Security Analysis on Cryptocurrency Exchanges

PROFESSOR:

SAZZADUR RAHAMAN

STUDENTS:

MUAZ ALI (MUAZ@ARIZONA.EDU)

FAHMIDA ALAM (FAHMIDAALAM@ARIZONA.EDU)

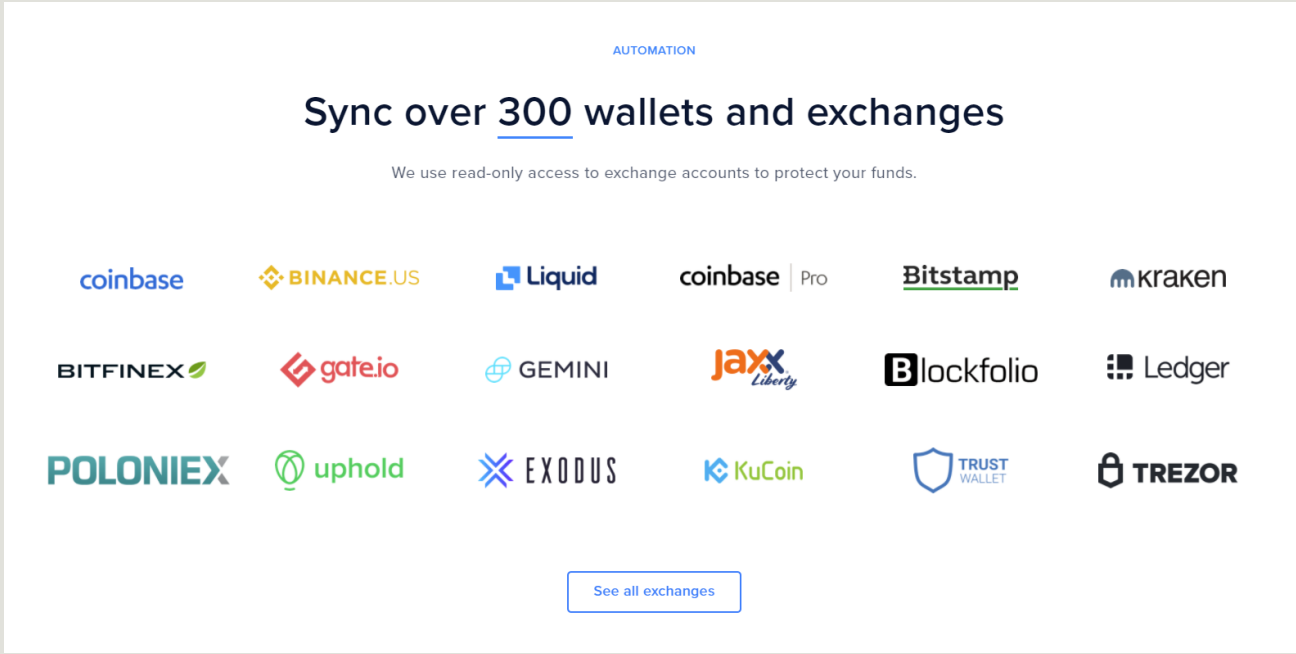
RUPAL JAIN (JAINRUPAL@ARIZONA.EDU)

PRIYA KAUSHIK (PRIYAKAUSHIK@ARIZONA.EDU)

PROBLEM

- 295 million blockchain cryptocurrency users.
- Most of them use cryptocurrency exchanges to perform transactions.
- These Exchanges store secret credentials of the clients (private keys).
- A surge in breaches in these exchanges
- It is important to inspect the security mechanisms of these exchanges

METHODOLOGY



- Select top 4 exchanges to perform analysis on: ***Binance, KuCoin, Bitfinex, Coinbase***
- Use state-of-the-art static analysis tool (Cryptoguard) to perform the security analysis of the android applications of cryptocurrency exchanges
- Perform a black-box forensic of the breaches that have been done on the selected exchanges.
- Using the insights from the study to suggest counter measures against future breaches

CryptoGuard

Binance analysed using cryptoguard

	Vulnerability	Instances found
1	Found broken crypto schemes	4
2	Used untrusted PRNG	17
3	Used untrusted HostNameVerifier	2
4	Used constant keys in code	6
5	Found constant salts in code	1
6	Used HTTP Protocol	17

```
private void m14650d() throws Exception {
    InputStream inputStream;
    InputStream inputStream2;
    BufferedOutputStream bufferedOutputStream;
    Throwable th;
    OutputStream outputStream;
    if (!this.f12916t) {
        String str = this.f12908l;
        if (!TextUtils.isEmpty(str) && Uri.parse(str).getScheme() == null) {
            str = "http://".concat(String.valueOf(str));
        }
        this.f12908l = str;
        HttpURLConnection httpURLConnection = (HttpURLConnection) new URL(this.f12908l).openConnection();
        this.f12914r = httpURLConnection;
        httpURLConnection.setConnectTimeout(this.f12910n);
        this.f12914r.setReadTimeout(this.f12911o);
        this.f12914r.setRequestMethod(this.f12909m.toString());
        this.f12914r.setInstanceFollowRedirects(this.f12912p);
        this.f12914r.setDoOutput(C6900c.kPost.equals(this.f12909m));
        this.f12914r.setDoInput(true);
        TrafficStats.setThreadStatsTag(1234);
```

