Senior Design Project
May - 2020

PassKeep: Encrypted USB Password Keeper

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

SENIOR DESIGN EXPO

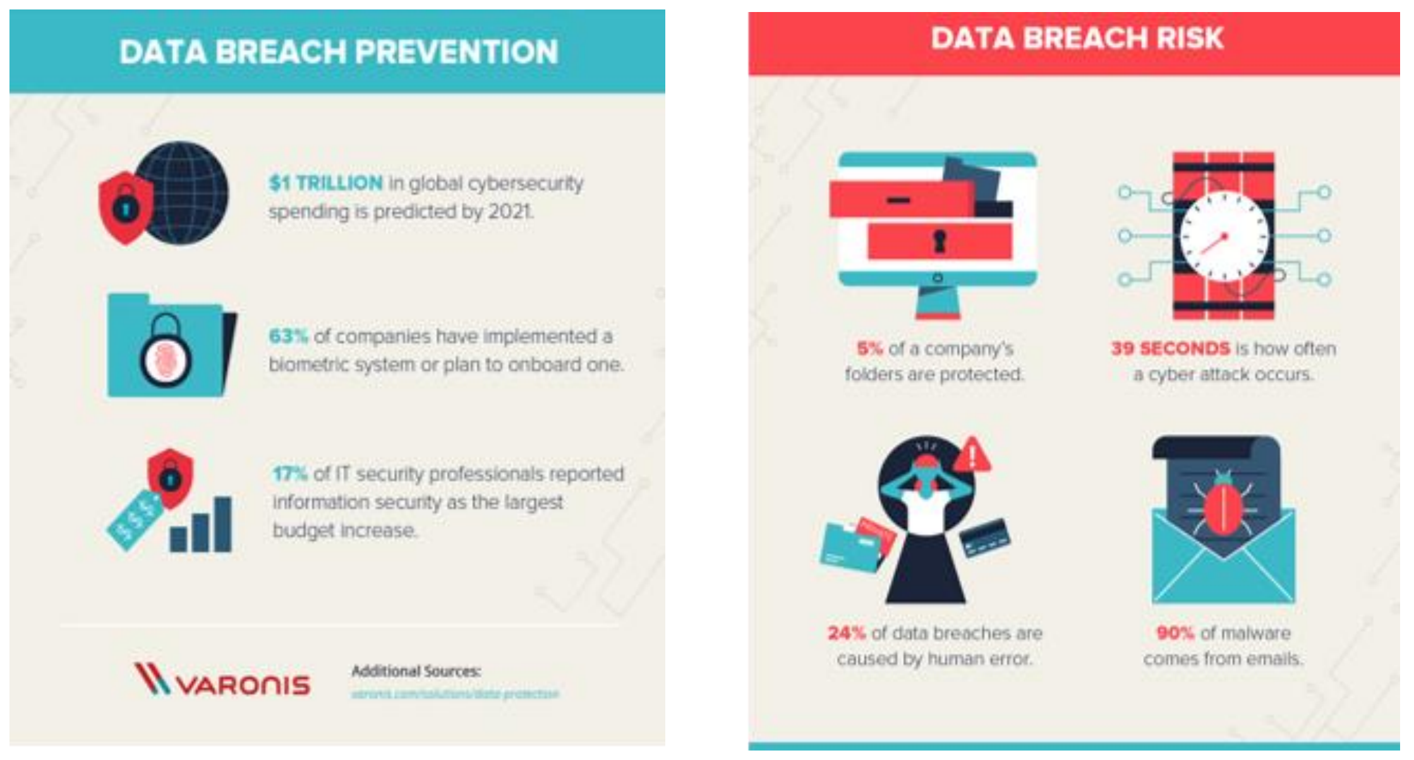
Abstract

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 USB dongle 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 being 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).

