

Password-Free Login

Darshan Ingle

Asst Professor, Comp Engg
Dept,
SIESGST, Nerul, Navi Mumbai.

Varsha Patil

Asst Professor, Comp Engg
Dept,
SIESGST, Nerul, Navi Mumbai.

Sanjay Talbar, PhD

Professor, EXTC Engg Dept,
SGGS Institute of Engg and
Tech, Nanded

ABSTRACT

Password-free login is a system that sets the user free from remembering the passwords used, so that the user can get an easy access to any website of his choice in a common password. The system is basically a password storage website that keeps all the login id's and password in a single database. The advantage of the system is that even if in mere future the user happens to forget the login of a website that has been accessed a long time back, it can be easily retrieved by the user using the common login id details for the website. Thus, this website will set the user free from remembering the login details of any website. The details of the work done can be seen in detail in the further part of the paper. So, this website will set the user free by making him remember just a single login id and password which in turn will retrieve the required login id and its password. This system is really going to be a boon for the all kinds of users. The paper also discusses the security aspects of the website so that the system can be proved to be a robust and concrete one. The uniqueness of the system can be seen in the further detailed discussion.

General Terms

One-time password, PFL, KeePass

Keywords

Two Fish, SHA256, master password.

1. INTRODUCTION

In today's world, there are lakhs of websites available on the internet. Each website provides some functionality for the ease of the user. These functionalities are unique and sometimes crucial for the user. Right from the basic emails like Gmail, Yahoo mail, etc to some vital transactional websites like banking, shopping, etc, each stores some or other data that is of importance to the particular user. Some websites directly provide the information to the user, while some specifically require to create a account at that website to get the required details out of that website. So, as a user, it is essential to create a account at that website with email id as the login and the password of the user's choice for that website.

This process of creating account at the website is a common process for a user whenever a website is to be accessed. A user can require any type of information from such websites. So, it is mandatory in almost all the cases for the user to create an account at the websites. There are going to many such websites where an account would be created by the user. It is not advisable to keep the password of all these websites same throughout as a leak of a single password can almost break all the user details. Hence, it is mandatory for security reasons to have different passwords for all such different websites. The user always has a challenge to remember so many login details and passwords. Many a times, user forgets the login details of the websites that has been accessed a long time

back. So, proposed system in the paper is going to be a full proof secured system that will be capable of storing all the login ids and passwords of the websites that a user has accessed so far so that he can be set free from remembering all the passwords.

2. LITERATURE REVIEW [1]

The research study seen so far shows that with the proliferation of the web services, a user always creates new accounts, each with a different username and password, remembering which, is almost impossible. The various attempts made by a user to remember the login details of a various website are as follows:

2.1 Spreadsheet Approach

One way to keep a track of passwords is to write it down every time on a piece of paper or in a spreadsheet. However, looking at this case from security perspective, it is highly vulnerable to theft. Any malpractice can lead to multiple copies of the same and render user sensitive data to be exposed. So, this approach is not a convenient one.

2.2 Mailbox Approach

A copy of all the account details can be maintained in an individual's mailbox like Gmail, Yahoo mail, etc so that the required data can be fetched whenever required. However, a mailbox is not a secured place for the sensitive data like passwords to be saved. Also if an attempt to save such data on mailbox is made, each time the user has to search for the required account details on the mailbox. This turns out to be time consuming. Even, a mailbox cannot keep a track of visited websites by the user. So this approach also turns out to be less efficient one.

2.3 Browsers like Firefox, IE, etc [3]

Some popular browsers like Firefox, IE, and Chrome offer fairly secure ways of storing username and password for different sites when the website is visited for the first time. This approach being handy saves a lot of time of the user.

But, in some cases, the password saved by the browser can be lost. So now the user is required to enter the password again. So, in such a case if the user is relying on the browser to remember the password, it is going to be a loss to him. If the browser is uninstalled or if the OS gets corrupt and needs to be formatted, then all the data saved by the browser will be lost. Also, this solution only works for online passwords, not for network or desktop passwords. So this is also not a feasible option for storing the user account's data.

