International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 06 Issue: 02 | Feb 2019 www.irjet.net p-ISSN: 2395-0072

Enhancement of Security using 2-factor Authentication, 2nd Factor being Fingerprint

U Kishore Malllya[1], Sandeep B[1], Derek Ashley[1], Sanath Kumar S[1] and Saravana M K[2]

[1]Dept. of Computer Science and Engineering, Jyothy Institute of Technology, Bangalore, India
[2]Asst Professor, Dept. of Computer Science and Engineering, Jyothy Institute of Technology, Bangalore, India

---

Abstract - *At home and work, we have more online accounts that we can possibly remember. And since 81% of breaches are caused by weak or reused passwords, it's essential that each account have a unique password. So how are we supposed to remember these strong, unique passwords? We use a protected password manager where the user have to just remember one strong and unique password. As passwords alone cannot do justice to the protection, we include the physical authentication (Biometric) to verify that the actual user is logging in.*

***Key Words*: Online Account, Breaches, Unique Password, Password Manager, Biometric Authentication.**

1. INTRODUCTION

The ever evolving digital age has made the need for cyber security more important as the rate of cybercrimes has been increasing day by day with the growth of technology. One of the important topics in this is Identity theft where a users credentials are used by someone else exploiting the users privacy. Passwords are being used in all industries such as banks, IT companies, Schools and colleges and many more. One of the main reasons of Identity theft is setting of weak passwords which makes it very much more easier for others to hack into accounts and access private information of the user such as card PIN, Cash transactions etc. Password is an hidden entity which should remain a secret. It prevents identity theft when incidents arise such as theft of username, UPI pin etc. Technology has made such a progress that passwords can be broken using hacking tools like Hashcat, Ncrack, THC Hydra etc. and phishing which is used to extract passwords from a duplicate website which imitates the original one. The basic form of in which passwords can be compromised is by brute force attack where access to users account can be gained using trial and error method. There are many automated software for these brute force attacks such as Brutus, John the Ripper, Medusa and many more.

A password manager is a software solution to help passwords remain a hidden entity which means kept as secret. It is a place where a user stores and manages the passwords of various accounts without the fear of getting hacked or forgetting passwords. Since there are many tools to extract passwords, security to this application is provided by 2-Factor authentication. There are many advantages of password manager some of them is restricting users to set weak passwords to various accounts, preventing phishing by logging into the trusted original website and keylogging by auto filling user credentials, visual spoofing is possible but is not completely enough as 2 factor authentication is implemented

2. LITERATURE SURVEY

Many Research papers have been published on implementation of password managers.

The summary of the research papers taken for the survey are as follows:

Analysis on the Security and Use of Password Managers by authors Carlos Luevanos, John Elizarraras, Khai Hirschi, Jyh-haw Yeh. [1]

In this Password Manager they are going to create 3 password managers for security purposes. All are different from each other by having their own uniqueness. Those were named as Passbolt, Padlock and Encryptr. All these 3 are open source and can be used as web extensions. Passbolt is for secure email communication. Padlock for copying and pasting of passwords. One major advantage of Padlock is, it'll automatically logout user from their account/profile when there is no user activity is detected for a minute. Encryptr is used to store some data in server only. Server itself will not find that, what it has been stored with. It is a cross platform password manager and used in e-wallet applications. Passbolt is designed for Firefox and Google Chrome. It is written in PHP, Javascript and Shell. It uses OpenPGP for their encryption purposes. The main disadvantage of this extension is, as it is open source someone could duplicate it and steal data from users who thinks that it is the real pass bolt. And another one is, it can't be modified. Encryptr is written in HTML, CSS, JSON and XML. As the name itself indicates that it includes encryption and decryption. It uses ECDSA (Elliptic Curve Digital Signature Algorithm) for digital signature verification. It is mainly depended on end to end encryption. So, that the user can feel more secure from attackers. One small disadvantage in this is, user's name is stored in plain-text format and it can be analyzed by database records. And this problem can be overcomed by setting strong password. User has to type his own password instead leaving it to generate one. Like Passbolt and Encryptr, it is also written in Javascript, CSS and HTML. Padlock has more disadvantages compared to Passbolt and Encryptr. It is responsible for tap-jacking, permanent DOS

attacks on mobile devices and also DOS email attacks. As all these 3 are open source applications, attacker can keep traps for users as vulnerability for performing future attacks. In closed source application, everything we store is hidden and attacker will not attack or keep traps easily as in case of open source.

Cloud Password Manager Using Privacy-Preserved Biometrics by authors Bian Yang, Huiguang Chu, Guoqiang Li, Slobodan Petrovic, Christoph Busch. [2]

This paper presents about the password manager using using password based security and biometric based security using fingerprint sensor. In this paper they have proposed cloud based scheme. The proposed password manager scheme relies on a cloud service that synchronize all local password manager clients in an encrypted form, which is efficient to deploy the updates and secure against un-trusted cloud service providers. There are several methods explained in this paper about the implementation method. By storing the plain text message. By using the encrypt password using cipher. Biometric authentication.There are two techniques discussed in this paper namely, Single Sign on and Biometric template Protection

Single Sign On is a software system that gives users to access to all the systems without needing a login each time after loging into it once. Using SSO it reduces the inconvinence of having user name and password for specific website.

