A PROPOSED CYBERSECURITY MODEL FOR CRYPTOCURRENCY EXCHANGES

Himani Gottipati
hgottipa@student.concordia.ab.ca

Primary research advisor: Dr. Shaun Aghili
shaun.aghili@concordia.ab.ca

Secondary research advisor: Dr. Pavol Zavarsky
pavol.zavarsky@concordia.ab.ca

A Project

Submitted to the Faculty of Graduate Studies,
Concordia University of Edmonton

in Partial Fulfillment of the
Requirements for the Final
Research Project for the Degree

MASTER OF INFORMATION SYSTEMS SECURITY MANAGEMENT

Concordia University of Edmonton

FACULTY OF GRADUATE STUDIES

Edmonton, Alberta

April 2020

A PROPOSED CYBERSECURITY MODEL FOR CRYPTOCURRENCY EXCHANGES

Himani Gottipati

Approved:

Shaun Aghili [Original Approval on File]

Shaun Aghili Date: April 20, 2020

Primary Supervisor

Edgar Schmidt [Original Approval on File]

Edgar Schmidt, DSocSci Date: April 20, 2020

Dean, Faculty of Graduate Studies

Abstract

There are various cryptocurrency exchanges which are accessible from all over the world. Due to the uptrend in cryptocurrency, interest in cryptocurrency seems to be increasing. Although cryptocurrency exchanges involve blockchain technology, it is ineffective in the management of security to cryptocurrency and wallets. The most common way for a novice user to handle cryptocurrency trading is through cryptocurrency exchanges. Users have insufficient knowledge of cryptocurrency trading and are prone to cyber-attacks. Due to the tremendous increase and popularity of cryptocurrency, antagonists make illegal attempts to gain the cryptocurrency. Therefore, this paper analyses the vulnerabilities and attacks that happened on exchanges and wallets between the years 2016 and 2019. Furthermore, this paper suggests the relevant security tools and techniques such as Runtime application self-protection (RASP) and Hardware security module (HSM) that secure the cryptocurrency exchanges and their wallets. Additionally, an incident response plan will be developed using an international standard like NIST. And OWASP web security testing guide has also been provided as best practices for exchange website testing to handle the existing application vulnerabilities.

Keywords: Cryptocurrency, cryptocurrency exchange, security threats, thefts, DDoS, cybersecurity, web application security, RASP, WAF, HSM.

A PROPOSED CYBERSECURITY MODEL FOR CRYPTOCURRENCY EXCHANGES

According to Hao, Chang, Lu, & Zhang (2018), there has been significant growth in the cryptocurrency industry over the previous years, with exchanges being the most common one. Within the virtual currency marketplace, a cryptocurrency exchange is a platform that enables the conversion of cryptocurrency to fiat money and vice-versa as well as the conversion between various cryptocurrencies. Many countries are beginning to introduce regulatory requirements for crypto-exchanges However, cryptocurrency exchanges are constantly being hacked. There have been many serious discussions on security-related issues on exchanges and it is one of the biggest concerns for cryptocurrency investors (Hao, Chang, Lu, & Zhang, 2018). An attempt is, however, made in this research to establish its risk factors, and to analyze how these risks may be managed.

Cryptocurrencies were started around more than a decade ago. Eitzman (2019) concluded that several exchanges and their services across the world experienced many breaches and thefts in recent years. This resulted in significant financial losses and closures in some cases. For instance, Binance, the global cryptocurrency exchange founded in 2017, lost more than $40 million in crypto assets. The lost funds were moved to hacker's wallet in a single transaction due to cyberattack by hackers using a combination of phishing, malware and other attack vectors (Wood, 2019). Similarly, the January 2018 breach of the Japanese crypto-exchange, Coincheck has lost $533 million in NEM coin, shutting operations down.

This research paper ascertains the security features of some cryptocurrency exchanges. As the global crypto exchange market continues to face an increasing number of

security breaches. Throughout the first six months of 2019, several crypto exchanges have seen a large-scale financial loss due to the hacking attacks (Young, 2019).

Crypto exchanges face two major types of security risks. The first risk is targeting the users' and administrators' accounts directly through simple account takeover via some techniques like brute force using the stolen passwords from databases or through phishing attacks. These techniques are straightforward and enough for a hacker to steal sensitive data and crypto-assets. The second is attacks on the exchange platform itself. The hackers look for vulnerabilities or misconfigurations in the application and infrastructure. These vulnerabilities like cookie poisoning or injections can be very damaging, as they can leak sensitive data and harm the business.

According to the CipherTrace Anti-money laundering report (2019), attackers stole more than $1.2 billion just in the first quarter of 2019 from various cryptocurrency exchanges. Cybercriminals have developed ingenious new techniques to drain millions of dollars from users' hot wallets in the exchanges. As such, cryptocurrency exchanges face great financial and reputational risks if proper security tools and techniques are not implemented to help reduce similar future security breaches.

The focus of this proposed study is to conduct a root cause analysis into several major cryptocurrency exchange breaches to determine the protocols and control failures that gave rise to such security incidents. The proposed research study will then aim at proposing a cybersecurity model with some security tools and best practices to enhance security in exchanges and wallets that would help to mitigate similar future incidents.

The following sections of the paper are organized as follows. In the Literature Review section, the paper presented a brief overview of cryptocurrency exchanges including

the description of its major components, the vulnerabilities and security threats towards the use of exchanges and hot wallets, and the evaluation of security features of some crypto exchanges In the methodology section, the scope, limitations, questions, and procedure of the study are discussed. A cybersecurity model with additional security tools and best practices for cryptocurrency exchanges have been proposed in the Presentation & Discussion of the results section. In Conclusion & Recommendations section, the paper presents a summary of the observations and provides recommendations for future studies.

LITERATURE REVIEW

CRYPTOCURRENCY OVERVIEW

Digital currency is a web-based mechanism of trade that uses cryptographic functions for financial transactions. Cryptocurrencies implement blockchain technology to gain decentralization, transparency, anonymity, and immutability.

Cryptocurrencies can be exchanged between two users using the public and private keys. These transfers are possible only with a transaction fee, which is less when compared to traditional financial institutions (Conti, Kumar, Lal, & Ruj, 2018).

CRYPTOCURRENCY EXCHANGES

Within the virtual market, a cryptocurrency exchange is a platform that allows users to convert different cryptocurrencies pairs. Firstly, a novel user to make P2P transactions must find a cryptocurrency exchange to exchange their coins (cryptocurrency). A user can make transactions by using public and private keys at the cryptocurrency exchange. Each exchange also offers an electronic wallet to store user credentials (Kim & Lee, 2018).

Due to the lack of expertise on cryptocurrency tradings and security policies of each exchange, users depend on these cryptocurrency exchanges. Because of the lack of

awareness on the usability of cryptocurrencies, users in the exchanges are experiencing major breaches and thefts.

CENTRALIZED EXCHANGE

A centralized exchange is an online service allowing users to buy, sell, and store cryptocurrency. These services are generally facilitated on web servers simply as a conventional bank site does. Exchanges provide virtual wallets to their users to store their cryptocurrency.

Most of the people choose to use these centralized exchanges as they operate similar to normal banks. Some of these exchanges allow trading of cryptocurrency just similar to how the stocks are traded. Coinbase and CoinJar are the most popular centralized exchanges. Currently, most of the cryptocurrency transactions are being carried out on centralized exchanges. The centralized exchanges provide quick transactions and support multiple cryptocurrencies on the same platform (Coincasso, 2019).

