sEptu

Cryptocurrency Exchange Security

November, 2020

Biggest bank robbery in history:
Aug 2006. Banco Central, Brazil
$72m stolen

Biggest crypto robbery in history:
Jan 2018. Coincheck, Japan
$534m stolen

sEptu

Background - the paradox of crypto security

Very hard to hack cryptocurrencies directly:

- Underlying distributed ledger (blockchain) technology for most cryptos is extremely resilient
- Guessing or trying to work out a private key is almost impossible

But - exchanges are vulnerable…

- Crypto keys - stored in internet-connected 'hot wallets' - can be stolen if the exchange is breached, giving immediate access to customer assets which can be transferred away anonymously
- Like banks, crypto exchanges are threatened by very aggressive forms of cyberattack, but generally have much less robust security than established financial institutions
- Many operate in unregulated jurisdictions, and do not share common standards, meaning that they aren't forced to apply stringent security controls

…and they are obvious targets

- Very large potential monetary gain for low risk

sEptu

An existential risk to crypto exchanges has resulted from the many high-profile robberies that have occurred on them, and the frequent lack of recourse for customers that lose money. This has prompted many investors to transfer funds out of exchanges to their own cold wallets

Robust security on the exchange means:

- A significant reduction of the risk of successful cyberattacks on the platform and corporate network
- Less delays and outages
- Easier to address risks from insider trading and market manipulation

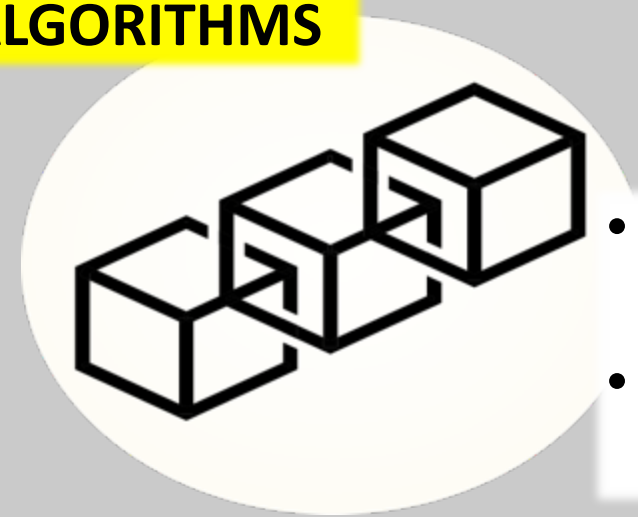
Leading to:

- Money saved by the exchange due to reduced probability of theft and lower legal fees
- Higher confidence in performance and reliability of the platform, and crypto-exchanges generally

sEptu

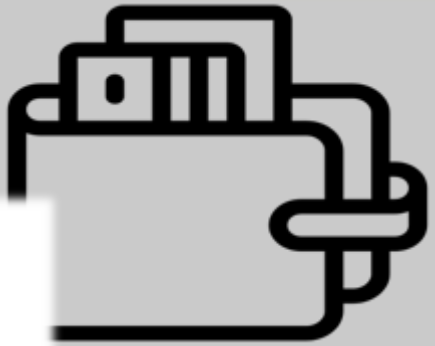
Crypto Attack Surface

BLOCKCHAIN ALGORITHMS

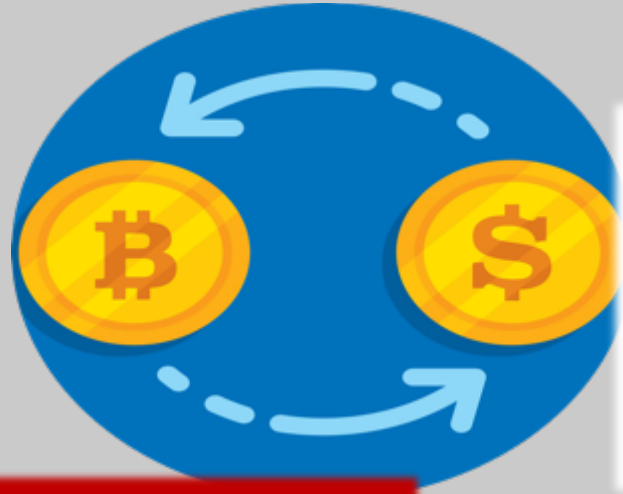


- Direct attacks on the cryptocurrency
- '51% attack', double spending etc

WALLETS



- Steal data from wallets
- Weak encryption or key generation



CRYPTO EXCHANGES

- Infiltrate exchange or company network
- Steal wallet data and keys
- Disrupt exchange