Biometric Template Protection (BTP) is such a technology to transform the biometric data into a protected template and store it in the database. The merits in this technique are, Biometric is added as second factor and it is designed in such a way that even if either one of it is compromised, the other one is there to keep it secured.

The steps that is been described in this paper are step 1 by creating a random number which is used to hife the master key and step 2 by using Biometric template protection and step 3, after the password binding process is done, both the random number and the generated protected template PT are discarded.

A Web Password Manager with Roaming Capability Based on USB Key by authors Xing Wang, Zhen Han, Dawei Zhang. [3]

This Password Manager consists of two entities:

1)USB-KEY - Physical device that stores passwords

2) IDKeeper - Extension for authentication, autologin, export and import passwords

This is a password manager which stores passwords corresponding to user-accounts in a USB-KEY which is a physical device. USB-KEY consists of a security chip and a flash disk. The core software will run on the security chip. The flash disk will store programs (a Firefox Extension) running in PC OS so that users need not to install any additional software. Passwords cannot be directly extracted from USB-KEY just by plugging in to a computer. Rather it requires a PIN to authenticate and send the authentication to IDKeeper which is a browesr extension. Once the user/USB-KEY is authenticated the browser checks for the webite URL of which credentials are to be obtained to prevent phishing attacks, later it scans the websites for text fields and autofills these fields and prevents keylogging and screenlogging or eavesdropping. When the user register a new account at a website, the user enters ID and Password on the website and click “Register”, then IDKeeper browser extension will ask the user whether to save the credential information into the USB Key. If it was allowed IDKeeper will parse the web page and store the information of the web site contains the Site Name, the URL of the site and the corresponding User ID and Password to the USB Key via the Trusted Path. Hence providing protection to passwords.

Amnesia: A Bilateral Generative Password Manager by authors Luren Wang, Yue Li, Kun Sun. [4]

In this Amnesia bilateral generative password manager is developed that enhances the security by generating the requested password knowing the master password and having a smartphone. How it basically works is if the user wants to obtain a password of a specific website, the user first enters a master password to log into amnesia web server. After user selects the account that has to get logged in, a password request is sent from amnesia web server to the users smartphone, after the confirmation from the user, the smartphone sends a token to the server and combines these to generate the password and this is sent to the user’s computer. Using this user can login anytime without being worried to install any software on the computer and as a generative password manager it is not vulnerable to database breaches. In case of lost smartphone the user can login using master password and backup the data to another smartphone. This prototype was built using android to develop amnesia mobile application and CherryPy web framework to build the amnesia web server

3. PROPOSED SYTEM

We implement a password manager which stores all the passwords of the user, the user must remember a master password for logging in. As passwords alone is insufficient and can be hacked a 2 factor authentication is implemented where the user needs to verify using fingerprint to grant access to the users password vault.

4. DESIGN

This system consists of a web application and an android application.

Web application is used for storing passwords, auto-login into users' account.

Android application is used for authentication purpose to login/gain access into the web application.

The web application is the actual place where passwords are stored. Here, users might store weak passwords which makes their accounts vulnerable. So, here the users are enforced to set strong passwords which should match our predefined conditions. It might be difficult for them to think of a new password for every new account. So, a feature is provided which sets a random password that satisfies our conditions. URL of the corresponding account must be provided by the user in order to prevent him from phishing attack. Auto-fill passwords feature prevents the users from keylogging attacks.

The android application is solely for the purpose of authentication.

And the authentication flow goes like this:

- Go to the website and, click “sign in”
- Enter my username/email-id, and password and press the "log in" button
- A notification on the Mobile phone pops up asking to confirm the login
- Tap “approve”, and swipe the thumbprint
- The website sees that user has confirmed the login request and starts the session

Step by step process of authentication

5. CONCLUSIONS

We help users by the following ways:-

- To help users set secure passwords.
- To help users keep their passwords in one place securely. The user has to remember only one password to access their entire password vault.
- To prevent phishing attacks on user credentials
- To prevent KeyLogging on users passwords.
- To Give the user a two factor verification by using a biometric (Fingerprint)

ACKNOWLEDGEMENT

The authors express their sincere gratitude to the Principal of Jyothy Institute of Technology, K Gopalkrishna, Head of computer science Dr. Prabhanjan S and our project guide Mr. Saravana M K for giving constant encouragement and support to complete the work.

REFERENCES

1) Analysis On The Security And Use Of Password Managers [Carlos Luevanos , John Elizarraras, Khai Hirschi, Jyh-haw Yeh], IEEE-2017

2) Cloud Password Manager Using Privacy-Preserved Biometrics [Bian Yang, Huiguang Chu, Guoqiang Li, Slobodan Petrovic, Christoph Busch], IEEE -2014

3) A Web Password Manager with Roaming Capability Based on USB Key [Xing Wang, Zhen Han, Dawei Zhang], IEEE-2012

4) Amnesia : A Bilateral Generative Password Manager [Luren Wang, Yue Li, Kun Sun], IEEE-2016