DECENTRALIZED EXCHANGE

Many cryptocurrency exchanges are misinterpreted as decentralized ones, but they are, centralized. The decentralized exchanges are cryptocurrency exchanges that are independent of intermediaries. Funds are stored and transactions also happen on the blockchain. Trading is automated and peer-to-peer (P2P). The server will only be controlled and centralized as obvious, but the exchanges are not. These decentralized exchanges are not supported by any company though it is designed to protect the funds from being stolen and users have complete control over their funds (Coincasso, 2019). In centralized exchanges, users rely on exchanges, while on decentralized exchanges, users rely on a digital signature.

DEX does not store any private information of the user and is a bit slower when compared to centralized.

However, most customers follow traditional practices like using centralized exchanges to make transactions. And the platform will make the payment process easy without involving blockchain. Users neglected decentralized exchanges for speed, ease, and accessibility. This approach made centralized exchanges to bring the advantage of instant transaction confirmation and good user experience (Hu, Lee, & Lam, 2019).

How do Centralized Exchanges work?

When users send cryptocurrency from one wallet to another, this means that there is no transmission of coins outside the exchange. So, this transaction will appear on the exchange itself by updating the database with the up-to-date transactions and balances. But will not be updated in the blockchain. The only time the blockchain will be updated is when users withdraw or deposit coins into the exchange. This is because if the user makes a transaction and if it should be included in the blockchain then it takes a lot of time even days to verify, validate and confirm the transaction.

Simply put, once you send cryptocurrency to your wallet inside an exchange, you are essentially sending your cryptocurrency to the exchange. The exchange internally bookkeeps all transactions in a centralized backend and when you cash out, they pay you back using the exchange's wallet address. Only these deposits and withdrawals appear on the blockchain (Stephenson, 2019).

WALLETS

One of the major concepts of cryptocurrency is a wallet that stores the bitcoins. But in fact, all necessary information like public keys, private keys, and details of the

transactions to send or receive bitcoins are stored in the wallet and not the cryptocurrencies. So, one can describe the bitcoin wallet as a software or hardware that stores the credentials of the user. It allows the user to manage the coins like accessing and spending (Dikshit & Singh, 2017).

HOT & COLD STORAGE

The difference between the hot and cold wallets is the creation and storage of private keys. So, the cold wallet is defined as private keys created on a device that never has access to the internet, also stored and used on the same device. Whereas, a hot wallet is a wallet that is connected to the internet. The concept behind the separation of the category is just the idea that wallets having access to the internet have chances of compromise (Padro, 2015). This does not mean that the cold wallet is completely safe, but it has a higher level of security on the cold storage. *Most of the exchanges store cryptocurrency in hot wallets for faster transactions that lead to thefts.* Finally, for spending the funds from cold storage, private keys should be loaded from the device to either online or offline wallets.

VIRTUAL MARKETS INTEGRITY INITIATIVES

The New York State Office of the Attorney General (the "OAG") introduced the Virtual Markets Integrity Initiative to ensure and illuminate New York occupants who exchange virtual or "crypto" money. In terms of exchange, virtual cash is complex and developing quickly. The OAG's Initiative, in any case, continues from a central guideline: buyers and speculators have the right to know about the functioning of their exchanges, secure client information, assets, and guarantee the reliability of transactions (Underwood, 2018). The OAG report included the following sections:

ONBOARDING REQUIREMENTS OF CRYPTO-EXCHANGES

Most exchange platforms try to permit just users from approved areas to get to their websites and to avoid users that do money laundering, asset manipulation, and other violations. this report also confirms that exchanges, to maintain fairness and ensure the integrity of their market, effective systems to verify and monitor the identity and location of users should be there to block unauthorized access to the website. So, customers should also be cautious about the onboarding requirements of the exchanges.

Each exchange implements the KYC program in different ways to confirm a new user's identity before allowing them to access certain trading. This OAG figured out that some crypto exchange platforms differ significantly in their identity management and website access policies. The platforms expect users to present any government-issued IDs for permitting users to trade. Few exchanges like Bitfinex and Tidex don't opt this KYC. The OAG conducted this survey on several exchanges and this paper mentions a few. The table 1 below reflects the onboarding requirements for all users/customers.

Table 1

Onboarding requirements for customers reported in the virtual market report (Underwood, 2018)

	E_1	E_2	E_3	E_4	E_5	E_6	E_7	E_8	E_9	E_{10}
Username	●	●	●	●	●	●	●	●	●	●
Address of user	●	●	●	●	●	●	●	●	●	
Proof of address	●	●	●	●						
State/country of residence	●			●	●				●	
Email	●	●	●	●	●	●	●	●	●	●
Mobile number	●	●	●	●	●	●			●	●
DOB		●	●	●	●	●		●		

Nationality			●							
SSN		●		●	●	●		●	●	
Last 4 SSN										
Government-issued ID	●	●	●	●	●	●		●	●	
Photo of face				●						
Banking information	●									
Occupation					●					
Employment information					●					

Note: The onboarding conditions of some of the crypto-exchanges for customers. Each of these exchanges is represented as E1 to E10

MEASURES FOR RESTRICTING UNAUTHORIZED ACCESS TO THE EXCHANGE'S PLATFORM

Online platforms normally utilize a few techniques to restrict their access. One regular safety measure is to screen IP addresses. Any computer connected to the internet will be assigned with a unique identifier called IP address. This allows the monitoring of the computers that are connected to its website. With different users, observing the user IP addresses permits the website administrator to find the geographic area of clients and trace their suspicious activities originating from a specific PC connection. Users try to cover their IP addresses by utilizing the virtual private network (i.e., VPNs) to restrict the monitoring of their computers. The VPNs cover the details like the user's area of login. For effective security results, the exchanges should incorporate enough steps to unmask and block or restrict access to those users connecting through VPNs (Underwood, 2018). The existing measures for restricting unauthorized access to platforms has been presented in table 2 below:

Table 2

Restricting unauthorized access to exchange platforms

EXCHANGE PLATFORM	COMPUTER IP ADDRESS TRACKING	BLOCKING ACCESS via VPN IP ADDRESS
E1	Yes	No
E2	Yes	No
E3	Yes	Yes
E4	Yes	No
E5	Yes	No
E6	Yes	No
E7	Yes	No
E8	Yes	No
E9	Yes	Yes
E10	Yes	No

Note: While most of the exchanges reported OAG that they track the computer IP addresses. However, only a few exchanges block VPN access. This raises the question about the ability of other platforms that do not block VPN access to restrict access to authorized users only.

AUTOMATIC TRADING POLICIES

Several abusive trading practices can be achieved through computer-automated or "bot" trading strategies. The submission of too many illegitimate transactions could impact the price of the cryptocurrency. Multiple traders or a single could use multiple accounts at the same time to manipulate prices. This is allowed by unsecured automated activities.

To have a clear idea of these risks, the OAG surveyed some of the exchanges if they allow automated trading, about their policies or procedures related to trading. some exchanges reported as mentioned in table 3. However, various exchanges accepted that they do not have any policies or procedures in place for automated trading. while some reported that the user's trading activities are monitored. others claimed their limiting of message rates and blocking of excessive trades that are made in a little timeframe (Underwood, 2018).

Table 3

Automatic trading strategies of some exchanges

Exchange platform	Automated trading policy	Message rate limits	Monitoring small orders
E_1	No	Yes	No
E_2	Yes	Yes	Yes
E_3	No	Yes	No
E_4	No	Yes	No
E_5	Yes	Yes	No
E_6	Yes	Yes	Yes
E_7	No	Yes	No
E_8	No	No	No
E_9	No	Yes	No
E_{10}	No	Yes	No

Note: Some of the exchanges reported OAG about the automatic trading strategies they opted for.