- Examples of some vulnerabilities
- Case #1 : Used HTTP protocol

- Case #2 : constant key used

```
L_0x0098:
    java.lang.String r2 = "1542658731108"
    java.io.File r4 = new java.io.File
```

- Case #3 : Used untrusted PRNG

```
public final class zzyu extends zzzz {

    /* renamed from: f */
    private final Random f23045f = new Random();

    /* renamed from: g */
    private long f23046g;

    /* renamed from: h */
```

```java
/* renamed from: j */
private static String m36522j(String str) {
    try {
        byte[] digest = MessageDigest.getInstance("MD5").digest(str.getBytes("UTF-8"));
        StringBuilder sb = new StringBuilder(digest.length * 2);
        for (byte b : digest) {
            byte b2 = b & 255;
            if (b2 < 16) {
                sb.append("0");
            }
            sb.append(Integer.toHexString(b2));
        }
        return sb.toString();
    } catch (NoSuchAlgorithmException e) {
        throw new RuntimeException("Huh, MD5 should be supported?", e);
    } catch (UnsupportedEncodingException e2) {
        throw new RuntimeException("Huh, UTF-8 should be supported?", e2);
    }
}
```

- Case #4 : MD5 Function used without incorporating salts

- Founded in 2013 by Michael Gan, Eric Don, Top Lan, Kent Li, John Lee, Jack Zhu, and Linda Lin, and was launched in September 15, 2017
- Grown into one of the most popular crypto exchanges and already has over 8 million registered users from 200+ countries and region
- Established local communities all over the world such as South Korea, Japan, Spain, Italy, Vietnam, Turkey, Russia, India, and other regions.
- However, restricted for US citizens due to a lack of license and the KYC (Know Your Customer) process.
- The exchange has over 200 cryptocurrencies, more than 400 markets, and has grown into one of the most colorful crypto hubs online
- Available cryptocurrencies are Bitcoin, Ethereum, BitcoinCash, EOS, Litecoin, Ripple, Dash, Cardano, Stellar, NEM and some of the supported fiat are USD, EUR, GBP, AUD.

CRYPTOGUARD STATISTICS

Rule	Vulnerability	Instances found
1	Predictable/constant cryptographic keys.	1
2	Predictable/constant passwords for PBE	67
3	Predictable/constant passwords for KeyStore Confidentiality H	3
4	Custom Hostname verifiers to accept all hosts	3
6	Custom SSLSocketFactory w/o manual Hostname verification	2
7	Occasional use of HTTP	9
10	Static Salts in PBE	25
13	Fewer than 1,000 iterations for PBE	57

MAJOR HACK

- On September 25, 2020, the cryptocurrency exchange KuCoin was hacked.
- Estimated stolen cryptocurrency amount is around $281 million in various cryptocurrencies.
- A North Korean hacker crew called Lazarus Group has been accused of carrying out this breach.
- However, KuCoin recovered 84% of stolen crypto after the hack and insurance funds covered the 16% unrecovered from the incident.

BREACH ANALYSIS

- The hack was due to a leak of the KuCoin hot wallet private keys.
- Private key, a randomly generated number that signs transactions and protects user's assets from malicious attacks. If it gets compromised or lost, users won't be able to access their crypto wallet to spend, withdraw, or transfer their coins.
- Stolen cryptocurrencies were stored in hot wallets (where the private keys are available in a database connected to the internet) which did not require multiple signatures (multi-sig) by operators of the exchange to clear an outgoing transaction.
- Therefore, the hackers were able to retrieve the wallet's private keys and sign the subsequent outgoing transactions without significant challenges and breached the security.

BREACH ANALYSIS

Probable way to obtain private keys:

