Hardware Backed Bitcoin Wallet

Degree programme: BSc in Computer Science
Thesis advisors: Prof. Dr. Kai Brünnler, Prof. Dr. Benjamin Fehrensen
Expert: Cyrill Brunschwiler

Android Bitcoin Wallet is one of the most popular open source wallets. It gives the user the option to protect their funds by encrypting the wallet using a PIN. Currently, it doesn't use security features like biometric authentication and Android KeyStore. This project adds the option to encrypt the wallet with a hardware-backed key requiring biometric authentication to increase security.

Motivation

Bitcoin is a P2P distributed currency and payment network that operates without intermediaries, such as banks. As Bitcoin becomes more popular, the wallets used to manage it are increasingly targeted by attackers. If an attacker obtains the private keys necessary for spending Bitcoin, they gain complete control over all the associated funds. This underscores the critical importance of protecting the wallet and its private keys.

Goal

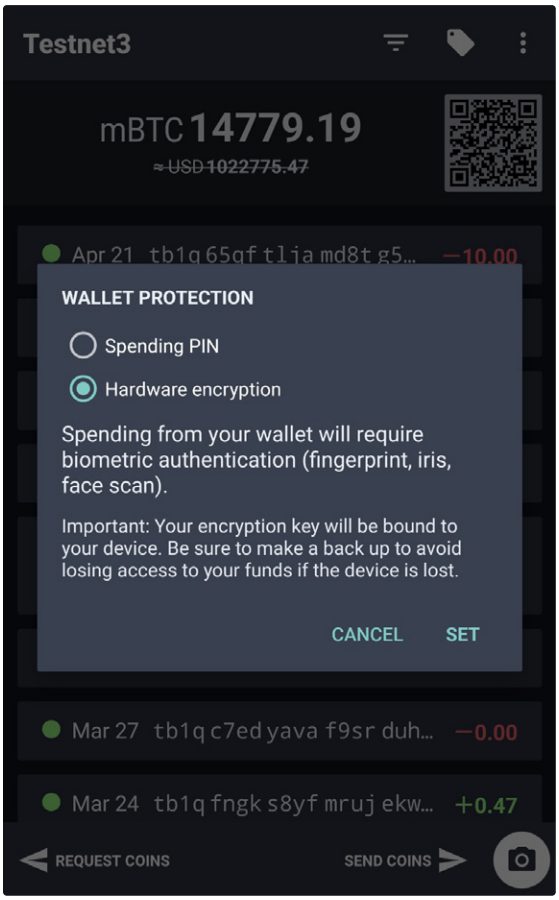
Currently Bitcoin Wallet provides the user with the possibility to set a PIN to encrypt the wallet. To increase the security of the wallet, we propose a new way to secure the wallet by using biometric authentication and the Android KeyStore. Security is increased by using secure entropy sources for key generation and protection against key extraction by storing the wallet encryption key in a biometrically protected KeyStore container.

Android KeyStore

Android KeyStore is used to generate and store cryptographic keys in a non-exportable secure storage environment which can be protected by biometric authentication. Android KeyStore uses the trusted execution environment (TEE) or, if available, an embedded secure element (SE) which provide a logically, or in the case of an SE physically, isolated execution environment that is separate from the main operating system and ensures strict access control.

Results

The introduced changes allow the user to choose between the PIN option or the newly introduced hardware-backed key encryption. When hardware-backed encryption is used, a key is generated inside the Android KeyStore. The wallet gets a reference to the key and transmits the plain text data to the secure environment, receiving back the encrypted data. This ensures that the cryptographic key doesn't enter the application memory. If the user wants to spend funds from the wallet, they will be prompted to provide biometric authentication, such as a fingerprint scan. This will unlock the key which is then used to temporarily decrypt the wallet and sign transactions. With this project, we successfully implemented biometric authentication and opened a pull request on GitHub with the proposed changes. Currently we are in contact with the repository maintainer, Andreas Schildbach, to integrate the changes into Bitcoin Wallet.



Oliver Aemmer
IT Security

Sebastian Nicol
IT Security