacks much more difficult. Use randomized TCP port as it will force the AS-level adversary to maintain state to keep track of these ports. In addition to TCP connections, bit coin clients could periodically send UDP messages with corroborating data. These UDP messages can be used as a heartbeat that will allow nodes to discover that their connection was partially intercepted. As UDP messages do not rely on return traffic, this would enable node to realize that they are out-of-sync and establish new connections.

The security of bit coin from network-based attacks has been relatively less explored compared to other attack scenarios, so other security measures will only arises when new attacks reported and on analyses on it.

III. HELPFUL HINTS

Abbreviations and Acronyms

TCP - Transmission Control Protocol
UDP - User Datagram Protocol
RTT - Round-Trip Time
VPN - Virtual Private Network
FPoW - Full Proofs of Work
MITM - Man-in-the-Middle attack
FAW - Fork After Withholding
SSDP - Simple Service Discovery Protocol
NTP - Network Time Protocol

CONCLUSION

This paper presented the vulnerabilities and security measures to be taken in the crypto currency system from a security analyst viewpoint. We carry out and measured some anomalies in the bit coin protocol that increase the risk of a block chain fork. The incitement of the problem however is deep-down to the way information is propagated in the network. We reviews a comprehensive analysis of crypto currency protection mechanisms in terms of both anonymity and transaction privacy. We believe close by and thorough collaborative ties between research analysts and finance experts can help to address this issue. We have observed that existing research is focused on preventive and detective countermeasures and significant research is needed on developing investigative countermeasures, which are equally important for defense against data exfiltration attacks.

REFERENCES

[1] Nicholas Roth, an Architectural Assessment of Bitcoin Using the Systems Modeling Language 2015 Conference on Systems Engineering Research, Procedia Computer Science 44 (2015) 527 – 536
[2] https://decryptionary.com/what-is-cryptocurrency/introduction-to-cryptocurrency/
[3] https://blockgeeks.com/guides/what-is-cryptocurrency/
[4] https://resources.infosecinstitute.com/future-information-security/
[5] https://blocksdecoded.com/cryptocurrency-hacks/
[6] https://www.liteforex.com/blog/for-investors/cryptocurrency-attacks-types-of-vulnerabilities-risks-and-results/
[7] Yujin Kwon, Dohyun Kim, Yunmok Son,,Be Selfish and Avoid Dilemmas: Fork After Withholding (FAW) Attacks on Bitcoin,CCS'17, October 30-November 3, 2017, Dallas, TX, USA
[8] https://www.cloudflare.com/learning/ddos/cryptocurrency-ddos-attacks/
[9] Christian Decker, Roger Wattenhofer,Information Propagation in the Bitcoin Network,13-th IEEE International Conference on Peer-to-Peer Computing
[10] Aaron Zimba, Zhaoshun Wang & Mwenge Mulenga (2019) Crypto jacking injection: A paradigm shift to crypto currency-based web-centric internet attacks, Journal of Organizational Computing and Electronic Commerce, 29:1, 40-59
[11] Qi Feng, Debiao He, Sherali Zeadally, Muhammad Khurram Khan, Neeraj Kumar,A Survey on Privacy Protection in Blockchain System,Journal of Network and Computer Applications (2018)
[12] Faheem Ullah, Matthew Edwards, Rajiv Ramdhany, Ruzanna Chitchyan, M. Ali Babar, Awais Rashid,Data Exfiltration: A Review of External Attack Vectors and Countermeasures, Journal of Network and Computer Applications
[13] https://www.csoonline.com/article/3253572/what-is-cryptojacking-how-to-prevent-detect-and-recover-from-it.html
[14] Maria Apostolaki,Aviv Zohar,Laurent VanbeverHijacking Bitcoin: Routing Attacks on Cryptocurrencies,Security and Privacy (SP), 2017 IEEE Symposium