Curtin University

BLOCKCHAIN RESEARCH AND DEVELOPMENT LAB

SECURING CRYPTO CURRENCY EXCHANGES

SECURITY REPORT

DATE

22 JUNE 2018

BY

DR VIDY POTDAR, PHD

SECURITY ATTACKS

OBJECTIVE

Securing cryptocurrency exchange is of paramount importance to maintain trust and reliability among crypto traders.

This report analyses security features implemented by 22 cryptocurrency exchanges. We provide a list of all security features reported on the exchange's website or in their white papers.

Cryptocurrency Security Standard (CCSS) is a relevant security standard for cryptocurrency exchanges. Exchanges should also comply with the Information Security Management Standards (ISO/IEC 27001:2013).

EXCHANGE HACKS

Bithumb exchange was hacked on 20th June 2018 and lost over 31 million dollars.

In the past several crypto exchanges were hacked such as MtGox, Cryptsy, Mintpal, Bitstamp, Bter, Bitfinex, Nicehash, Coincheck, BitGrail, CoinSecure, Coinrail, causing significant losses.

"According to CoinGecko, a whopping $606 million worth of cryptocurrencies were lost so far, with most of these losses happening through exchanges."

ATTACK EXPLOIT

So why were hackers able to attack these exchanges? To understand this, we researched key security features of several well-known cryptoexchanges.

CRYPTOEXCHANGES

22 CRYPTO EXCHANGES STUDIED

- Bitfinex
- Binance
- Huobi
- Coinbase
- GDAX
- HitBTC
- Bitstamp
- itBit
- CoinSpot
- BTCMarkets
- Coinloft
- Paxful
- Kucoin
- QuadrigaCX
- Gatecoin
- Coinfloor
- TradeSatoshi
- Gtaecoin
- Go4crytos
- Abucoins
- LakeBTC
- BitFlyer
- Bittrex

COMMON SECURITY FEATURES ACROSS ALL 22 EXCHANGES

- Two factor authentication
- Cold Storage
- DoS and DDoS resilience
- DigiCert SSL Server Certificates
- Password protected databases
- Protection from DDoS attacks
- Cookies
- Multi-Factor authentication
- Cross-Site Request Forgery (CSRF) attack prevention
- PCI Scanning to protect servers from hackers and vulnerabilities
- Phishing prevention
- Employees using encrypted hard drives and strong passwords

COMPLETE LIST OF SECURITY FEATURES

- The next section lists the security features adopted by 22 cryptoexchanges.

SECURITY FEATURES

AUTHENTICATION

- Two-factor authentication
- Universal 2F authentication
- Facebook authentication
- Password hashes and salts
- Multi-factor authentication

WITHDRAWAL SECURITY

- Withdrawals protection
- Verification of deposit and withdrawal transactions
- Payment Card Industry Data Security Standard (PCI DSS7)

CUSTOMER SAFEGUARDS

- Identity verification for major changes
- Anti-social force check by external agency database
- Segregated Customers
- Segregated Customer Fiat Currency

EMAIL SECURITY

- Email Encryption with OpenPGP

STORAGE SECURITY

Offline storage / Cold Storage
Data centers compliance ISO 270014, 270175 and 270186
Secure Data Centre
Script Hash (P2SH) cold storage

SYSTEM SECURITY

- Always up-to-date software
- Monitor account integrity
- Password protected directories
- Automatic operating system patching
- Auto alert with self-diagnosis function
- Advanced API key permissions

BACKUPS

- Automatic database backup once a day
- Automatic backup duplication

DATABASE SECURITY

- Encrypting customer database
- Password protected databases

SECURITY ANALYSIS

AUDITING & RISK MANAGEMENT

- Professionally audited securityInternal risk control and operation process
- Collaborative Security with Cloudflare
- Systematic Procedures & Checks

WEBSITE FUNCTIONALITY

- Limit a variety of actions on the site
- Prevent mass-assignment vulnerabilities
- Automatic Timeout
- IP Address Restriction
- Global Load Balanced Network
- Cookies

DIGITAL CERTIFICATES

- DigiCert SSL server certificates
- SHA-2 (SHA-256)
- SSL for internal communications

NETWORK SECURITY

- Protection from DDoS attacks
- SQL injection filters
- Prevent Cross-Site Request Forgery (CSRF) attacks
- PCI Scanning to protect servers from hackers and vulnerabilities
- Threat Detection
- Transport Layer Security (TLS)
- XSS (Cross Site Scripting) preventive measures
- Phishing resilience
- Session hijacking

STANDARDS

- Information security management standard (ISO/IEC 27001:2013)
- CryptoCurrency security standard (CCSS)

EXCHANGE EMPLOYEES SECURITY

- Employees using encrypted hard drives and strong passwords
- Auto screen locking
- Employee compliance training
- Multi-level review and approval to check and use all online data
- Anti-social force check via external database (Japan)

FINAL THOUGHTS

Dr Vidy Potdar
Director
Blockchain R&D Lab
Faculty of Business & Law
Curtin University

Dr Vidy Potdar is a cybersecurity expert with a PhD in Cyber Security from Curtin University, Australia. He has over 15 years of experience in the Australian university sector involving teaching, contract research, and consulting and technology development. Vidy has worked with numerous industries on diverse projects including Department of Transport (data analytics), StatoilHydro (Security in the Internet of Things), Main Roads (traffic congestion management), Fleetwood (energy management).

He regularly appears in media sharing his technology insights. His expertise lies in the blockchain, cybersecurity, and smart grids, with application in the energy sector, supply chain and logistics, and mining. Vidy has published over 150 technology research articles in leading international journals and conferences.

SECURITY IS PARAMOUNT

- Security is of paramount importance in running a cryptoexchange.
- We have seen several cases of attacks on cryptoexchanges where the investors and the exchanges have lost a significant amount of money impacting their reputation.
- Bithump was attacked on 20th June 2018, losing over 31 million dollars.
- As a result of such attacks consumers, lose trust and brand suffers severe damage.
- Hence, securing the cryptoexchange from the start is the best-recommended approach.
- New cryptoexchanges should take inputs from their security advisor from the time the development begins.
- Information security is a functional requirement for cryptoexchanges and is not an afterthought.

THANK YOU

for the opportunity