EXCHANGE SECURITY REPORT

In an exchange security report generated by ICORATING in 2018, some exchanges whose daily trading value exceeded $100,000 were selected and compared on different parameters under four classifications as follows:

- User Account Security: 4 parameters analyzed
- Registrar and Domain Security: 4 parameters analyzed
- Web Security: 10 parameters analyzed
- DoS attack protection: 1 parameter analyzed

Table 4

Exchange security report generated by icorating

Name	User Account Security	Registrar & Domain Security	Web Security	DoS Attack Protection
E_1	4/4	3/4	7/10	1/1
E_2	4/4	3/4	8/10	1/1
E_3	2/4	1.5/4	9/10	0/1
E_4	3.5/4	2.5/4	4.33/10	1/1

E_5	3.5/4	2.5/4	4/10	1/1
E_6	3/4	2.5/4	7/10	1/1
E_7	4/4	2.5/4	8/10	1/1
E_8	3/4	1.5/4	9/10	0/1
E_9	4/4	1.5/4	6.3/10	1/1
E_{10}	4/4	2/4	6.75/10	0/1
E_{11}	4/4	2.5/4	6/10	0/1
E_{12}	4/4	2/4	8/10	1/1
E_{13}	3/4	2.5/4	8.5/10	1/1
E_{14}	4/4	2.5/4	4.25/10	1/1
E_{15}	4/4	3.5/4	9/10	1/1
E_{16}	3/4	2.5/4	8.6/10	0/1
E_{17}	4/4	3.5/4	8/10	1/1
E_{18}	2/4	1.5/4	5/10	1/1
E_{19}	2/4	1.5/4	6/10	0/1

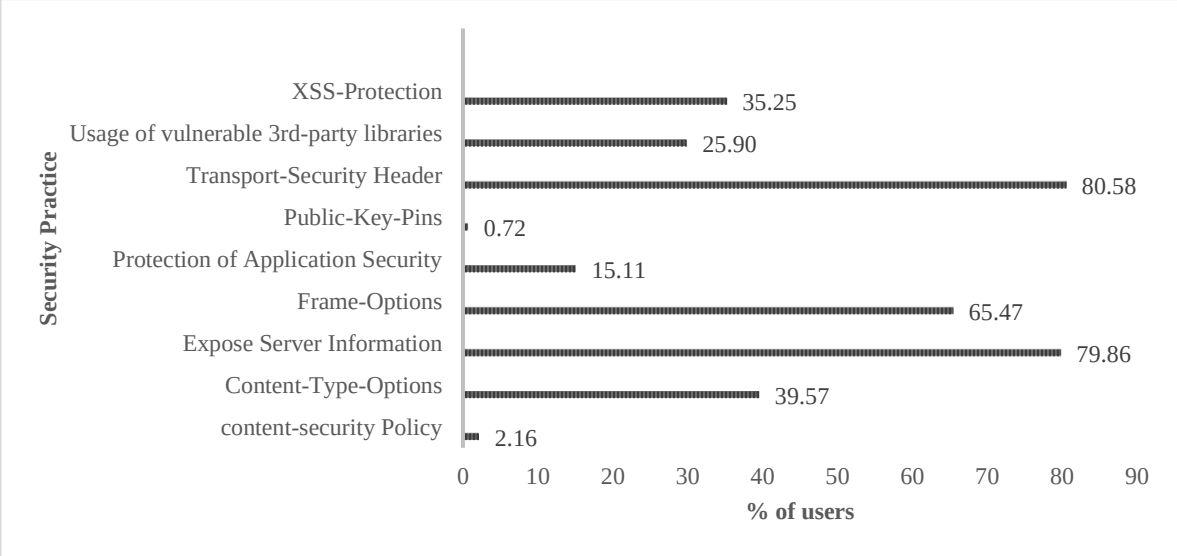
Note: Some exchanges were selected and compared on different parameters under four categories.

SECURITY STATUS IN CRYPTOCURRENCY EXCHANGES

A list of cryptocurrency exchanges was selected and checked for their fundamental security issues that applications must apply (Paul, 2018).

Table 5

Security status in Cryptocurrency Exchanges



Note: This chart indicates that out of the 140 exchanges that were analyzed, only 35%

implements XSS-Protection, the server information is exposed by around 80%. About 26% of them use the vulnerable open-source libraries and only 2% implemented a content-security-policy that protects clickjacking if done properly. This chart clearly shows the implementation of low-level security practices (Paul, 2018).

WEBSITE SECURITY SCANNING USING IMMUNIWEB ONLINE TOOL

Based on Table 5 above, the following list of crypto-exchanges was selected and tested using an online tool called Immuniweb[1] . The following security parameters and compliance were analyzed and reported in a table. The final grade for each exchange has been allotted by the tool based on its security level. The website grade and compliance are subject to change from time to time as the exchanges keep on improving their sites.

Table 6

Web Security status of crypto-exchanges tested using "Immuniweb" tool

Name	**CMS security analysis**	**GDPR**	**PCI DSS**	**Content security policy analysis**	**HTTP headers security**	**Grade**
E_1				Missing		A
E_2		1 issue		Missing		A
E_3		2 issues				A+
E_4		1 issue		Missing	6 issues	C
E_5			1 issue	Missing		A
E_6		1 issue				A+
E_7		1 issue	1 issue	Missing	5 issues	B
E_8		1 issue		Missing		A
E_9	1 issue		1 issue		6 issues	B
E_{10}				Missing	6 issues	C
E_{11}					5 issues	A+
E_{12}		1 issue		Missing		A

[1] https://www.immuniweb.com/websec/

E_{13}	Failed	2 issues	2 issues		5 issues	C
E_{14}		1 issue				A+
E_{15}	Failed	2 issues	2 issues	Missing		C
E_{16}	Failed	1 issue	2 issues	Missing	5 issues	C

Note: This table shows the application vulnerabilities of each exchange at the time of this testing and allotted with a final grade based on its security level. The grade and compliance are subject to change with the improvements made by the cryptocurrency exchanges.

CRYPTO-EXCHANGE ISSUES

The cryptocurrency thefts focus on personal user wallets or exchange accounts through malware such as cryptocurrency-stealing malware (CCSM). Hundreds of unique kinds of malware exist on the Internet to steal wallets or to steal cryptocurrency using other means (Litke, Stewart, & Dell, 2015).

Due to the anonymity with transactions, wallet owners and increased adoption from businesses and users have increased the malicious users (including hackers and scammers). The hackers thereby target the cryptocurrency to hack and gain control over cryptocurrency wallets and transact the funds. Holding cryptocurrencies in exchange wallets remains unsecured and makes the user still face some security issues irrespective of the recent evolution of blockchain technology.

Wallet credentials are the primary targets of attackers. The attackers try to use the simple way of an attack like Phishing attacks on cold wallets and on hot wallets (Lu, Wang, & Li, 2019) through the exchange's web application where transactions happen. The attackers might use a combination of attacks on the exchange and its services (Chiew, Yong, & Tan, 2018).

CRYPTOCURRENCY EXCHANGE VULNERABILITIES

Among all threats and vulnerabilities, hackers and malware are other inherent risks

with crypto-exchanges. This hacking is happening at the touchpoints of users. Thus, when users use the website to transfer crypto assets, the website will be a common touchpoint. This will be a vulnerability associated with hacks and malware (Jaeger, 2019).

Since some crypto-exchange use the openly available, third-party libraries with some known vulnerabilities. These vulnerabilities could be easily known by attackers to design phishing attacks based on the vulnerabilities (Hao et al., 2018).

Cookie Misconfiguration

The cookie misconfiguration is one of the vulnerabilities of cryptocurrency exchanges. The sensitive user information such as identity-related credentials is contained in the cookies. This leads to cookie poisoning where the contents of the cookie are modified by hackers to make unauthorized access to the exchange application or webpage.