2.4 KeePass[4]

KeePass is one of the most popular password manager available in the market. It is an open-source password manager which works on platforms like Windows, Linux and even on mobile devices. It keeps all passwords in a secure database that is encrypted using the Two Fish algorithm. So the user has to remember a single master password. Alternatively, the encryption of the database can also be done with the help of a key file which can be stored by the user on a USB stick, floppy disk or can be burned onto a CD. This makes it important for the user to preserve this disk safely. A combination of the above i.e using a master password and a key file both can be used to encrypt the database to get a stronger encryption using this technique.

However, this system still cannot be called as a full proof secured system as there can be a possible leak of password or mishandling of the key file which will render the system to be attacked.

2.5 Clipperz

Clipperz is another such password manager which is available online. This works on a similar basis as compared with KeePass . However, Clipperz uses an encryption method in such a way that not even the admin of Clipperz is aware of the encryption technique used for storing the data and thus provides a powerful security.

But, again from the security point of view, Clipperz has just one level protection by using a single master password.

3. PROPOSED WORK

It can be seen from the rigorous study of the literature review that the online storing of the passwords is still not reliable option for the end user. There is always a chance of threat for the use of a single master password. So, the paper proposes a new technique that uses two strong encryption algorithms namely SHA256 and Two Fish algorithm[2] to store the password data.

It is been observed that the data is always classified for the user whenever the user access the internet. Some confidential data like credit card numbers, account numbers, etc is of crucial importance to the user. There lies one more level below, which stores the less critical information like the users mailbox passwords, drop box password, free messaging websites passwords, etc. Apart from this, there are some websites which have a constraint of compulsory registration before accessing the contents of the website. Some of such websites are freshersworld.com, sarkariaukri.com, and many of the corporate company websites.

It is difficult for the user to remember all such passwords. Frequently used passwords can be remembered by the user easily. However, there are some websites where the user has to forcefully create the account when some information has to be extracted from that website. Such websites are of temporary importance to the user. Once the information is obtained, that website is never accessed again. So it is very obvious that the user forgets the registration details of this website. However, it is very much possible that the user happens to login into the same website after a long span of time and realizes that he is already registered on the website but the password details are not recollectable for the user.

The paper proposes a solution to solve the above problem by broadly classifying the data into three categories as Very critical, Less critical and Tolerant. Very critical stores data like net banking passwords, credit card passwords, debit card passwords, cash locker password, etc. Less critical stores data like mailbox passwords, drop box password, free messaging website passwords. Etc. Tolerant stores data like registration details of rarely used websites.

It also adds to more security by using one time password generation. That is, when the user enters the master password for accessing his account of online stores passwords, the system will generate a one-time password that will be sent to the users mobile phone. Only when the user enters this password correctly, access is granted to him. Thus, apart from the strong encryption algorithms used, the paper provides the best possible security by generation one-time password.

The system will demand the user to create an account for the first time and provide some of the mandatory details like name, phone number, etc. Thereafter, the user has to simply save the passwords. However, this process requires for the user to provide the details like the URL of the website, the login id and the password of the website of which the information is to be stored. Once the details are saved, the user can simply access the registration details of the required website by simply provide the URL of that website to the system. The URL provided by the user would be compared to the database of the system and the required registration details like login id and password will be fetched.

As far as the security is concerned, Two fish and SHA256[2] algorithms will be used for a powerful encryption. The system provides a security in such a way that even the admin of this website doesn't know the stored details of the user.

