remme

Cryptocurrency Exchange Security Risk Mitigation with REMME

Research Paper

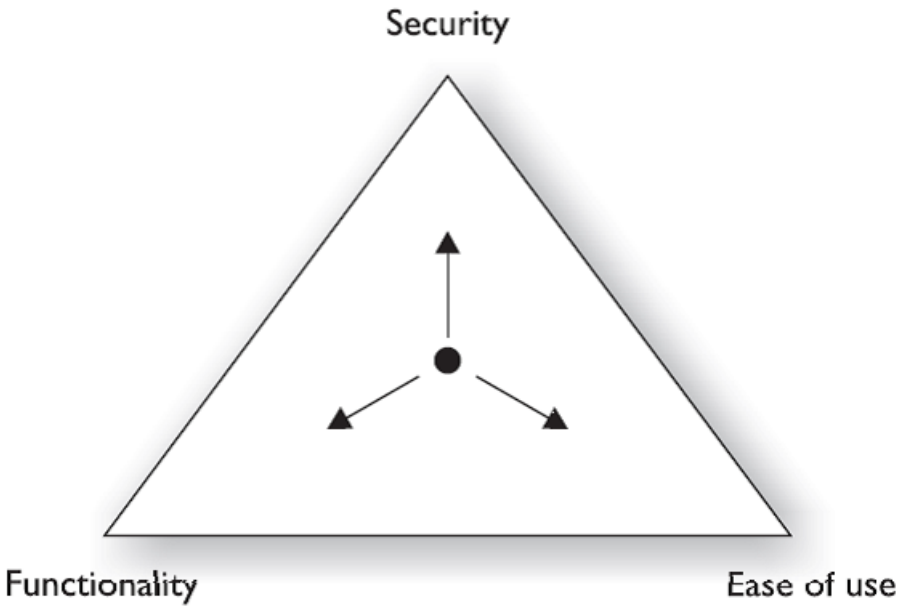
Authors: Daniel Hall, Oleksii Baranovskyi, Alex Momot

remme.io

April, 2018

Introduction

This research paper investigates the two main areas of risk in relation to using a centralized cryptocurrency exchange such as Bittrex or Binance in addition to possible mitigation techniques. The premise of this paper is based on the security triangle below whereby any solution will occupy a single point within the triangle, and improving one attribute will always move it further away from the others. Any solutions outlined in this paper, will aim to strike a **balance between Ease of use, Security and Functionality**. However, the quality, depth and sustainability of this balance require increase cost, it is the aim to demonstrate that REMME's service offerings can help manage and reduce this cost through wider adoption and economies of scale rather than taking a "roll your own" technique.



Risks affecting usage of exchanges

1. Being re-directed via a DNS-hijacking, fake DHCP server, clickjacking and other attacks or accidentally ending up on a phishing site

Risks:

- Loss of funds
- Loss of user credentials

The count of such kind of attacks has been on the rise recently. Also we should mention that black SEO and malvertising became more and more popular: phishing sites being advertised via search engines like Google and Bing so that they appear higher up the list than the official site with help of contextual advertising and different SEO techniques. These sites' uses the same title and description as the official site listing and makes use of a domain with a similar name (e.g. by replacing a "l" symbol with "i" for example). The site itself is built to look visually similar and also could re-direct the end user to the legitimate site after harvesting 1 or 2 two factors authentication (2FA) credentials. These credentials are then used to steal user's funds or been used into advanced attacks to other user's. For example, phishing attack was recently used on the Bittrex exchange*. Relying on SSL/TLS certificates will not save you here as the attackers can use a non self-signed certificate easily obtained through services such as LetsEncrypt. This results in the user not getting a warning about an invalid certificate and will instead see the padlock icon that they have likely been told to look out for. While the attackers will not have a fully verified certificate (green bar), it will at least not prompt any concern from most users.

Another different attacks are DNS-hijacking and DNS cache poisoning. There are different techniques but with the same outcome involves an

attack on the DNS servers used for resolving the sites hostname. So instead of www.binance.com sending you to it's ip address, it would instead send the user to a fake site IP address, again used to harvest funds, this would even work if entering the correct address for the site. This type of attack was recently used on the Etherdelta exchange**. Hackers can create new SSL/TLS certificate for fake site using a CA that checks special DNS entry to prove ownership, which in this case, is of little use as the attacker already controls the DNS server and any entries on it for the domain in question.

Mitigation

Since these types of attacks do not involve using a vulnerability on an exchange, and instead re-direct the user before they even get to the site, this would likely be the best method of mitigation by verifying that the site a user is on is indeed the correct site. Also site an proof that user is correct user with two way SSL/TLS authentication. This could be achieved by having the exchanges and users public certificate status (valid or revoked) stored on the REMME blockchain. There is no additional risk to the parties, as it is only their public certificate being used. Utilizing either a mobile app or browser plugin (best if required for higher verification levels with the exchange), a user could be protected by having the application verify the certificate being served by the website also matches the public certificate status being stored on the REMME blockchain and has not been revoked. While this would likely carry a cost for the exchange, reducing the risk of bad press may well be worth it. This implementation takes little away from the easy of use of the service, increases security and, surprisingly, functionality according to new possibilities of ceritificate-based authentication and would not likely carry a huge cost when taking into account the benefits.

This measure also acts as a precursor for the next mitigation below, and could be used as a method to sign up exchanges to REMME, albeit on a lower tier initially.