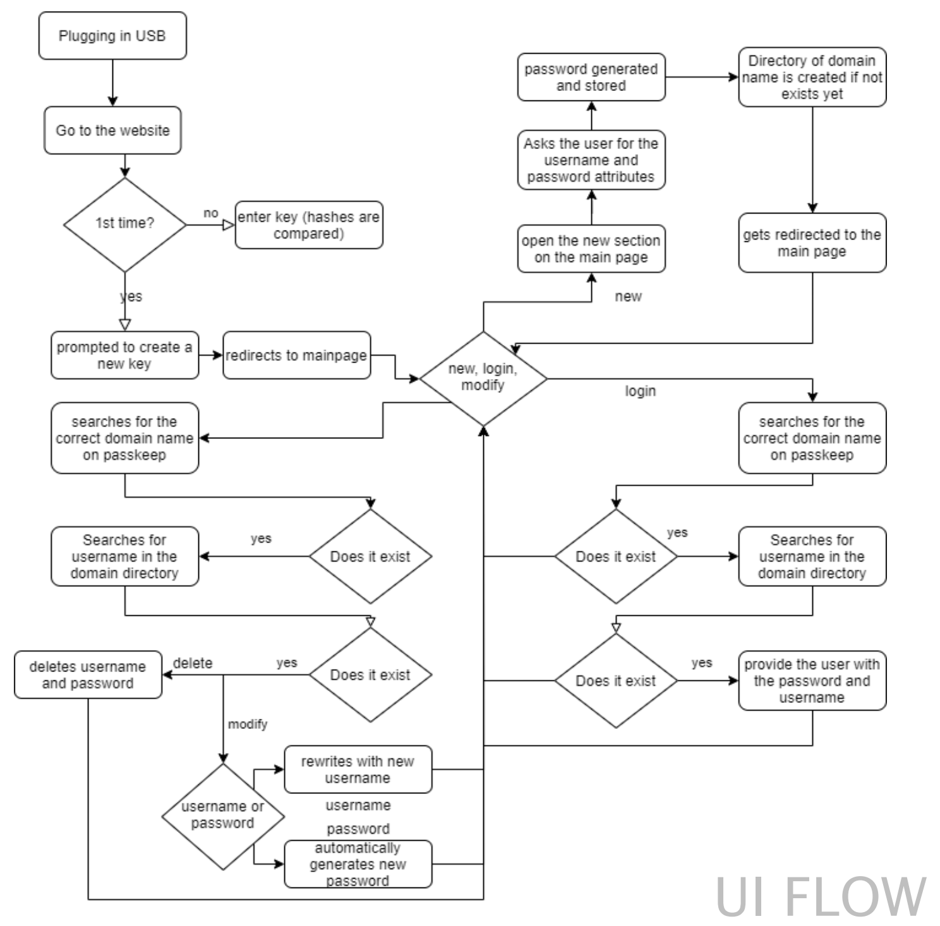

DATA BREACH PREVENTION
$1 TRILLION in global cybersecurity spending is predicted by 2021.
63% of companies have implemented a biometric system or plan to onboard one.
17% of IT security professionals reported information security as the largest budget increase.
VARONIS
Additional Sources:
varonis.com/solutions/data-protection
DATA BREACH RISK
5% of a company's folders are protected.
39 SECONDS is how often a cyber attack occurs.
24% of data breaches are caused by human error.
90% of malware comes from emails.

Data Breach Research[1]

Methods | Design | Analysis

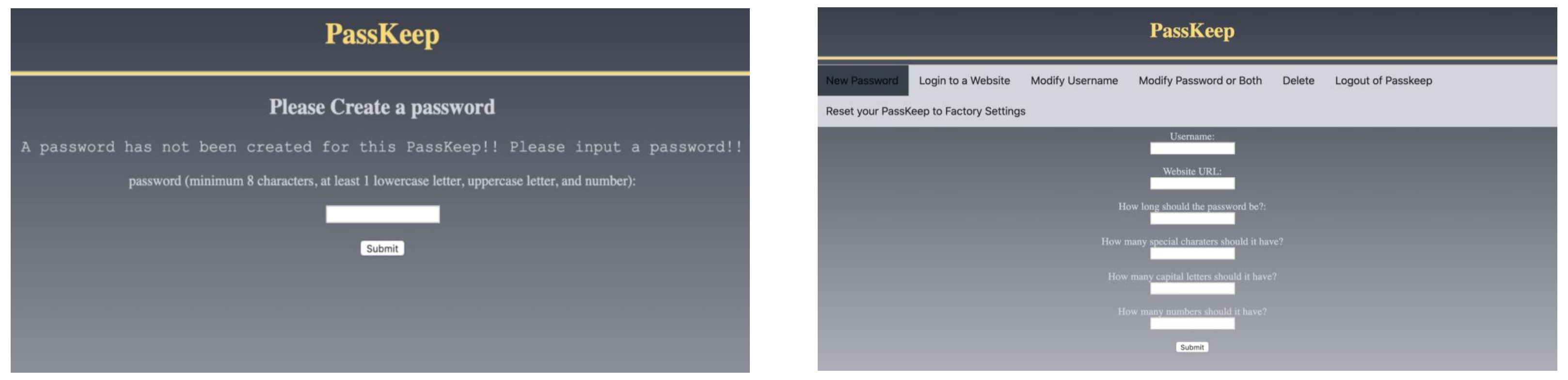
Place explanation of methods, design, and/or analysis here. Be clear and concise without relying on too much jargon.

- PassKeep password is hashed and store 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


Plugging in USB
Go to the website
1st time?
no
enter key (hashes are compared)
yes
prompted to create a new key
redirects to mainpage
new, login, modify
new
open the new section on the main page
Asks the user for the username and password attributes
password generated and stored
Directory of domain name is created if not exists yet
gets redirected to the main page
login
searches for the correct domain name on passkeep
Does it exist
yes
Searches for username in the domain directory
Does it exist
yes
provide the user with the password and username
searches for the correct domain name on passkeep
Does it exist
yes
Searches for username in the domain directory
Does it exist
yes
delete
deletes username and password
modify
username or password
username
rewrites with new username
password
automatically generates new password

UI FLOW

Results


PassKeep

Please Create a password

A password has not been created for this PassKeep!! Please input a password!!

password (minimum 8 characters, at least 1 lowercase letter, uppercase letter, and number):

Submit

PassKeep

New Password | Login to a Website | Modify Username | Modify Password or Both | Delete | Logout of Passkeep
Reset your PassKeep to Factory Settings

Username:

Website URL:

How long should the password be?:

How many special charaters should it have?

How many capital letters should it have?

How many numbers should it have?

Submit

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

[1] Sobers, R. (2020, April 15). 110 Must-Know Cybersecurity Statistics for 2020: Varonis. Retrieved from https://www.varonis.com/blog/cybersecurity-statistics/

UNIVERSITY OF MIAMI
COLLEGE OF ENGINEERING

Transforming Lives Through Teaching, Research, & Service