- Social engineering attacks e.g. phishing
- Insider threat

PEOPLE

sEptu

Cyberthreats to crypto exchanges

Data breach and hot wallet compromise: "If you don't have the keys, it's not your crypto"

- 'Hot wallet'
  - Cryptocurrency wallet that is stored on a device on the exchanges connected network
  - Contains the key(s) needed to spend and receive cryptocurrency

- Hot wallet data files are susceptible to the same hacking risks as other files – network infiltrators look for vulnerable files and then use the keys to steal cryptocurrency

- Data breaches usually start via an attack vector such as a phishing email or insecure VPN. Malware is injected into the organisation via this vector, and the attacker subsequently roams the victim's network looking for targeted information – in this case crypto wallets and keys

- All organisations should secure themselves against the risk of data breach: At the very least they normally have an obligation under local privacy regulations to protect the private information (PI data) of customers and employees. However, crypto exchanges have to be particularly careful

- **<u>Attackers targeting wallets and keys are the main financial and reputational risk to crypto platforms</u>**

sEptu

Cyberthreats to crypto exchanges

Insider threat

- A person within the organisation that has access to sensitive data - such as wallet files - either steals them or transmits them externally to someone that should not have them
- This may be for malicious reasons or due to an error (e.g. copying the wrong person on an email)
- Not necessarily a current employee – could also be an ex-employee for which login rights have not yet been deactivated, or a contractor or other third party

Account take-over

- Login attacks, whereby malicious actors attempt to access user accounts on the platform, and then transfer funds and/or abuse the accounts in other ways
- Often achieved by 'credential stuffing' where stolen username/passwords are tested against the platform
- Regulators don't like this at all!

Threat from nation-state supported and criminal hacking groups (APT)

- N Korean 'Lazarus' group has allegedly stolen ~$2bn from crypto including exchanges
- Russian and Chinese groups also linked to similar activities
- Advanced Persistent Threat groups (APTs) have time, resources and expertise

sEptu

Cyberthreats to crypto exchanges

Phishing, Vishing

- Fraudulent emails (phishing) that request sensitive data such as passwords, or deliver malware via attachments or malicious website links. Still the preferred attack vector of cybercriminals

- Spearphishing attack: emails are carefully constructed, sent directly to targeted employees (CEO, IT admin etc.) and sometimes combined with fraudulent phone calls (vishing) and/or text messages

Specialised malware

- Criminal groups use tailor-made malware such as 'Pony Loader' and 'Anubis' to attack cryptocurrency exchanges via phishing emails or malicious website links

- The malware has a range of functionality including modules that can record keystrokes ('keylogger'), do brute-force attacks on passwords, steal crypto-credentials and exfiltrate data

- Sophisticated attackers such as APT groups often use 'Zero-Day' malware that has not been observed before and evades traditional signature-based detection software

sEptu

Cyberthreats to crypto exchanges

Website and web application attacks on the platform

- **Login attacks**
  - Attempts to hack the login of the platform (a form of account take over), including:
    - Credential stuffing (many user name/password combinations that have been stolen elsewhere are tested against the login)
    - Password spraying (known or guessed user names are tested against a database of potentially viable passwords)

- **Denial of Service (DoS), Distributed DoS (DDoS)**
  - The attacker floods the website with data requests
  - Intention might be to
    - Disrupt the business for competitive reasons
    - Extort money (‘pay us and we’ll stop’)
    - Distract security while a more subtle attack (e.g. a data breach) is carried out

- **Injection attacks, API attacks and other web application exploits**
  - Technical attacks that exploit vulnerabilities in the coding of the website and the APIs
  - Refer to the OWASP Foundation ‘Top 10 Web Application Security Risks’

sEptu

Examples of attacks

- **Mt Gox - 2011-2014**
  - Attacker allegedly compromised an auditor's computer and stole credentials from it, enabling them to access the company network and access (unencrypted) private keys of Mt Gox customers
  - 850,000 BTC stolen