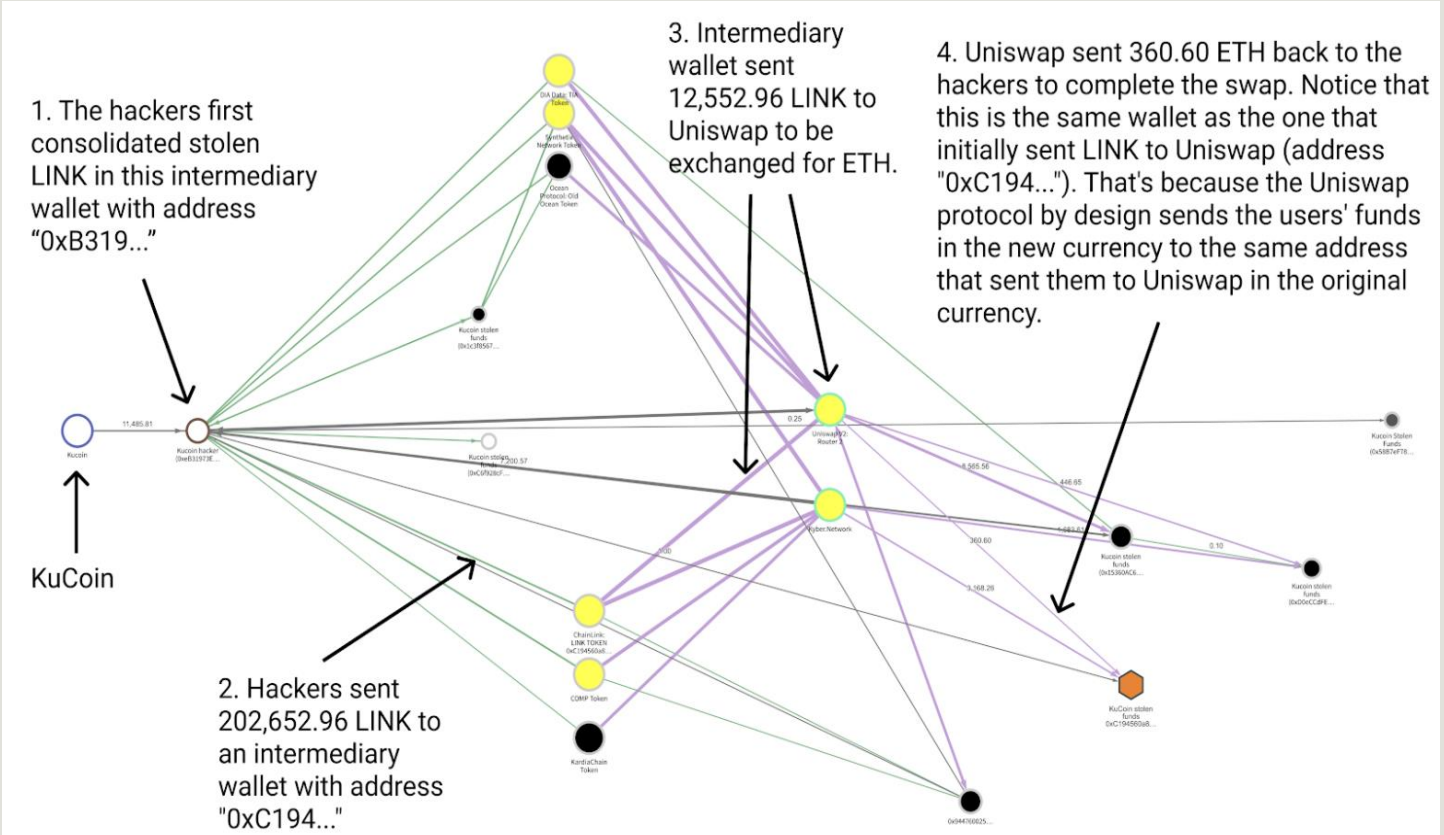
- **Social engineering attack -** Hackers could obtain access to private keys as a result of a phishing attack by using exploits, viruses, and backdoors on employees who had access to private keys.

- **Malicious actions of responsible employees -** This could have been done by someone from the exchange staff who had the appropriate access.

- **Attack on web infrastructure -** An attacker could gain access to the exchange's hot wallet services.

BREACH ANALYSIS

- Lazarus Group used DeFi platforms to launder a portion of the stolen funds.
- DeFi platforms allow users to swap one type of cryptocurrency for another without taking KYC information from customers, making it easier for cybercriminals to move funds with greater anonymity.
- In this case, the KuCoin hackers used platforms like Uniswap and Kyber



Green lines represent ETH or Token transfers. Purple lines represent DeFi platform interactions.

PREVENTION

- Using specialized hardware wallets that store private keys offline. Stealing private keys from a hardware wallet would require physical access to the wallet and corresponding PIN or the recovery phrase.
- The hot wallet must be reinitialized periodically.
- Two-man rule can be adopted such as using secret sharing schemes.
- One must not store more than 5% of all deposits in the hot wallets and 95% must be stored in a cold wallet.
- User should store crypto in several hot wallets for each cryptocurrency platform and each wallet must have its own private key.
- Performing regular penetration tests, phishing simulation, red team exercises are must.
- Performing audits of the cryptocurrency storage system that is included in SOC2 and/or ISO27000 auditing is also compulsory.

- Founded in December 2012 by Raphael Nicolle and Giancarlo Devasini.
- Owned and operated by iFinex Inc, a Hong-Kong based company and is registered in the British Virgin Islands.
- It is a peer-to-peer Bitcoin exchange digital asset trading which provided services to the users across the world.
- 4 Fiat currencies as USD, EUR, JYP, GBP and 10 Cryptocurrencies as Bitcoin, Bitcoin Cash, Ethereum, Ethereum Classic, Litecoin, Ripple, OmiseGO, Monero, NEO, EOS.
- Bitfinex was started as P2P margin lending, exchange trading, margin funding, OTC Desk platforms for Bitcoin but later they also added some more cryptocurrencies.
- List of countries prohibited from accessing the exchange includes Iran, North Korea, Cuba, Syria, Crimea, Donetsk People's Republic, and the self-proclaimed Luhansk People's Republic. Apart from them U.S. citizens, citizens or residents of Canada, the British Virgin Islands, the Government of Venezuela and residents of Austria or Italy are also restrained from accessing the Bitfinex application.

