Describe your project

A Hardware based password manager used to store all passwords efficiently and securely. A portable device which can be plugged in to automatically enter your user name and passwords for the selected website thus making keylogging and screen capture attacks used by hackers ineffective. It uses a two factor authentication with the help of a fingerprint sensor and a TOTP(time based otp) which changes every given period of time . The passwords are encrypted using encryption techniques such as sha 256 and aes 256 and stored in the ROM of the hardware device itself.

Project Name

Hardware Based Password Manager

Tagline

"Your Passwords, Your Control, Our Hardware"

"Putting Passwords on Lockdown, Key by Key"

The problem it solves

Drawbacks of using Software Password Manager ● The main objective is to avoid any communication with the internet, which is a huge bottleneck for security in software-based password managers such as Google password manager, LastPass, KeePass. Most of the widely available password managers, merely encrypt the password and store them on the cloud, making them vulnerable to database breaches. ● Another major issue for password leaks is phishing, in which users are tricked into revealing sensitive information, which may include passwords. Also, most of them repeat passwords for multiple accounts as it is a hassle to remember many strong passwords. ● We plan on eliminating the issue of cloud database breaches by storing the encrypted passwords locally, on chip. There may be cases where the user would like to have backups of their passwords, in case they lose the device. Hence a facility will be provided to backup the passwords on to an auxiliary flash storage, which the user can store in a secure place. Since there is no way to decrypt the passwords without the master passwords, there is no worry even if the contents of the flash are read by an unwanted person

The Hardware Password Manager is based on the concept of zero knowledge proof, to store encrypted passwords in a secure manner. ● Users can store their passwords on the device, which is unlocked with the help of a master password. The approach behind this project will be to encrypt users’ passwords in a secure manner using AES-256. ● The crucial building block of this project is that the key for decrypting user passwords is not stored on the device. The key for these user passwords is a SHA-256 hash of the master password. ● This hash is used as the key for the AES algorithm to encrypt user passwords and only the encrypted password is stored on the device flash. ● When the user wants to retrieve any password, the master password must be entered, which is use to compute the hash which is then validated, to check if the entered password is correct. ● Once the validation is completed, the user can select the required account for which the password is required.

Challenges we ran into

Localising timestamp-Python was giving gmt and rtc was giving in ist format, which took considerable time to localise into one format

Finding libraries for integrating rotary encoder and Raspberry PI pico.

Technologies we used

Hardware

• Raspberry PI pico to carry out encryption and decryption operations

• Rotary Encoder for taking in user input

• DS1307 RTC to store encrypted data and maintain time

• OLED Display

• Buzzer

Software

• Arduino IDE

• SHA-256 to hash master password

• AES-256 to encrypt user accounts and password

• Flask-Python to provide user interface for taking backups

Links

<https://github.com/bharath-reddy07/revahack>

BRIEF DESCRIPTION ON HOW YOUR PROJECT FITS INTO BEST USE OF GITHUB TRACK

Creating issues and pull requests helped us to simultaneously work on different parts of the hardware and helped us to seamlessly merge and integrate all the different parts to obtain the final fully functioning model.

BRIEF DESCRIPTION ON HOW YOUR PROJECT FITS INTO BEST DOMAIN NAME FROM GODADDY REGISTRY TRACK

"SecureKeyVault.com is the perfect domain name for a hardware password manager product or service. Just as a vault provides maximum security for valuable assets, this domain conveys the message that your hardware password manager is a secure and impenetrable solution. It instills trust in users that their passwords and digital identities are safeguarded within this virtual vault, protecting them from cyber threats."

BRIEF DESCRIPTION ON HOW YOUR PROJECT FITS INTO BEST USE OF MATLAB TRACK

We used matlab to simulate the functioning of the totp.

BRIEF DESCRIPTION ON HOW YOUR PROJECT FITS INTO BEST USE OF HEDERA TRACK

Our Hardware base password manager embodies the Best Use of Hedera by harnessing the power of Hedera Hashgraph's robust distributed ledger technology. Through secure and efficient consensus mechanisms, we achieve unmatched scalability, speed, and trust in our solution. By utilizing Hedera's native token (HBAR) and smart contracts, our project ensures transparent and tamper-proof record-keeping and facilitates seamless, high-speed logins .