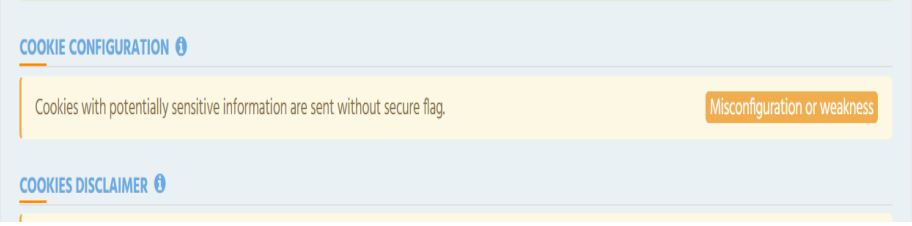


Figure 1. Cookie configuration vulnerability

Backdoor and Debug option

The developers make the debug options enabled while publishing the website. This makes hackers change the code and implement on the website. Since these debug options facilitate an easy backend entry to hackers into the website and make modifications at the website level.

Server Signature

A server signature is the identity of the webserver to the public and holds sensitive

information that can be used to take advantage of any known vulnerability. If the website signature/server signature is turned on, then it means that the hacker could know the details of the server and version that it is running on and potentially exploit the site by stealing sensitive information.

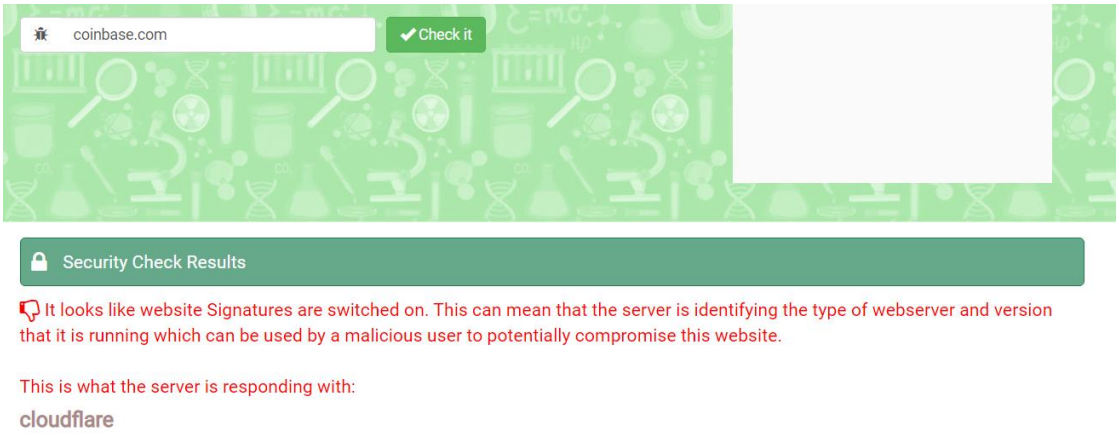


Figure 2. Server signature vulnerability of coinbase exchange

Hacking the Server

For a hacker, this is one of the most lucrative methods to gain access to huge amounts of money. The best way to avoid instances of such attacks is to invest in good security providing devices.

Social Engineering

This is one of the simplest and yet the most unavoidable methods to encounter. The best way to stay safe from these attacks is to understand that even the minutest of information could open the back door to your wallet. Malware and Phishing attacks come under social engineering.

ATTACKS ON CRYPTO-EXCHANGE AND USER WALLETS

Users sign into the exchanges or potentially wallets with their passwords to access exchanges to get some data or make transactions. Nonetheless, usually, users either overlook

or ignore to sign out of their accounts after subsequent visits to the exchanges. Now all the sites that the user visits can approach the user wallet data and all exchanging history (Hao et al., 2018).

Attackers use malware such as keyloggers to steal secret keys and clipboard captures to alter the destination address. The keyloggers are referred to as a significant threat to users because it records keystrokes to steal passwords, seed, passphrase, and PINs that users type. Now, this malware runs an undetectable program on the user's PC or mobile and sends the recorded data to the attackers. In case the wallets get hacked, the users cannot recover the lost money. This method will be very easy for an attacker to access personal data or accounts (BlockSafe, 2018).

Cryptocurrency Exchange Cyber-Attack Vectors

According to cryptomarketcap.com (2018), a cryptocurrency trading volume has passed the $30 billion index in the last quarter of 2018. Because of this heavy trading, many attackers identified various attack vectors to steal cryptocurrency. Due to all the above-discussed vulnerabilities and threats, the following are the major attacks:

1. DDoS (Distributed Denial of Service) Attacks

The distributed denial of service (DDoS) is the generally known cyber-attack on exchanges where the attacker intends to disrupt its services, normally by flooding the server, website or overall infrastructure with too many requests to respond. In 2017, around three in four cryptocurrency exchange sites were victims of this DDoS attack alone (Imperva, 2017) as they are easier and cheaper to perform.

DDoS attacks can be recovered relatively quickly. The most widely recognized intention in a DDoS attack is an interruption. System managers ought to react to them

quickly, so they experience as little downtime as possible that could be expected under the circumstances. The issue is, while they are doing that, they cannot inspect their network to detect various other attacks. Regardless of whether the DDoS targets are just disconnected for few moments, those few minutes may give an attacker a lot of time to conduct data breach or get malicious remote access to the PCs and network (Crawley, 2019). DDoS Attack on some Cryptocurrency Exchanges: Bitfinex (2016) and Bittrex (2017).

2. Phishing Attacks

Phishing refers to an attack where the attacker attempts to imitate either a real site or an individual through an email. It requests the user to make any move that would give the attacker an entry point that helps in stealing vital information or data of users (Chiew, Yong, & Tan, 2018).

This attack mainly sends a message or email to the user and triggers the user to click that link and visit the malicious site. The attacker creates phishing sites similar to real websites with the same user interface to target users. This type of attack is easy because the available third-party source code used by the exchanges could also be taken and used for phishing by attackers. Attackers use phishing to mislead users to send their coins to the attacker's wallet.

By changing the transfer of coins function in the source code, the user sends all the coins to the wallet address preset by the attacker regardless of the recipient’s address as input. This happens without the user knowing and the hack is difficult to detect (Hao et al., 2018). Examples: Bithumb (2018) and Bitstamp (2015)

In the phishing attack on Bitstamp exchange, one of the employees of the exchange received separate messages and emails on skype from legitimate sources. The employee

downloaded malware on to his workstation by clicking the illegitimate links that he received through an email. Therefore, the Bitstamp got hacked and 19,000 BTC that is equal to $5 million approximately, was stolen (Quenston, 2016).

3. Hot Wallet Attacks

Hot wallets are connected to the internet, called as online wallets that help in storing private keys for cryptocurrencies. Exchanges offering hot wallets to store private keys for more security. They claim to store the only required amount of money on hot wallets but that's not always true. Some Hot Wallet Attacks: CoinCheck (2018) and Bitfloor (2012).

4. Exit Scams

Many exchanges collected the user's money and disappear suddenly. This is called exit scam. A South Korean crypto-startup scam called "Pure Bit" has done exit scam screwing over all their users. one of the founders of the exchange escaped with at least 13,000 ETH ($2.7M during the scam) and brought their website down. Due to the anonymous and regulation-free operations, it was difficult to trace the scammers.

While no generally acknowledged security standards exist, such incidents will occur. However, an increase in cybercrime cannot be overlooked and unless cryptocurrency exchanges implement adequate security measures, things could turn out to be worst (Connor, 2019). So, the cryptocurrency exchanges to elevate their security levels, a list of useful security measures must be put together.

Since bitcoin's inception in 2008, many vulnerabilities and attacks were reported to date. Out of all the attacks, the Mt.Gox transaction malleability attack in 2014 was the greatest damage in cryptocurrencies. This biggest bitcoin exchange was closed because the

attackers used malleability attacks and drained all the bitcoins approximately 450 million dollars from its wallets (Decker, 2014).

