COMP3004B - Deliverable 4

Metadata

Team Name: Hyggelig Security
Application: hyggelig secure
Team Members:

- Kavan Salehi 101046945
- Connor Stewart 101046945
- Kevin Sullivan 100896774
- Gabriel Valachi 101068875

App Functionality

Cryptocurrency Subsystem

The cryptocurrency subsystem currently allows users to create public blockchain addresses to send or receive cryptocurrency using Block.io. As Block.io hosts the wallet that transactions are made against, private addresses are handled by Block.io. As such, FR4.1 is satisfied. The crypto activity also shows users their wallet balance upon opening the activity, and users are also able to check the balance of individual blockchain addresses in addition to their entire wallet, satisfying FR4.2.

Help Subsystem

The Help Subsystem uses a database to store text with a short explanation of how the activities offered in hyggelig secure help improve their security and privacy. Users can access these help pages through the Help activity, satisfying FR5.1. It was decided not to pursue completion of FR5.2, as the application consists mainly of buttons with explanatory text, and no hidden functionality. A tutorial for the current system would mainly consist of showing the user each activity, which should be an exploration of the app that comes naturally given the layout of the main menu. The help subsystem successfully implements all parts of NFR2.

Password Subsystem

The Password subsystem implements two key features, a password manager and a password generator to improve user security and ease of use. The Password generator prompts the user for a password length and 4 radio buttons from which they can select the complexity/preferences for their password. The Password manager uses a SQL database to store the users passwords locally and allows a user to view passwords they currently have saved in their database, and to add new passwords to their database. The only functionality that was not met for the password subsystem in FR1/2 was FR2.1 which was for the password manager to always be encrypted when not running, the reason this functionality was

dropped was because of time constraints and not essential to functionality of the subsystem. The password subsystem successfully implements all parts of NFR1/5 and NFR4.b.

Encryption Tools

The Encryption Tools allow for the user to encrypt and decrypt their files with either symmetric or asymmetric encryption, sign and verify files with a private and public key respectively, satisfying FR3.4. Additionally, users can store potentially sensitive files in an encrypted folder, satisfying FR3.2. The ability to locally generate public and private key pairs is implemented subsequently satisfying FR3.1. Users can import and generate public and private keys in the keyring; these keys are stored as Base64-encoded files in an internal directory inaccessible by other programs. The user can encrypt or sign not only files on accessible storage, but also pictures and videos taken straight from the application. The functional requirements have mostly been met. However, requirement FR3.3 (optional permanent deletion of input files upon encryption) is impossible for a non-rooted phone due to Android's security measures and file system - these limitations discovered only on the attempt to implement this feature - and requirement FR3.5 (encrypting output from other applications) is infeasible due to difficulty of securely retrieving output. Signing/verification and asymmetric encryption/decryption of files is compliant with RFC 4880 as per NFR3.A and works with other tools such as GnuPG, but symmetrically-encrypted files can only be decrypted with Hyggelig at this time. NFR4c is satisfied due to the ability to export generated/imported keys and files from the private folder.

Miscellaneous

FR6.1, the ability to (possibly automatically) store backups of keys, private files, and the password database on a cloud-based service such as Google Drive has not been implemented due to lack of time and higher priorities.

Dev Logs

https://github.com/Chainmanner/COMP3004B-Nameless-Project/tree/master/dev_logs

YouTube Video

https://youtu.be/GlfG_-VzhsI