Advantages:

- Simplified UX for users
- Greatly reduced risk

Disadvantages:

- Could require a separate application or API integration

2. Logon details being stolen

Risks:

- Loss of funds
- Loss of user credentials

While this has a similar outcome to item 1 above, there are a multitude of ways that a bad actor may obtain a users logon credentials, as these may not be limited to Phishing/DNS attacks, it is worth listing as a separate item as detection is much harder, and so a different response is required. These attacks may take the form of key loggers, malware built to look for login credentials stored in plain text or even social engineering attempts such as someone looking over your shoulder in a public place or stealing your identity (using DOB, Mothers maiden name etc) in order to persuade your cell network provider to activate a new SIM card in the possession of the attacker (to have your 2FA codes sent to them instead of yourself***)

Once the implementation in item 1 is completed, a further implementation can be carried out with the aim of protecting access to the users' accounts in a more general way. Most exchanges allow and even recommend two-factor authentication (2FA), this means a user must provide both a

username/password in addition to a one-time code from an authentication service such as Google Authenticator or Authy, some also offer SMS text messages or phone call as a medium for receiving these codes. While the likes of Authy are generally considered fairly secure, there is still a risk that a bad actor can obtain the users backup codes, additionally SMS 2FA is proven to be insecure due to the different type of possible attack's: SIM cloning, active GSM interception, provider interception etc.

This implementation looks to outline a multi-factor authentication method that is effectively 4FA minus biometrics plus PKI, so 4FA-B+p or it can simply be referred to as Multi Factor Blockchain Assisted Authentication (MFBAA). The premise is that while REMME looks to remove Username/Password requirements, in the case of digital currency and the state of the current ecosystem, it makes sense to add as many hurdles as possible for an attacker, without putting much additional onus on the user and applying significantly increased costs to the service provider (exchange). This would be achieved by once more, utilizing a mobile app, messaging app (Telegram, Facebook Messenger or others) or desktop browser plugin that acts as a secure gateway to the exchange and requiring any or ideally all of the below:

- Username
- 2FA code (e.g. Authy) or 2FA approve using messaging app or REMME app
- REMME private certificate (with public held on blockchain for verification)
- Geo-fencing data
- Finger print lock for mobile devices (user optional)

An exchange would allow a user to set a list of locations (that are not able to be displayed after the fact) that they want to allow logins from, blocking or restricting withdrawal of funds if this is not met. This could either be exchange specific, or held encrypted in the public certificate CN fields. This can be read by the users' app, decrypted using the private certificate and

sent via SSL/TLS to the exchange. If the location of the device (IP and/or GPS) is not within the geo-fence then access can be blocked. (another potential option would be to use/partner with a location verification service, such as the the proof-of-location outlined by FOAM here: http://bit.ly/2n6stGI)

The private certificate held on the device would also be used as an additional factor for login. When enabled, the exchange would use the public certificate on the REMME blockchain for verification with the username.

If utilized, this method could greatly reduce the risk of an attacker being able to login successfully as they would need the username, 2FA code, private certificate and location data. Whilst the exchange is only doing 2 extra checks per login (automatically), and the user still has an easy to use authentication method.

One of the possible ways of implementation may look as follows:

1. Go to the exchange you want to login to
2. Exchange website SSL/TLS cert is verified against certificate held on the REMME blockchain
3. Confirm authentication using the second factor (REMME 2FA, Google Authenticator, Yubikey, etc)
4. REMME application seamlessly sends a message signed with the private key to be verified by the exchange using the public key
5. REMME application seamlessly grabs encrypted location data from the REMME blockchain, decrypts it and sends it to the exchange via SSL/TLS and signed by the private certificate
6. Once all checks are passed, exchange grants access

It is possible to use messaging app (Telegram, FB Messenger) instead of REMME app. This will make process even easier and step #6 will not be

needed. It could be other combination of factors based on specific needs of exchange.

User facing process

1. Go to the exchange you want to login to
2. Click “Login” button
3. Confirm authentication using the second factor
4. Logged in

For the highest security, all of the above items would be recommended, however, even just using the certificate check from the previous section coupled with certificate-based authentication from the device would help to improve security greatly.

Advantages:

- Little to no increased workload for users
- Greatly reduced risk

Closing Comments

The use of REMME's PKI (d) on blockchain is key to ensuring that the exchange website has not been compromised and that only the account owner can login. While nothing is 100% secure, the above mitigations go a long way to reduce the success of an attack. While new attack methods are likely to surface in the future, REMME is well positioned to help exchanges and their users face these threats with a greater confidence than currently.

An additional benefit of the model outlined, is that it could also integrate with identity providers used for KYC on exchanges and ICO events. This would ensure that a user has the authority to submit the KYC data in question, and that the site has not been compromised. This helps to give confidence to the user, ensures that their KYC data is secure, and also offer a more streamlined process for completing KYC requirements.

User experience is key to gaining mass adoption of cryptocurrency, however giving up control to centralized entities should be avoided where possible. And the mitigations listed above can serve as a starting point to achieve this.

References:

1. * https://www.newsbtc.com/2017/08/29/new-bittrex-phishing-scam-website-tops-google-search-results/
7. ** https://themerkle.com/etherdeltas-dns-hacked-website-replaced-with-hackers-duplicate-to-steal-funds/
8. *** https://www.theverge.com/2017/9/18/16328172/sms-two-factor-authentication-hack-password-bitcoin
9. **** https://bitcoinexchangeguide.com/top-cryptocurrency-theft-hacks/