METHODOLOGY

This research has conducted a root cause analysis on cryptocurrency exchange breaches. It identified the losses occurred and determined relevant threats or attacks that led to such incidents with a comprehensive study of their impact on security. This study focused on proposing a cybersecurity model with tools and techniques that need to be in place to improve the security of exchange web applications and user wallets.

There are many attacks on crypto assets from the time Cryptocurrency was invented. However, this research was limited to cryptocurrency security breaches that happened between the years 2016 and 2019. This study mainly focused on application layer attacks on cryptocurrency exchanges and user wallets that were suffered by critical attacks like malware, phishing, and including DDoS.

This research paper aimed specifically at addressing the following questions:

1) What are the various cryptocurrency exchange vulnerabilities and/or attack vectors?
2) What relevant security components could be tailored for Crypto Exchange applications and wallets to increase security and prevent such security breach incidents in the future?

This research paper reviewed the concepts of cryptocurrency exchanges, their related services such as wallets and, their vulnerabilities. Firstly, a bitcoin vanity address, as well as two cryptocurrency wallets were created to transfer funds and assess the related security and account setup procedures. Further, the survey conducted by the virtual markets integrity

initiative was considered to assess and report the security features such as the onboarding requirements, the measures taken by exchanges and monitoring the IP address. This was assessed to check the ability of the exchanges in providing security to users of different existing cryptocurrency exchanges. Additionally, an exchange security report generated by icorating was considered and some exchanges were selected and checked for their fundamental security issues that applications must apply.

Further, a list of exchange's website security scanning was conducted using an "Immuniweb" online tool to check the vulnerabilities and the final grade for each exchange has been allotted based on its security level. Though blockchain technology secures data in transit using cryptographic techniques, private keys are vulnerable to theft based on the location of storage. Malware like techniques can be used to compromise the security of wallets by leaking the private keys. To protect private keys from theft, a Hardware Security Module and a Runtime Application Self-Protection (RASP) to protect from application-layer attacks including DDoS have been proposed.

Furthermore, an analysis of cyber-attacks on crypto-exchanges due to identified vulnerabilities was conducted to generalize and identified various control gaps to make recommendations based upon the findings. The above research was used to propose some security tools and techniques to better secure cryptocurrency exchanges and user wallets.

PRESENTATION & DISCUSSION OF RESULTS

CRYPTOCURRENCY EXCHANGE SECURITY MODEL

The proposed security model suggests new security components that need to be included in the existing model. Most users are not aware of web application attacks. Below are the components of the cybersecurity model with connections.

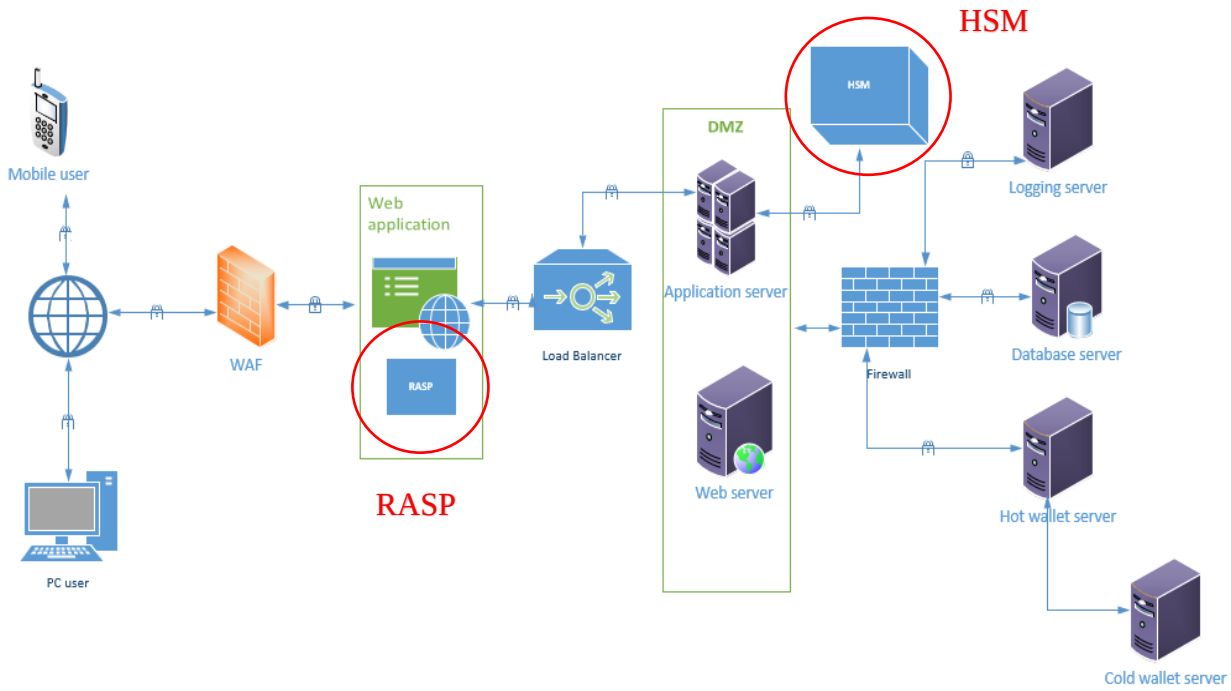


Figure 3. Cybersecurity model for cryptocurrency exchanges

1. **Web Application Firewall (WAF)** that already being used in the existing exchange websites will be kept in place. As it adds a layer of security. But **WAF** has some false positives and false negatives. So, **RASP**, a **runtime application self-protection** will be implemented in the proposed model. RASP is an in-built security component of the web application. If RASP identifies the malicious input, it will stop the execution of that activity to prevent exploitation. RASP has some benefits over WAF i.e., no false positives. This is an advantage of RASP over the WAF.

RASP

RASP is a runtime application self-protection that provides deeper visibility and in-depth protection against the HTTP(S) layer. It is a security component that automatically adapts to the application stack and will protect the application from inside. It controls the application execution, detects and prevents real-time attacks.

How do RASP solutions work?

Like web application firewalls (WAFs), RASP security tools defend a web application against attacks. However, RASP solutions reside and work within the application at run-time that does not require any code modifications. RASP can determine an attack due to vulnerability in code by monitoring the behavior of the application in real-time rather than relying on predefined patterns or signatures. They have access to the full application context along with vulnerable code. They can distinguish normal instructions or requests from malicious ones. Thus, it detects attack accurately, providing a full trace to developers by pinpointing the exact vulnerable line of code. It removes false positives. When RASP detects a threat, it can prevent exploiting the vulnerabilities and perhaps take actions like terminating the existing session, closing the application, sending a warning to the user and alerts the security personnel. RASP aims to close the gap left by the application security testing and network edge controls.

RASP could be deployed in two modes:

Self-protection mode: they stop the execution of requests at run-time for attacks that trigger actual vulnerabilities in the code.

Monitoring mode: it works like the self-protection mode but instead of blocking the attack, it will only report the vulnerability details to the dashboard.

Since developers can’t find and fix every vulnerability pre-production, additional layers of protection are needed. WAFs filled this production protection role for many years but, rulesets and pattern matching create too many false positives causing an inability to catch zero-day vulnerability.

For a comprehensive application security strategy, RASP must be used together with some tools such as WAF, an IAST, and a CDN to protect from DDoS attacks.