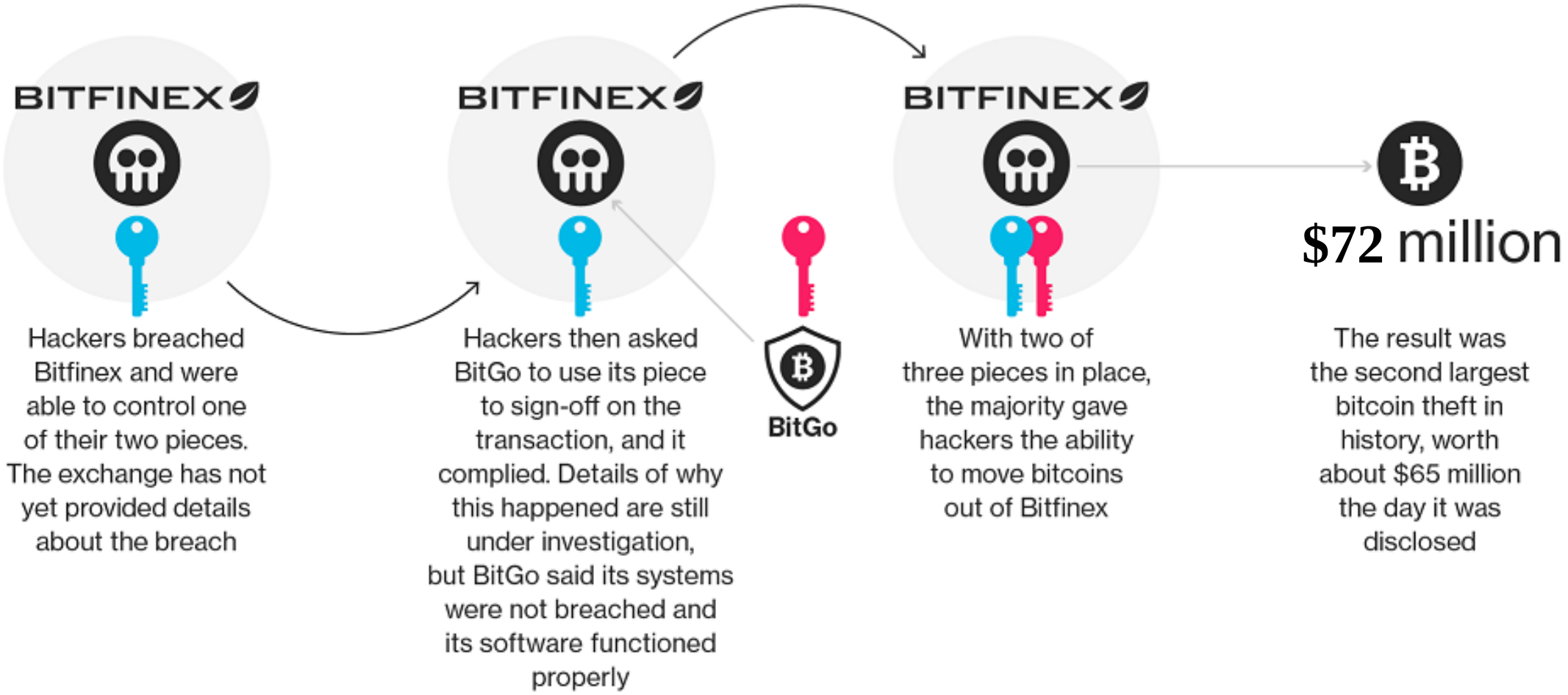
CRYPTOGUARD STATISTICS

Rule	Vulnerability	Instances Violated
2	Predictable/constant passwords for PBE	27
6	Custom SSLSocketFactory w/o manual Hostname verification	1
7	Occasional use of HTTP	6
8	Predictable/constant PRNG seeds	23
10	Static Salts in PBE	5
11	ECB mode in symmetric	1
13	Fewer than 1,000 iterations for PBE	49

MAJOR HACK

- Bitfinex suffered a major security breach on August 2, 2016 which become the second-biggest breach of a Bitcoin Exchange platform.
- A New York couple, Ilya Lichtenstein, and his wife, Heather Morgan, a U.S. national stole 119,756 units of Bitcoin, worth about $72 million.
- Hackers initiated 2000 approved transactions and the funds were sent to a single wallet called “Wallet 1CGA4s5”.
- Bitcoin's trading price plunged by 20% which caused the value of the stolen Bitcoin to dip to US $58 million.
- In early 2017, 10% of funds made an exit from the Wallet 1CGA4s5.
- The hackers then carried out the transfer through Alphabay (darknet market). After routing the Bitcoin through Alphabay, the trail of money on the blockchain itself would run cold (offline).
- After Alphabay shutdown, the hackers routing the money through Hydra.
- Within three years spent, the launderers took another transaction known as “Coinjoin” using Wasabi wallet.
- The stolen bitcoin was lying in hackers account from August 2016 until January 31, 2022, worth $7.45 billion.
- On 10 February 2022, Heather Morgan was detained in Manhattan, followed by her husband, Ilya Lichtenstein who was caught 8 February 2022.
- The couple was being federally charged in February 2022 with intrigue to laundering the Bitcoin that lead to 20 years of lock away and conspiracy to cheat the United States which leads to 5 years of lock up.