4. ALGORITHM

1. Enter the system by using the following URL "www.passwordfreelogin.com". This is a proposed name.
2. Register on the website by creating an account.
3. Save the registration details by copying the URL of the website, its login id and password.
4. The URL, login id and password are saved in the database by encrypting it using SHA256 or Two fish algorithm [2].
5. Classify the above URL as Very critical, Less critical or Tolerant.
6. Repeat the above procedure for storing all the required details.
7. Logout of the website after the details are saved or the account will be by default logged out after the timer expires.
8. When some information is required from the website, login into the system using the master password.
9. This generates a one-time temporary password token which is sent to the users mobile phone number which he has provided to the website while registration.
10. Enter the one-time password as it is into the system.
11. If the master password and one-time password match, the user is granted access to his account, else the session expires.
12. If login was unsuccessful, then a warning message is sent to the user's mobile phone and mailbox as "Some unknown user has tried to access your account".
13. If login details are correct, the user has a successful login.

14. All the saved URL's are now visible to the user.
15. The required URL can be selected or a search option is also present to easily search the required URL from a long list of the saved URL's.
16. The user selects the required URL of which he wishes to extract registration details.
17. Now, the URL is used for decryption of the login id and password [2].
18. The decrypted details are now provided to the user.
19. Repeat steps 8 to 18 for further retrieval of other information.
20. Logout of the website when no more information is required.

5. SCOPE OF THE PROJECT

The above proposed work can be great importance to the end user. Also, it is an open source. The proposed websites has a strong advantage that it uses encryption method such that doesn't know what it is storing. So, even the admin of the website cannot track the user details.

Also the encryption algorithms are tried and tested ones. They are proven algorithms to provide a high level of security. So, the user details are always safe and protected.

A registration form consisting of several input fields and buttons. The fields include: First Name, Last Name, Phone Number, Email, Password, Confirm Password, Gender (Male), Date Of Birth (mm/dd/yyyy), and two buttons at the bottom: Register and Cancel.

Fig 5.1 Registration Page

Fig 5.1 shows the 'Registration page for Password-free login system. When a new user want to use the system facility, the registration should be done, This takes as input some basic fundamentals as input from the user. It includes some of the details like First name, Last name, contact details, email id, password, etc. Once the details are filled in by the user, registration process is complete. This registration form successfully creates an account for the user.

A form with four buttons: Add Data, Edit Data, Retrieve Data, and Cancel.

Fig 5.2 Select operation

Fig 5.2 shows the various operations that the user can perform using his account. When an account is created for the user, a new data can be added by the user. This new data is the new registration login id and the password of the website which is intended to be saved. Also an edit operation can be performed on the existing data whenever the password is changed. This operation can be performed with the help of Edit button provided to the user. When the user requires any registration details which is stored in his profile, it can done using the Retrieve data button.

A form with four fields: Enter Url, Enter Login Id, Enter Password, and two buttons: Encrypt and Store and Cancel.

Fig 5.3 Store registration details

Fig 5.3 shows the registration details storing phase for the user. This page will be opened when the user selects the Add data button from Fig 2. Here, the user can store any registration details along with the websites url. The advantage of storing the url along with the password is for the efficient retrieval of the login details and password thereby reducing the search time considerably.

A form with three fields: Enter Url (containing 'Url 1'), a dropdown menu, and two buttons: Retrieve Data and Cancel.

Fig 5.4 Select url page

Fig 5.4 is an extension of fig 3. When an user selects "Edit data" item in Fig 3, the following page is prompted. Here, the user has to select the url of the specified website of which he wishes to edit the data.

A form with two fields: Username (abc@xyz.com) and Password (xyz@12345), and two buttons: Edit and Back.

Fig 5.5 Edit option page

When the user selects the required url, the page is prompted as shown in Fig 5.5. Whenever a user wants to edit some data, he has to enter the master password again as a security measure as shown in Fig 5.6.

A form with one field: Enter Master Password, and two buttons: Confirm and Cancel.

Fig 5.6 Enter master password

When the user enters a master password, there is another level of security measure. This is one time password generation phase as shown in Fig 5.7. This one time generated password is sent to the users authenticated mobile number. Here in the label field, the user must enter the one time password received on the mobile phone. This phase makes it sure that the user who wants to edit the data is an authenticated user. After entering the password, 'Accept' button should be clicked.