Table 7

Implementing RASP and mitigating the issues outlined in Table 6

<table>
<tr><th>S.no</th><th>VULNERABILITY</th><th colspan="3">MITIGATION using RASP</th></tr>
<tr><td>1</td><td>WAF – False Positives</td><td colspan="3">WAF and RASP can work together in a complementary way. WAF can detect potential attacks and RASP can verify it by studying the actual responses in the internal applications. Today, applications mostly rely on external protections like WAF or IDS/IPS, the first line of defense. So, WAF with RASP (double approach) could help in removing false positives in WAF, as RASP has no limited context on logic, behavior, and execution of the application and acts as the last line of defense.</td></tr>
<tr><td>2</td><td>GDPR & PCI DSS Compliance</td><td colspan="3">RASP could make the organizations meet required strict regulatory security and data privacy compliance standards. PCI DSS and GDPR compliance can be achieved in a way that is fast, accurate, and simple to maintain. Since applications have become an integral part of data processing systems, RASP will ensure fulfilling compliance.</td></tr>
<tr><td>3</td><td>Content Management System (CMS) Security Analysis</td><td colspan="3">CMSs are vulnerable by nature because they are built on open source frameworks. Therefore, RASP checks the website for the latest vulnerabilities and makes sure the CMS is secure.</td></tr>
<tr><td>4</td><td>Content Security Policy Analysis</td><td colspan="3">The content security policy is also one of the HTTP headers. If an attacker succeeds in injecting a script or iframe, its ‘src’ will not be on the list and the content will not be loaded. This too acts as a whitelist of the acceptable content for web pages. RASP provides data validation mechanisms to prevent the exploitation of potentially vulnerable coding constructs in software. Data that flows into and through an application can be inspected by a RASP to protect from known, common application layer attacks and zero-day threats.</td></tr>
<tr><td>5</td><td>HTTP Headers Security</td><td colspan="3">All the required HTTP headers related to security and privacy configurations will be checked by RASP. It intercepts each HTTP response from the server. For each response, specific security-related HTTP headers are set automatically, based on the content type of the body and personal preferences. This ensures safe client-server communication. The security headers are added to every request by default. Different security headers with values and descriptions are listed.
<table>
<tr><th>Header</th><th>Value</th><th>Description</th></tr>
<tr><td>Strict-Transport-Security</td><td>max-age=31536000; includeSubdomains</td><td>Keep users on HTTPS</td></tr>
<tr><td>X-Content-Type-Option</td><td>nosniff</td><td>Prevents browsers from sniffing the content-type.</td></tr>
<tr><td>X-Frame-Options</td><td>deny</td><td>Prevents your webpage from being put in an iframe.</td></tr>
</table></td></tr>
</table>

		Content-Security-Policy	script-src 'self'; object-src 'self'	Whitelist of things that are allowed on the webpage.
		X-XSS-Protection	1; mode=block	Basic protection against XSS.

Note: Implementing RASP and mitigating vulnerabilities of Cryptocurrency Exchanges' web security mentioned in table 6.

2. The cryptocurrency exchanges should deploy a **Hardware Security Module (HSM)** as a separate device or can be connected to a server to protect private keys from hackers.

SECURING WALLETS USING HSM

To minimize the risk of loss, all crypto assets must be stored in cold wallets and only a minimal amount for immediate transactions should be stored in hot wallets. To keep the crypto assets safe, the wallets should also be safeguarded by using HSM

An HSM, a hardware security module is a secure physical and external device. It is designed for crypto processing i.e., securely generates and stores (encrypting and decrypting) private keys specifically to protect sensitive data. HSM is built with specialized hardware with strictly controlled access and thoroughly tested by third-party regulators.

Hardware security modules are a must only for organizations that deal with payments such as credit/debit card information. Some industries like banking, government and healthcare sectors use this HSM for enhanced protection and to meet PCI DSS compliance regulations. HSMs come with a certain level of regulatory assurance, such as the Federal Information Processing Standard certification. Also, the crypto exchanges need to regularly monitor the network activity all-around their wallets to detect unauthorized transactions. All-access transactions to HSM should be logged to create an audit trail.

HSM provides the highest level of security against external threats. It helps protect from malicious hacks and safe to use. Some IT providers offer HSM as a service, which makes this HSM affordable to companies that could not invent in an HSM. Rather than storing a key in software, HSM alone keeps the key in a safe and secure place, making it easier to track and safeguard the keys. An HSM provides tamper-proof protection. It provides a level of security that's difficult to achieve using software alone.

OWASP TESTING GUIDE FOR WEB APPLICATION SECURITY

Normally, the cryptocurrency exchanges do not put enough amount of assets into security best practices. Exchanges do not have regular penetration tests on their systems and do not have formal security verification standards set up. So, these organizations become vulnerable to cyber-attacks because of such characteristics. The web application security testing guide created by Meucci & Luptak in 2016 provides a framework of best practices employed by penetration testers and organizations all over the world to prevent cyber-attacks. All typical functions should be tested by the subsequent methods which include a brief version of the OWASP web security testing guide:

Table 8

OWASP web security testing guide

TESTING		Authentication	Verification	Account	Security settings	Wallet	Trading	API	other
Deployment & configuration management	Network or infrastructure configurations testing	●	●	●	●	●	●	●	●
	Application configuration Testing								
	Enumerate admin interfaces								

	Testing of HTTP methods and strict transport security								
	Test SSL/TLS								
Identity management	Testing role-based definitions	●		●					
	Testing the process of user registration								
	Testing the process of account suspension or resumption								
	Test password reset process								
Authentication	Test default credentials	●		●					
	Test weak password policy-change/reset								
	Test multi-factor authentication								
Authorization	Test for privilege escalation		●	●	●	●	●	●	
Data validation testing	Testing for Stored Cross-Site Scripting	●	●	●	●	●	●	●	●
	Testing for SQL Injection								
	SQL Server Testing								
	Testing for Code Injection								
	Testing for Buffer overflow								
The Business logic test and assessment	Testing the Business Logic Data Validation	●			●	●	●	●	
	Testing the capability in Forging Requests								
	Testing the Integrity Checks								
	Testing the limit on function usage								
	Testing the upload of malicious and corrupted files								

Note: All typical functions like authentication, verification, etc should be tested by the subsequent methods like deployment and configuration management, etc which include a brief version of the OWASP web security testing guide.

INCIDENCE RESPONSE PLAN FOR MALWARE

Attacks create enormous pressure for time and developing a detailed incident response plan beforehand is critical to acting quickly and minimizing damage. The incident response plan of this research uses six phases as identified in NIST to handle incidents in exchanges. After analyzing the attack incidents in Exchanges as shown in Appendix A, an incident response plan has been developed as identified in NIST.SP.800-83r1 by Souppaya & Scarfone (2013) and NIST.SP.800-61r2 by Cichonski, Millar, Grance, & Scarfone (2012).

The key steps for creating an effective incident response plan are included in table B1 in Appendix B.

CONCLUSION & RECOMMENDATIONS

Cryptocurrency has already been proven as a popular digital currency in the market. However, the popularity of cryptocurrency has attracted many hackers to use cryptocurrency exchanges for their benefits. The outstanding recognition and rise of the crypto exchanges made the adversaries attracted to launch several security threats. The cryptocurrency exchanges are dreaded with several attacks.

A survey was conducted by the New York State Office of the Attorney General (the "OAG") to illuminate their New York occupants about the existing security features and requirements to handle cryptocurrency in exchanges. This survey paved a way in identifying several security flaws, the onboarding requirements of exchanges, and measures taken by the exchanges. A web security scanning has been conducted and analyzed the threats of some exchanges and the vulnerabilities that led to the prevalent attacks (Table A1) like DDoS, malware, and phishing which are outlined in table 6.

This paper identified several attacks and there are some solutions. However, the robust and effective security solution to these attacks has been proposed through a model (figure 3) with the implementation of RASP, a runtime application self-protection along with the existing Web application firewall (WAF) and HSM.

How the proposed model mitigates the vulnerabilities identified in table 6 has also been outlined. Today, none of the exchanges introduced RASP into their system architecture. Whereas, most of the traditional banking systems use Hardware security modules to store the funds along with user's personal information like credit and debit cards. Therefore, to keep the crypto assets safe, HSM has also been proposed in the model for cryptocurrency exchanges.