How Hackers Pulled Off a $72 Million Dollar Heist



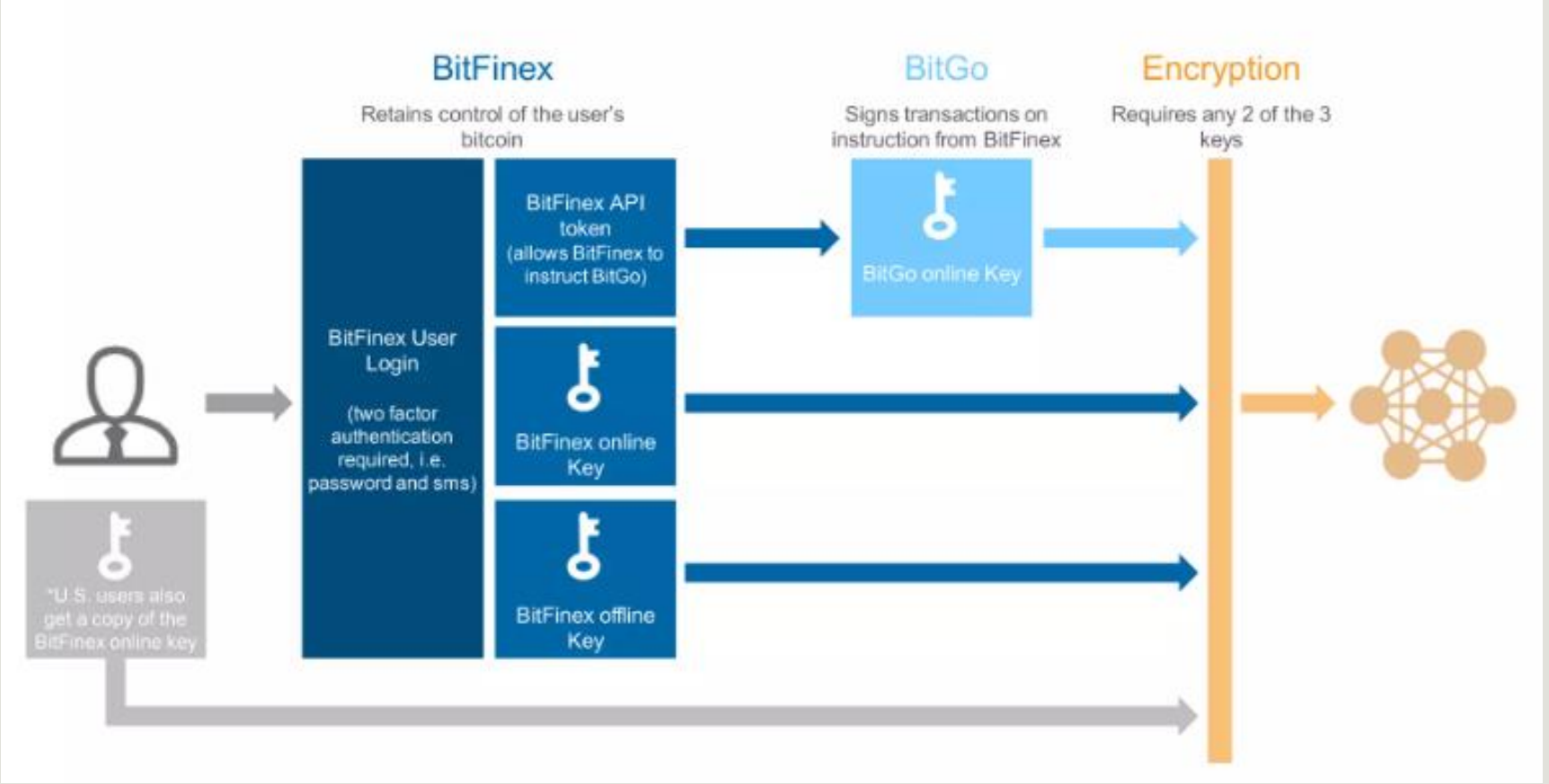
Bloomberg

BREACH ANALYSIS

- Bitfinex uses two-factor authentication, Universal 2nd Factor (U2F) authentication, advanced APIs for connecting third-party services, withdrawal protection features. These include storing 99.5% of user funds in cold storage, DDoS protection, database encryption, and regular backups.
- Bitfinex was securing the funds with BitGo, which uses multiple-signature security. Its wallets has 3 keys: one held by BitGo, and two held by the wallet's owner.
- On January 31, 2022, law enforcement gained access to Wallet 1CGA4sand obtained a search warrant for a cloud storage account belonging to Lichtenstein (hacker), where they found a spreadsheet.
- Law enforcement could have obtained access to the password somehow and didn't need to brute force its way through the files in the cloud storage. After decrypting the file, they found 2,000 virtual currency addresses, along with corresponding private keys linked to the hack with their passwords.
- Each virtual currency address has a corresponding private key, which is roughly equivalent to a complex password or PIN code.
- Private keys are essential to operating bitcoin wallets and are long alpha-numeric chains.
- Using Lichtenstein's passwords in the cloud, the investigators entered the account and seized the funds.

BREACH ANALYSIS

- Due to the openness and transparency of the blockchain, law enforcement was able to track the money.
- The source of the vulnerability appears to lie in the structure of the Bitfinex accounts and its use of bitcoin wallet provided by BitGo which is an additional layer of security on user's transactions.
- One cause is the Bitfinex itself, since it had the ownership of 2 out of 3 private keys needed for the funds lost from the multi-signature accounts. Advocacy group Coin Center has claimed that multi-sig is one of the security approaches that is prone to vulnerability or failure.



PREVENTION

Ways by which Bitcoin user can protect their Bitcoin in the view of security.

