PROJECT PROPOSAL

BY Jayden Lupold, Logan Krause, Dary Demchuk, and Lian Welch

"Personal Safe" Password Manager

Table of Contents

Project Abstract

"Personal Safe" password manager will be developed as a lightweight application to securely store and manage passwords. It will allow users to create a master account, then add, retrieve, and organize all their login credentials, which will all be encrypted and decrypted locally on their own personal device. There are plenty of password managers like LastPass and 1Password, but unlike "Personal Safe", many of them rely on cloud storage which introduces risks if their servers are compromised. This project is different because all encryption happens on the client side, meaning data never leaves the user's device in a plain form. The intended users are everyday people who want better security or people who are just serious about their privacy. Ultimately, this project will provide a security tool for users wanting to protect their passwords.

Conceptual Design

The initial design concept for "Personal Safe" is a client-side password manager created with Python 3 using tkinter for GUI and JSON/AES encrypted local storage. It would run on multiple platforms including windows, macOS, and Linux. The initial design would ensure that any credentials would remain fully under the user's control and balances security with ease of use. Some of the features would include a master account, adding/deleting credentials, a password generator, a strength meter, secure local storage, the ability to copy to clipboard, and optional encrypted import/export for backups.

Use Case Diagram
Sequence Diagram
Class Diagram

Background

"Personal Safe" will enable users to generate, store, and manage passwords securely, with any encryption and decryption performed locally on their device. This approach ensures that any sensitive data never leaves the device in plain text, while reducing risks from breaches of centralized servers. The main features will include a master account login, password storage and retrieval, a password generator, a strength meter, and an optional encrypted export for any backups.

While proprietary products like LastPass and 1Password are useful, they heavily rely on cloud storage, which can make them targets. Other open-source options like Bitwarden and KeePass provide flexibility, but they come with harder setups and even partially rely on external infrastructure. This project won't reuse any of their source code but it will likely need to borrow some design inspiration. Its main difference between those other products is the focus on full client-side encryption and user-controlled storage, which combines usability with even more protection.

lastpass reference
1password reference

Proof of Concept

https://github.com/cis3296f25/final-project-04-personal-safe.git

Required Resources

This password manager will be developed using Python 3, which I'm familiar with. I'll also use the tkinter library to create a simple GUI for entering and viewing passwords, and the json and base64 libraries to store encrypted passwords locally. For encryption I'll implement a XOR-based method for this prototype, but I'll most likely be added stronger encryption later using the cryptography library if I need to. The project can be run on any computer without the need for special hardware, and any necessary Python libraries are either built-in or installed relatively easily.

New Implementation (Future)

-Add stronger encryption by switching from XOR to AES-256.

-Add a password analyzer that detects weaker or reused passwords and give a better password recommendation.

-Add a local extension to autofill credentials.

-Add master account authentication.

-Add auto-lock after inactivity for user account.

Ideas/Feedback

-Conduct functionality testing to ensure reliable encryption.

-Measure usability through user testing. (setup time, navigation, etc)