Additionally, an incident response plan has been developed to handle malware attacks on exchanges. The web application security testing guide by OWASP has been used to create a framework of best practices for cryptocurrency exchanges to prevent cyber-attacks.

In conclusion, this research was conducted to highlight security issues and secure cryptocurrency exchanges from similar incidents in the future. The proposed cybersecurity model could eliminate false positives and provide best security to the exchanges. Finally, users need to gain enough knowledge of exchanges and be aware of potential threats to websites. Users should also maintain knowledge of all security features followed by each exchange they use.

Regarding the future work on this research, an interesting direction would be discovering new vulnerabilities, identifying different network attacks, mining attacks and propose stringent security and privacy techniques.

References

Bancor. (2018). “Here is the latest update on the recent security breach:” pic.twitter.com/JroypFvBri. Retrieved from https://twitter.com/Bancor/status/1016420621666963457.

Bitfinex. (2016). Bitfinex is under DDoS attack. The DDoS attack started during earlier maintenance and has been ongoing since. Retrieved from https://twitter.com/bitfinex/status/934799838239223808?lang=en.

BlockSafe. (2018). Security Token Offering White Paper - BlockSafe Tech. Retrieved from https://www.blocksafetech.io/BlockSafeWhitepaper.pdf.

Chiew, K. L., Yong, K. S. C., & Tan, C. L. (2018). A survey of phishing attacks: Their types, vectors and technical approaches. Expert Systems with Applications, 106, 1–20. doi: 10.1016/j.eswa.2018.03.050

Cichonski, P., Millar, T., Grance, T., & Scarfone, K. (2012). Computer Security Incident Handling Guide: Recommendations of the National Institute of Standards and Technology. doi: 10.6028/nist.sp.800-61r2

Connor, R. (2019). Ways to make your cryptocurrency exchange secure? Retrieved from https://nowfuturetech.com/how-to-make-your-cryptocurrency-exchange-secure/.

Conti, M., Kumar, E. S., Lal, C., & Ruj, S. (2018). A Survey on Security and Privacy Issues of Bitcoin. IEEE Communications Surveys & Tutorials, 20(4), 3416–3452. doi: 10.1109/comst.2018.2842460

Crawley, K. (2019, April 10). What is Distributed Denial of Service and what do DDoS attacks look like? Retrieved from https://cybersecurity.att.com/blogs/security-essentials/explain-what-ddos-is

Decker, C., & Wattenhofer, R. (2014). Bitcoin Transaction Malleability and MtGox. Computer Security - ESORICS 2014 Lecture Notes in Computer Science, 313–326. doi: 10.1007/978-3-319-11212-1_18

Dikshit, P., & Singh, K. (2017). Efficient weighted threshold ECDSA for securing a bitcoin wallet. 2017 ISEA Asia Security and Privacy (ISEASP). doi: 10.1109/iseasp.2017.7976994

Eitzman, R. (2019). Cryptocurrency and Blockchain Networks: Facing New Security Paradigms. Retrieved from https://www.fireeye.com/blog/threat-research/2019/01/cryptocurrency-blockchain-networks-facing-new-security-paradigms.html.

Hao, P., Chang, V., Lu, S., & Zhang, C. (2018). Decentralized Cryptocurrency Exchange Security Analysis.

Hu, Y.-C., Lee, T.-T., & Lam, C. (2019). A Risk Redistribution Standard for Practical Cryptocurrency Payment. 2019 IEEE International Conference on Decentralized Applications and Infrastructures (DAPPCON). doi: 10.1109/dappcon.2019.00020

"ICORATING". (2018). Exchange Security Report V 2.0 Update. Retrieved from https://icorating.com/report/exchange-security-report-v-20-update/

Imperva. (2017). Global DDoS Threat Landscape Q3 2017. Global DDoS Threat Landscape Q3 2017.

Jaeger, J. (2019, November 14). Internal control best practices for blockchain technology. Retrieved from https://www.complianceweek.com/accounting-and-auditing/internal-control-best-practices-for-blockchain-technology/28032.article.

Khatri, Y. (2019, March 26). Singapore-Based Crypto Exchange DragonEx Has Been Hacked. Retrieved from https://www.coindesk.com/singapore-based-crypto-exchange-dragonex-has-been-hacked.

Litke, P., Stewart, J., & Dell. (2015). The Cryptocurrency-Stealing Malware Landscape. Retrieved from https://www.secureworks.com/research/cryptocurrency-stealing-malware-landscape.

Lu, Y., Wang, G., & Li, J. (2019). Keyword guessing attacks on public-key encryption with keyword search scheme without random oracle and its improvement. Information Sciences, 479, 270–276. doi: 10.1016/j.ins.2018.12.004

Meucci, M., & Luptak, P. (2016). Testing Checklist. Retrieved from https://wiki.owasp.org/index.php/Testing_Checklist

Paul. (2018). Security analysis of the most popular cryptocurrency exchanges. Retrieved from https://blog.sqreen.com/cryptocurrency-exchanges-security/

Stephenson, B. (2019). The Secret to Making a Wallet For Your Cryptocurrency. Retrieved from https://www.lifewire.com/making-a-cryptocurrency-wallet-outside-a-centralized-exchange-4160942.

Souppaya, M., & Scarfone, K. (2013). Guide to Malware Incident Prevention and Handling for Desktops and Laptops. doi: 10.6028/nist.sp.800-83r1

Underwood, B. D. (2018). Virtual Markets Integrity Initiative Report. Retrieved from https://virtualmarkets.ag.ny.gov/#section1

Wood, A. (2019). Hackers Withdraw 7,000 Bitcoins in Binance Crypto Exchange Security Breach. Retrieved from https://cointelegraph.com/news/hackers-withdraw-7-000-bitcoins-in-binance-crypto-exchange-security-breach.

APPENDICES

Appendix A

Table A1

Attacks on Cryptocurrency Exchanges

TIME FRAME	CRYPTO EXCHANGE	LOSS	DESCRIPTION	ATTACK
May 2019	Binance	$41 million	The attackers got the multifactor authentication codes and API keys. 7,000 bitcoin (BTC) was moved to the hacker's wallet in a single transaction. The CEO of the Binance exchange stated that only 2% of the funds were stolen from hot wallets (Wood, 2019).	Hacked through a combination of phishing and malware attacks.
May 2019	DragonEX	USD 7.09M	DragonEX was hacked and it provided some wallet addresses of cryptocurrencies to which the stolen funds were transferred. The top 5 cryptocurrencies in the list were bitcoin (BTC), ether (ETH), XRP, Litecoin (LTC) and EOS. DragonEX exchange requested the fellow exchanges to block the stolen crypto assets (Khatri, 2019).	Attack on Hot wallet.
February 2019	Coinmama	-	Coinmama serving a total of around 1.3 million users was attacked and the customer database was hacked with 450k user emails and passwords. It was assumed that the attackers used the stolen credentials to access the wallets.	The database was hacked.
Jan 2019	Cryptopia	USD 2.44M	Cryptopia exchange clarified on twitter that it suffered a security breach and reported to the relevant New Zealand's authorities. The total amount of lost funds was unidentified, but 19,390 ETH was transferred to an unknown wallet.	Insider attack
July 2018	Bancor	USD 13.5M	Bancor confessed that unidentified actors compromised a wallet that was used to upgrade smart contracts. User wallets were not hacked. The hackers also stole 3,200,000 of Bancor's BNT tokens worth approximately USD 10 million (Bancor, 2018).	Compromised hot wallet
June 2018	Bithumb	USD 30.8M	Attackers stole cryptocurrencies worth USD 30.8 million from South Korea's largest cryptocurrency exchange, Bithumb. According to Cointelegraph Japan, the attackers hijacked Bithumb's hot (online) wallet by sending malicious emails to Bithumb users. Hackers gained the credentials and other information when users clicked on the links.	Attackers hijacked hot wallet by sending malicious emails.
February 2018	BitGrail	USD 195M	BitGrail claimed that USD 195 million worth of customers' cryptocurrency in Nano (XRB) was stolen.	DDoS