1. Bitcoin can be stored entirely offline on a secured hard-drive, called “cold” storage.

2. The most efficient way to hold a wallet is on a “custodial” basis because in this way the exchange operates and controls a single wallet or a set of wallets for its clients with its clients essentially being allocated bitcoin within that wallet.

3. To prevent hacks on hot wallets, we can deploy multiple private keys to operate the wallet. One key will be held by the exchange and the other with the user.

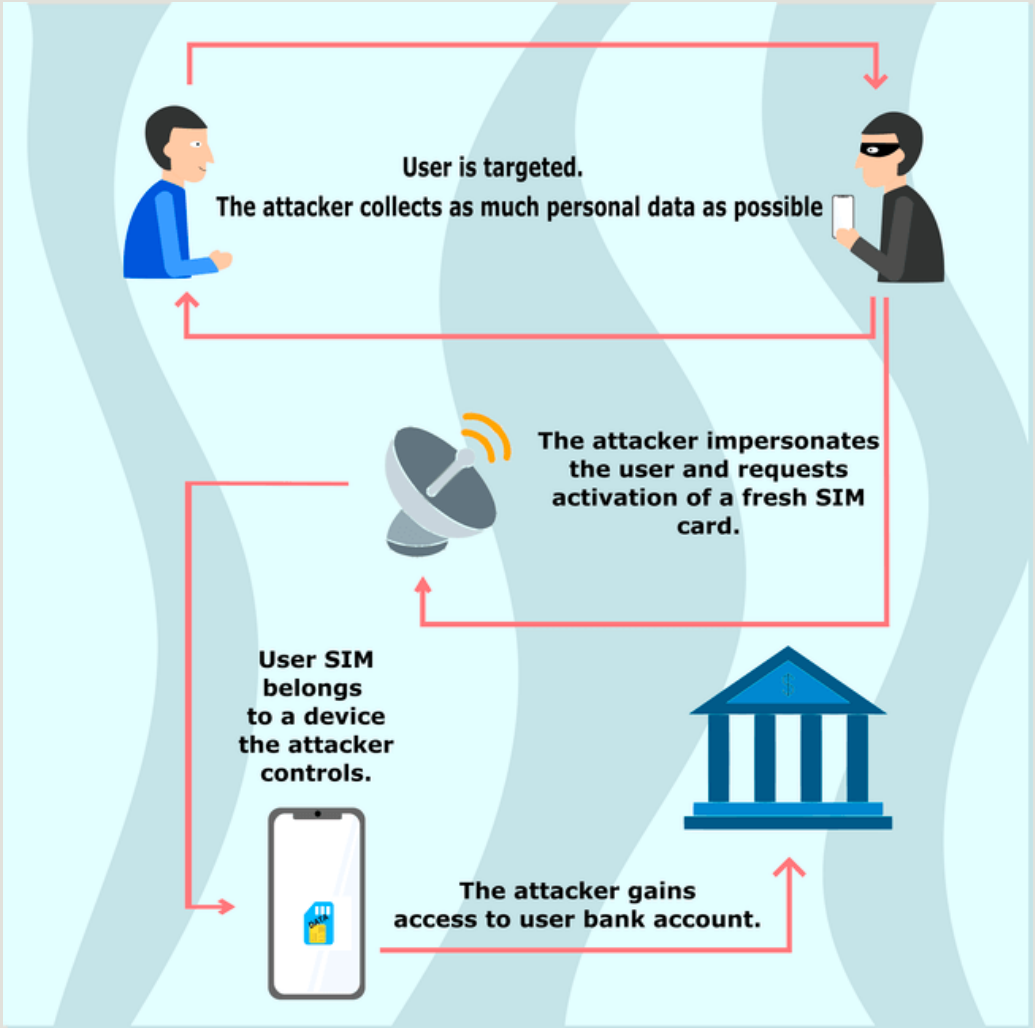
- Founded in June 2012 by Brian Armstrong & Fred Ehrsam.
- It is the largest cryptocurrency exchange trading more than 170 cryptocurrencies.
- In October 2012, the company launched the services to buy and sell bitcoins through bank transfers.
- Coinbase is an app used to buy, store and trade different cryptocurrencies, such as Bitcoin, Bitcoin Cash, Ethereum, Ethereum Classic & Litecoin.
- Coinbase has a mobile app for both iOS and Android.
- On April 14, 2021, Coinbase became a public company on the NASDAQ exchange via a direct stock lisiting.

MAJOR HACK

- Hackers stole from the accounts of at least 6,000 customers of Coinbase Global Inc between March and May 20, 2021.
- Affected Coinbase customers had funds removed from their accounts.
- Attackers targeted phishing emails to achieve access to victims' email inboxes.
- They aimed to exploit a flaw in Coinbase's two-factor SMS system to break into Coinbase user accounts.
- Coinbase accepted that a vulnerability existed in their SMS account recovery process.
- This has allowed hackers to gain the SMS two-factor authentication token needed to access a secured account.

