PassKeep: Encrypted USB Password Keeper

Nisha Chaudhari, Mart Francisco, Sean Seruya
Nigel John
Department of Electrical and Computer Engineering

Abstract

Currently there is a large security risk in terms of private information and cyber security. Online accounts and passwords, especially those that store a lot of personal information are being targeted by cybercriminals. To address this problem, the goal of the project was to create a USBdongle hosting a server that can only be accessed through a physical connection to the device. It will contain a file system with full encryption of stored data. It would also be able to generate random passwords for user registration.

Introduction

This project is designed to tackle the security risks involved with the storage of secure information online. Passkeep creates, encrypts, stores and modifies passwords for the user. All of this is done offline. The key idea to keep this offline is to avoid the ability of a hacker to be able to access the device through online connection. For a hacker to be able to break into the device, they would require physical access to the device since all information is stored in the physical hardware.

To achieve these design requirements, we built the program in Python, incorporating modern hashing and asymmetric key algorithms to protect user data and information. The python code runs back-end in parallel with the front-end HTML code that creates an easy-to-use GUI for the user. The HTML code is reached by the user through a hosted server on the raspberry pi testing device (the pi must be hard connected to a computer to be reached by a user).

Methods | Design | Analysis

Place explanation of methods, design, and/or analysis here. Be clear and concise without relying on too much jargon.

- PassKeep password is hashed and stored within the device (sha256)
- Account passwords generated and encrypted with Advanced Encryption Standard (AES)
- Passwords stored by username under category of domain name
- Decryption method uses PassKeep password to decrypt increasing security

Results

User Interface

Conclusion

Place concluding remarks here. Try to answer the question: How does your project fit into the grand scheme of things?

- Portable device allows for easy use
- Can access the device on any computer
- Login information is kept safe
  - Offline
  - Encrypted
  - Unique encryption based on user’s master password

Acknowledgments

Thank you to Dr. Nigel John for his guidance and assistance with helping us throughout this project. Without his expertise and knowledge, we would have never been able to complete this project the way we wanted to. He taught us so much this past year throughout this whole process, and we are very happy with the results of this project because of it.

Again, thank you very much Dr. John for everything.

References