January 2018	Coincheck	$534 million	Unidentified attackers stole 523 million NEM coins (approximately USD 534 million) from the exchange's hot wallet. Coincheck stated that NEM coins were kept on a single-signature hot wallet rather than a more secure multi-signature wallet and confirmed that stolen coins belonged to Coincheck customers.	Attack on Hot wallets of users
June 2017	Bithumb	$1 million	Bithumb, a large exchange for ether and bitcoin, admitted that malicious actors stole a user database from an employee's computer that includes the names, email addresses, and phone numbers of more than 31,800 customers. Bithumb stated that its internal network was not compromised.	The attacker has stolen the database and later used phishing against the exchange's users to steal wallets.
April 2017	EtherDelta	$266,789	EtherDelta is a DEX that lists nearly all the existing Ethereum-based tokens. The smart contracts that govern EtherDelta's behavior weren't compromised in the attack. However, the attacker managed to take over the EtherDelta's DNS server and a lot riskier than the normal phishing attack was performed, providing a fake version of the website like the real one (such as etherrddeltta.com) to the users.	Phishing attack
August 2016	Bitfinex	$72 Million	When Bitfinex first announced the hack, it was the largest dollar-based exchange for Bitcoin in the world, and this theft was the second-biggest security compromise in the history of cryptocurrency (Bitfinex, 2016).	Attack on hot wallets.

Note: Some of all the thefts between 2016 and 2019, aiming at multiple cryptocurrencies are recorded and reported.

APPENDIX B

INCIDENCE RESPONSE PLANNING FOR MALWARE

Table B1

Incident Response Plan for malware using NIST 800-61r2 (Souppaya & Scarfone, 2013) and NIST 800-83r1 (Cichonski, Millar, Grance, & Scarfone, 2012)

Preparation	Detection & Analysis	Containment	Eradication	Recovery	Post-Incident Activity
• Build and maintain the malware-related skills in the incident response and communicate and coordinate throughout the organization. • Deploy necessary software such as antivirus/anti-spyware & hardware tools. • Maintain resources such as incident analysis resources and incident mitigation software.	• Detect and assess possible incidents like identifying malware detection sources such as network-based and host-based IDPS, antivirus software, log analyzers, and SIEM technologies. • Identify the infected hosts. • A well-trained capable staff is required to conduct incident detection and analysis.	• Identify infected hosts and what measures to take. • Strategies and procedures should be developed for making containment-related decisions. • Determine which method or combination of methods of containment to employ initially. • Unknown malware copies must be sent to security	• Eradication is removing the malware from infected hosts by eliminating or mitigating the weakness or vulnerability of the host. • Various techniques including the combination of eradication techniques should be used simultaneously. • The common tools for eradication of malware are	• Administrators restore systems to normal operation, confirm that the systems are functioning normally, and remediate vulnerabilities to prevent similar incidents. • Restore data from backups, rebuild systems from scratch, replace compromised files with	• Conduct a robust assessment of lessons learned from major malware incidents. • Improve security measures and incident handling process. Improve malware defenses like identifying changes in security policy,

• The configurations and security of their hosts should be constantly monitored. • The host-level (e.g., server and workstation OS), the application server level (e.g., email server, web proxies), and the application client level (e.g., email, SMS) should be deployed with malware protection. • Users/clients should be informed of the policies and procedures for the appropriate use of network frameworks, systems, and applications.	• Prioritize the handling of each incident on NIST SP 800-61 guidelines. • Notify the appropriate individuals who would be involved in the handling • Every step during the detection and analysis should be documented, timestamped and signed by the incident handler.	software vendors for analysis and guidance on handling new threats when incidents could not be identified by existing software. • Control and manage communications to the public	antivirus software, vulnerability management technologies, and network access control software must be used. • Use efficient automated eradication methods, such as triggering antivirus scans remotely. • Perform awareness activities to reduce the stress on organizations that various malware incidents cause.	clean ones. Also, install patches and tighten the perimeter network security. • Higher-level security System logging and network monitoring should be implemented.	software configurations, and malware detection and prevention software deployments.

APPENDIX C

Table C1

Best Practices for exchanges

S.no	FEATURE	DESCRIPTION
1	2F Authentication	Using a 2FA adds a layer of security as the user must enter the 6-digit password generated by a google authenticator app. This service is more secure than SMS, securing users from a sim swap.
2	Use Linux OS to reduce OS vulnerability	Linux OS-based systems are more secure than windows OS-based systems. Because Linux users could not download software easily unlike on windows. However, software on the command-line interface must be installed from an open repository where all viruses can be spotted by technical analysts.
3	Double-check the exchange's website URL before logging in	To steal user credentials, many phishing websites are designed like real exchange platforms and gain access to user accounts.
4	Beware of public Wi-Fi	When browsing sites using public wi-fi, it probably redirects to phishing sites and steals credentials and data.
5	Adblocker	To install malware on the system, hackers use highly tempting phishing ads to make users click on it and install malware. It is recommended to install an ad blocker in the browser to be safe from malware-infected ads.
6	Download safe extensions	**Netcraft Extension:** This extension permits users to see the risk rating of each site given by existing users of this extension and secure against phishing i.e., When users report a suspicious connection, the extension would keep all clients from getting to the site. **Cookie AutoDelete: T**he web browser sends the HTTP Cookie data from the website and store on the user's PC while the user is browsing. Hackers use these cookies to retrieve information such as passwords and steal data. So, by installing an extension like Cookie AutoDelete could automatically delete the stored cookie data as soon as the user exits the website.
7	Say "No" to VPN	Platforms must block the users that try to access the website through a VPN. Because users mask their IP address using a VPN connection to obscure their location of login and avoid the security analysts from tracking their real location.
8	Salting authentication credentials	Authentication credentials such as passwords should be salted and hashed (not encrypted) on the back-end systems, to protect them if they are compromised, and to prevent leakage via an inside job.

9	2FA for withdrawal transactions	For digital asset withdrawals, digital asset exchanges should use a security feature that requires users to click a link sent to an email before the release of the transaction. The exchange can also use 2FA and the user should enter the security code generated by 2FA and authenticate the transaction. If the link is not clicked or code is not entered within a short period, the withdrawal should be canceled.
10	Login notifications	Login notifications are an extra security feature that can help alert users if someone accesses their account.
11	IP Whitelisting	IP Whitelisting allows users from specific domains only. All the trusted IP address ranges must be created as a list to give access.
12	Multi-signature wallets	Steps should be taken to require multiple employees within the exchange to approve/authenticate transactions over certain limits, to mitigate the insider threat. This can be done technically (using multi-signature wallets), rather than just relying on operational procedures.
13	Monitoring hot storage	Limits and triggers on the percentage of assets held in hot storage should be set, with monitoring measures put in place to ensure limits are adhered to.
14	KYC	Digital asset exchanges should aim to conduct verification of users as early as possible in the account signup process, and any event before the deposit of money or the commencement of trading.
15	Restrict multiple accounts	Multiple accounts should be discouraged as there is a heightened risk of structuring (split transactions or wash trades)

Note: Best Practices derived through Literature Review.

APPENDIX D

List of Cryptocurrency Exchanges

The Cryptocurrency Exchanges that were tested by Virtual Markets Integrity Initiative and Immuniweb online tool were listed below:

Binance, Bitfinex, Bitflyer, Bitstamp, Bithumb, Bittrex, Coinbase, Coindeal, Cryptopia, DragonEX, Gemini, GOPAX, Hbus, HitBTC, Itbit, Kraken, OTCBTC, Poloniex, Tidex, and Zaif.