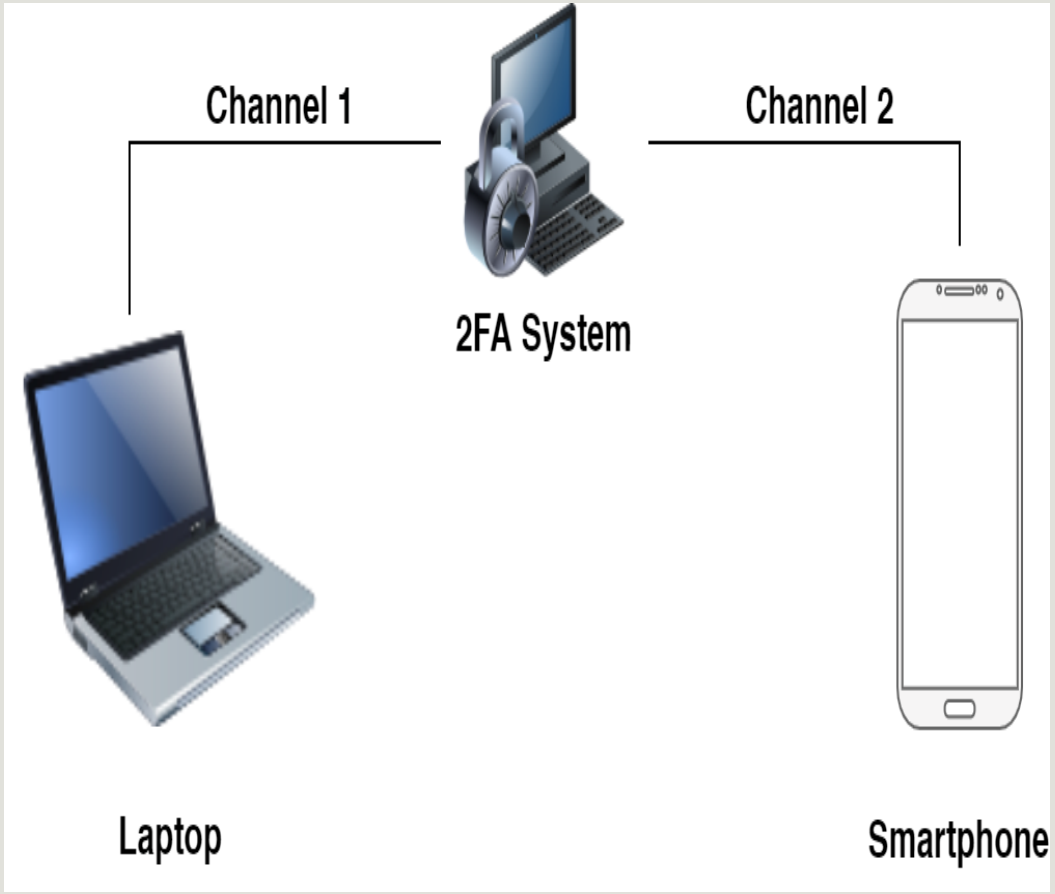
BREACH ANALYSIS

- One of the reason for such incident could be SIM Switching.
- Clearly, the attacker has the access to the customer's phone number which they transferred to their own device which was under their control.
- This SIM swapping would further lead to RDP(Remote Desktop Protocol) Attack.
- In, RDP Attack, the attacker gains the control of the computer over the internet.
- It's commonly used for customer support.
- And many of the RDP attacks seen these days are the brute-force attacks.
- When scammers have enough data, they impersonate you and pretend to have lost or damaged (your) SIM card to the Customer Care Executives.



INSTEAD OF USING SMS 2-F AUTHENTICATION:

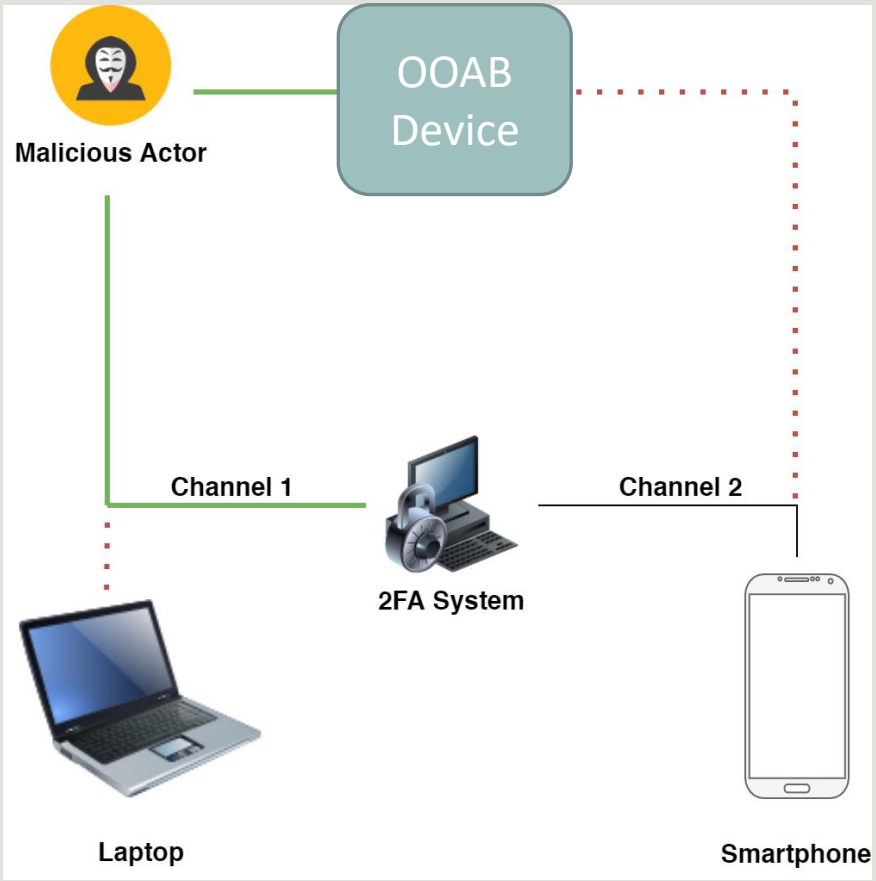
- **QR Codes:** It is a more visual representation of One Time Passwords and we can make sure the website the QR code links to is SSL certified and encrypted.
- **Mobile Push Notifications -** It is resistant to many types of attacks, e.g., keylogging. Mobile Push is a valid form of Out-of-Band Authentication(OOBA).
- OOB Authentication can help prevent man-in-the-middle attacks by introducing an extra channel of communication between the user's phone and the 2FA system.
- OOB makes attacks much harder for hackers because now they need access to both communication channels to successfully break the system.



