Executive Summary

EggBeater

Purpose

The consistent lack of file security has become a serious issue within the consumer market. With the recent worries of personal security, consumer's need a reliable way to keep their files and information secure from threats.

Our purpose was to create an open source encryption system that provides file security that surpasses other systems. Other file encryption systems required only a strong password to access the encrypted files, while our system uses the user's fingerprints to access the encrypted files. Eggbeater, a tool for generating encryption keys from fingerprints, will provide consumers with a free and reliable way of securing personal and private files.

Design & Methodology

Eggbeater's architecture is split between three main domains, the graphical user interface, the command line interface, and the embedded interface. This configuration follows the Model-View-Controller architecture style where the user GUI is view, the embedded interface is the model, and the command line interface is the controller attribute.

Our team followed the agile development method of developing software with alterations that best fit within the scheme of the project. These alterations originate from the embedded interface and therefore must be accommodated for the system to be complete and functional. The verification of the project follows test-driven development, thus the testing is composed mainly of Unit Testing and some Acceptance Testing.

Conclusion

Eggbeater, a system that encrypts files by using a user's fingerprints as the passkey, is a well thought out and planned system designed with the agile-development process. While the main features of Eggbeater were implemented, not all of the features desired made the deadline, thus there leaves much room to improve upon Eggbeater. Eggbeater is open source, extensible, and maintainable, thus allowing anyone to build upon further.