One time Password sent to xxxxxx4477

Enter OTP

Accept Cancel

Fig 5.7 Enter one time password

Fig 5.8 shows the username and password field in an editable form. Now the user can either change the required user name or password.

Username

Password

Save Cancel

Fig 5.8 Display username and password

Enter URL

OR

Enter LoginID

Confirm Cancel

Fig 5.9 Enter url or login id

Fig 5.9 is the page opened when the user selects the button "Retrieve data" from Fig 5.2. This is used when the user wants to retrieve some data about the registration details. For a user to retrieve data, as an input, user can give the url of the website or the username of the website and press "Confirm" button.

Enter Master Password

Confirm Cancel

Fig 5.10 Enter master password

Fig 5.10 asks the user to enter the master password for his login.

Enter OTP

Accept Cancel

Fig 5.11 Enter one time password

Fig 5.11 asks the user to enter the one time password generated and sent to his mobile phone and press "Accept" button.

Following are the required details

Username:	abc@xyz.com
Password:	xyz@12345
Ok	

Fig 5.12 Retrieved details

Fig 5.12 shows the user, retrieved username and password in a non-editable format. This will fulfill the users purpose.

6. CONCLUSION

The password storing for the various websites can now be done easily by maintaining a single master password which needs to be changed at frequent intervals. This website also has an advantage that if the user forgets to change his password at regular intervals, it asks the user to 'Force Change' the password. So the master password now remains more secure, thereby making the website reliable. The website also has a unique behavior of one-time password token generation which is not available in any of the existing systems. This provides the security of highest level.

7. FURTHER WORK OF THE PROJECT

Some further work which can be done in this project can be as follows. Now a days, many websites have a 'Login with Facebook' facility provided for registration. However, this facility is available only for less critical and tolerant websites. Banking systems don't have this facility. The aim of the future work is to provide the user with direct login facility. That is, whenever the user goes to a previously registered website, it will show an option below to the user as 'Login with PFL' meaning 'Login with passwordfreelogin.com'. The user now has to simply select that option and the user will be diverted from the current website to the website 'passwordfreelogin.com' where he will be asked to enter the login id and master password which will send a one time password to the users mobile phone. Entering the correct master password and one-time password will provide access to the website. Now, 'passwordfreelogin.com' will map the details of the websites the user required directly with the database and 'passwordfreelogin' will automatically substitute the login id and password of the users requested website thereby relieving the user from explicitly going to the website 'passwordfreelogin.com' for accessing the details.

Thu, it saves a lot of time of the user and makes the system more efficient.

8. REFERENCES

- [1] 10 Free Ways to Track All Your Passwords - Lifehack.org, Available: <http://www.lifehack.org/articles/technology/10-free-ways-to-track-all-your-passwords.html>
- [2] Shay Gueron, Simon Johnson , Jesse Walker, *Department of Mathematics, University of Haifa, Israel*, Mobility Group, Intel Corporation, Israel Development Center, Haifa, Israel, Intel Architecture Group, Intel Corporation, USA, Security Research Lab, Intel Labs, Intel Corporation, USA.
- [3] Manage your website passwords - Chrome Help - Google Help, Available: <https://support.google.com/chrome/answer/95606?hl=en>
- [4] KeePass Features, Available at: <http://keepass.info/features.html>
- [5] Xing Wang, Comput. & Inf. Technol., Beijing JiaoTong Univ., Beijing, China, Zhen Han, Dawei Zhang, "Keep Passwords Away from Memory: Password Caching and Verification Using TPM", *Industrial Control and Electronics Engineering (ICICEE), 2012 International Conference*, 23-25 Aug. 2012
- [6] Hua Wang ; Sch. of EECS, Peking Univ., Peking ; Yao Guo ; Xiangqun Chen, "DPAC: A Reuse-Oriented Password Authentication Framework for Improving Password Security", *High Assurance Systems Engineering Symposium, 11th IEEE Conference*, Dec 2008.