INSTEAD OF USING SMS 2-F AUTHENTICATION:

- **Use an OOAB DEVICE :** Out-of-Band Device is an authentication device that establishes an additional channel of communication with a 2FA system to receive an authentication request.

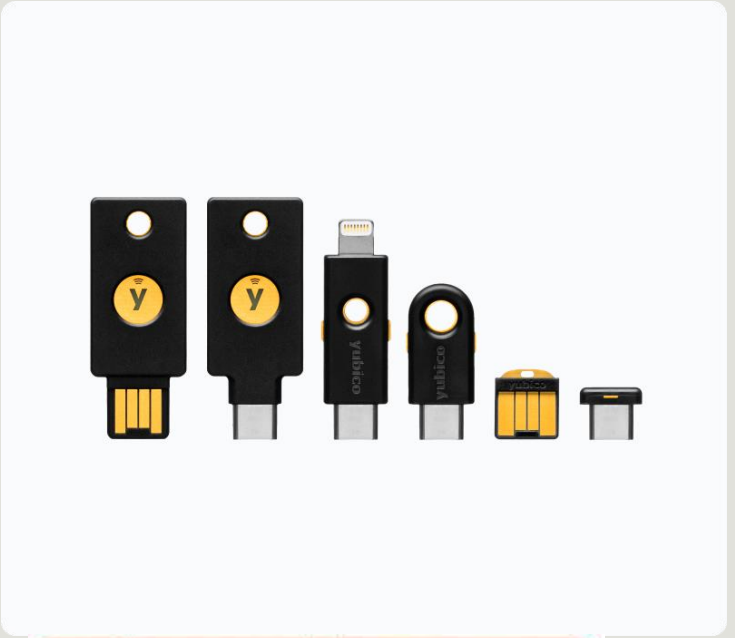
- Even if a malicious actor manages to insert themselves into the first channel of communication and intercepts User's password, the hacker is derailed by the push notification sent over another channel.



INSTEAD OF USING SMS 2-F AUTHENTICATION:

- **U2F Security Keys :** Many organizations opt for hardware authentication, which requires a dedicated physical device for account access. Sign in requires users to know and enter their credentials, then they are prompted to submit additional proof of identity by inserting the key and tapping it.

- Example: YubiKey, Token2



REFERENCES

- https://en.wikipedia.org/wiki/Coinbase#2012%E2%80%932019:_founding_and_early_years
- https://privacypros.io/u2f/sim-swapping/
- https://securityboulevard.com/2021/12/why-using-sms-authentication-for-2fa-is-not-secure/
- https://www.darkreading.com/threat-intelligence/rdp-attacks-persist-near-record-levels-in-2021
- https://www.vice.com/en/article/5dmbjx/how-hackers-are-breaking-into-att-tmobile-sprint-to-sim-swap-yeh
- https://rublon.com/blog/what-is-out-of-band-authentication-ooba/
- https://en.bitcoinwiki.org/wiki/KuCoin
- https://golden.com/wiki/KuCoin_Exchange-NMGDK49
- https://cryptonews.com/reviews/kucoin/
- https://kuwallet.com/?spm=kcWeb.B1homepage.Header8.1&utm_source=kucoin_web
- https://www.privateinternetaccess.com/blog/is-kucoin-available-in-us/
- https://www.kucoin.com/news/en-privacy-policy
- https://www.ledger.com/coin/wallet/kucoin-shares
- https://blog.coinmarketcap.com/2020/10/16/kucoin-september-2020-hack-hacken-research/

REFERENCES

- https://thegenesisdaily.medium.com/kucoin-hack-explained-by-crypto-curry-live-956aeffa4285
- https://hacken.io/insights/kucoin-september-2020-hack-hacken-research/
- https://www.justice.gov/opa/press-release/file/1470211/download
- https://www.jdsupra.com/legalnews/the-us-4-5-billion-bitfinex-hack-five-7029856/
- https://www.allenovery.com/en-gb/global/news-and-insights/publications/bitfinex---could-greater-regulation-have-prevented-its-hack
- https://bitcoinmagazine.com/technical/how-authorities-found-bitfinex-bitcoin
- https://www.coolwallet.io/bitfinex-hackers-lessons-for-crypto-security/
- https://time.com/6146749/cryptocurrency-laundering-bitfinex-hack/

THANK YOU!