MAS.S62 - Cryptocurrency Engineering and Design

Anthony Rolland
William López-Cordero
Miranda N McClellan
Elorm Koto
Irene Hernandez

Project Proposal: **Enhanced Key Recovery**

Background

A rising concern over cryptocurrency wallets is the fact that consumers are required to take full responsibility over authentication credentials; that is, private keys. If the user loses their private key, they cannot recover their funds. Public Key encryption is widely used in security systems; however, the general public's understanding of authentication methods is limited to the use of username and passwords they have experience with. This poses a security risk in itself, in that users will manage private keys with the same degree of carelessness as they manage passwords. Many users might store private keys insecurely on cloud storage, lose the USB or phone the key is stored on, or misplace the paper the key is written on. For this reason key recovery methods are popping up in the crypto world.

BiP39 is one of the most common key recovery methods for cryptocurrency wallets. BiP39 relies on the user memorizing an ordered 12 word sentence used to recover the seed of the private key. This method, albeit increasingly popular, solves neither of the current issues of convenience nor security. Because the length of the sentence is too long, the majority of users often write the phrase down on an electronic file or physical paper, which leads to the same storage challenges faced with the original private key. Other methods, which leverage multisignatures, include a collaborative approach, where friends or other trusted parties are designated to assist in the key recovery. This approach does not burden the user with credential storage, but requires them to interact with and trust the other parties in their recovery network. If these parties not available or not cooperative, the key recovery can take too long to be reliably convenient or not occur at all.

Proposed solution

Our team proposes a new private key recovery method to enhance the usability and security of existing key recovery methods. We will investigate cryptographic proofs such as Diffie Hellman, Shamir's Secret Sharing Scheme (SSSS), Fuzzy Vault Encryption, and BIP39.

Particularly, we will explore the use of fuzzy extractors to encrypt and authenticate BIP39 phrase codes with biometric fingerprints as keys. Fuzzy Vaults allow to encode and unlock a secret with keys that are not identical, but very similar. Since biometric fingerprints cannot be reproduced exactly, fuzzy vaults represent an enabling tool to incorporate biometric security. To add an extra layer of security, we will explore the possibility of using SSSS to split the passphrase and then lock each piece with a different fingerprint in fuzzy vaults. In order to retrieve their secret key, a user must have all fingerprints and remember the specific order in which they were signed.

Objectives

- Improve on existing key recovery methods for cryptocurrency wallets
- Enable users to recover private keys for accounts without trusted third party
- Enable users to store their private mnemonic phrase or other recovery information securely to prevent permanent loss of data/money
- Enable users to recover their private mnemonic phrase in a fast and convenient way without current potential leaks of data .

Deliverables

The main deliverable for the final project is the definition and implementation of a novel enhancement to current key recovery methods that is non-interactive, more secure than BIP39, and based on cryptographic proofs.

Development Timeline

4/18/2018 - Project Proposal Deadline
5/11/2018 - Final Code Submission
5/14/2018 - Final Presentations

References

https://en.wikipedia.org/wiki/Shamir%27s_Secret_Sharing#Shamir's_secret-sharing_scheme
https://pdfs.semanticscholar.org/0c6d/4f9d14be760d3786617aab4e5c49ed61f142.pdf
https://pdfs.semanticscholar.org/32fc/d7eeba1aa594e76dbef944f4a74dddfdf1c3.pdf
https://www.geeksforgeeks.org/implementation-diffie-hellman-algorithm/
https://en.wikipedia.org/wiki/Elliptic-curve_Diffie%E2%80%93Hellman
https://en.wikipedia.org/wiki/Diffie%E2%80%93Hellman_key_exchange
https://en.bitcoin.it/wiki/Mnemonic_phrase
https://www.ncbi.nlm.nih.gov/pmc/articles/PMC4385657/
https://pdfs.semanticscholar.org/51eb/01e8a6170f40bbda1d3b89aff04bad14a5d3.pdf