- **Coincheck - Jan 2018**
  - Employee computers allegedly infected by virus associated with a Russian hacker group
  - Attack vector was probably an email phishing attack
  - Coincheck was not subject to new exchange registration requirements with Japan's FSA
  - $534m of NEM ('New Economy Movement') stolen (from one, single hot wallet)

- **Binance - May 2019**
  - Attackers 'used a variety of techniques, including phishing, viruses and other attacks' according to the CEO
  - 2FA (two factor authentication) was compromised, as were a number of 'high-net-worth' accounts
  - 7,000 BTC stolen – around $40m equivalent value at the time

- **KuCoin – Sep 2020**
  - Detailed information not yet released but apparently likely due to either an employee illegally sharing hot wallet private keys or a phishing attack
  - A variety of cryptocurrencies stolen including BTC, LTC, XRP and ETH with total value of ~$275m

sEptu

Threat mitigation

- **Security Awareness Training, Email security**
  - Software that trains employees to spot phishing emails and other malicious activity
  - Email security uses methods including machine learning to help automatically detect and block phishing attacks

- **Multi-Factor Authentication (MFA)**
  - Password authentication is combined with another type of authentication e.g. a pin number sent by email
  - Should be used everywhere (employees, customers), and enforced rather than optional on platform login
  - Helps to prevent Account Takeover and other login attacks

- **Endpoint Protection**
  - Protects corporate endpoints such as PCs, servers, laptops and mobile devices
  - Detects malware and suspicious activity that might indicate that an attacker has infiltrated the network
  - Part of a ‘defence-in-depth’ posture regarding Advanced Persistent Threat activity
  - Can also offer Encryption and Data Loss Prevention functionality

sEptu

Threat mitigation

- **Data Loss Prevention and Insider Threat Protection**
  - Discovers sensitive data (e.g. wallet files, keys) on databases, devices and the cloud
  - Controls transmission of sensitive data (e.g. block attempts to send keys to personal email or cloud storage – whether due to malicious reasons or negligence)
  - Identifies and flags suspicious user behaviour
  - Encrypts sensitive files

- **Web Application Firewall (WAF)**
  - Firewall on the platform and corporate website; protects against:
    - Denial-of-Service attacks and vulnerability exploits such as injection attacks
    - Automated attacks (via 'bad bots') such as Account Takeover, price scraping, vulnerability scanning etc.
  - Using a WAF and content delivery network (CDN) can also significantly improve website performance

- **Web app vulnerability scanning**
  - Crawls through and scans the website for coding vulnerabilities, misconfigurations and out-of-date software
  - Able to detect all the OWASP10 web application vulnerabilities, and many more
  - Aids compliance with main regulatory requirements including PCI:DSS (credit card payments)

sEptu

Hot wallets and keys – security requirements

- Keys (or seeds used to initiate the process that generates keys) should be generated using a sufficiently random process, or as the Cryptocurrency Security Standard (CCSS) puts it:

"The key or seed is generated using a Deterministic Random Bit Generator (DRBG) that conforms to NIST SP 800-90A, and has been seeded with at least two separate cryptographically secure sources of entropy that have been combined in a cryptographically secure manner (e.g. SHA256[UnguessableFactor1 + UnguessableFactor2])"

- They should be stored in encrypted form on a secure computer, with (at least) two-factor authentication required to access them

- It is prudent to use multi-signature wallets, where two or more keys (held by different people, on separate devices) are required to access funds

- A large proportion of the client's cryptocurrency should be in cold storage, meaning that the private keys are stored on a device that is not connected to the internet (cold wallet). Coinbase stores 98% of customer assets in cold storage

sEptu

Some relevant frameworks

- **CCSS (Cryptocurrency Security Standard)**
  A set of standards for information systems that make use of cryptocurrencies

- **ISO/IEC 27001**
  International risk management standard covering electronic, physical and contractual aspects of information security

- **PCI:DSS (Payment Card Industry Data Security Standard)**
  An information security standard for organisations that use branded credit cards

- **Mitre ATT&CK**
  Continuously updated matrices of tactics and techniques employed in cyberattacks, along with mitigations

- **OWASP 10**
  A list of the main known risks and vulnerabilities associated with websites and web applications, including automated attacks, and ways to mitigate them

sEptu

For more information: **robin.long@septu.tech**

Copyright © Septu Ltd 2020. All rights reserved