A Survey on Existing Password Storage Methods and their Security

Samruddhi Patil[1], Kumud Wasnik[2]

[1]M. Tech Computer Science & Technology Student, UMIT, SNDT University, Mumbai, India

[2]Professor, Computer Science & Technology Department, UMIT, SNDT University, Mumbai, India

Abstract: ***Each user need accounts to access service for website. Any account authentication or identification password is required , but most of the user choose easily remembered password which give low security protection. Some user keeps same password for all accounts. Proposed system pendrive is used to store more number of password with high security. In this paper, there are few methods to store password securely.***

Keywords: Password, Pendrive, Password Protection, Security

1. Introduction

Currently many users are likely tend to use password which is easily remember or single password for all website. These are insecure and can leak easily and also using different passwords to different website is difficult to remember. Because of this, there is high risk of security and confidentiality of user account.

Now-a-days more people are using internet for shopping, banking and paying bills, for all the activity user need to register for that service and open account to access web services. Many website are basically used text password protected security for users account, but for one user. It is more difficult to remember all password. Sometime it happens that user open account after long time or user need to open sometime only, so it is more difficult to remember password. Some user have tendency to use one password for all account or there are chances that user can use easy password which can be easily remember or use same password all over internet, this causes password guessing attack and chances of leakage of passwords.

We take passwords for granted, but they are often the only defence against someone getting their hands on our personal information, including financial information, health data, and private documents.

Generally user write down their password in diary or in text file using encryption technology. The main purpose of password is to protect users confidentiality and there personal information, but if password get leaks or hacked then hacker can misuse there account for their use.

It's easier than we think to crack or break passwords. Hackers crack passwords in a number of ways. Hence, there is high risk of security and confidentiality of user account.

This survey focuses on identification and authentication of user's account using pendrive stored password over existing password protected system or password manager. The rest of the paper is organized into 4 sections. Section 2 gives literature review of different password stored method used by different researchers for their research. Section 3 discusses the analysis of different password store method and security based on previous work that the researcher can choose for their research. Section 4 contain problem statement. Section 5 contains conclusion.

2. Literature Review

There are many password managers to store password that can be store in cache file, on cloud or in mobile device. Some techniques are implemented by different researcher shown in table 1. Some password storage method provide good security for password. But they have some disadvantages. Strong passwords are complex. The longer the password, the harder it is to crack and we shouldn't limit our self to just the alphabet. Instead of using only text or alphabet password if we add physical devices it will provide more security to users account.

S. Agholor et. al [1] suggest solution for memorability of password in authentication system using mobile based password manager. In this passward , it creates faux password using Transformed-Based Algorithm and the Modified Levenshtein Distance. It is also used Decentralized File Format architecture to distribute credential information into different files for storage. But as they used mobile based password manager, the space to store passwords is limited. Fig 1.

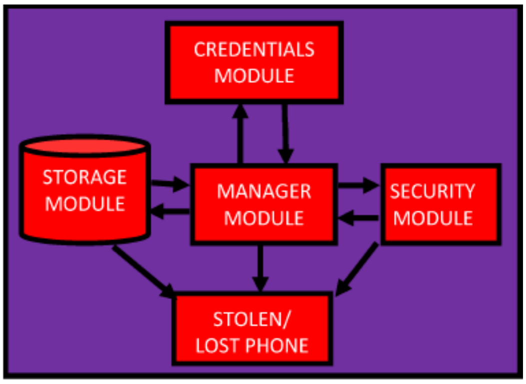


Figure 1: Architecture of DFF-PM

HaoFang et. al[2] suggested the Security Enhanced Secret Storage Scheme, when the client needs to access account or any secure data, it will starts a session with server and master-key related information will be stored locally. User needs to remember master key for authentication. If the authentication is successful, the server will send its partial data to the user.

Bian Yang et. al[3] proposed password manager is cloud based using biometric . It uses privacy enhanced biometric to achieve more security. They added 2nd factor security as biometric feature. In this, two factor of master key and biometric feature are combined. Fig 2.

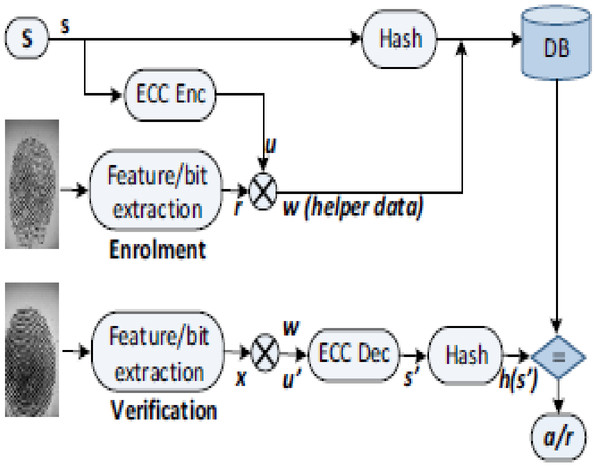
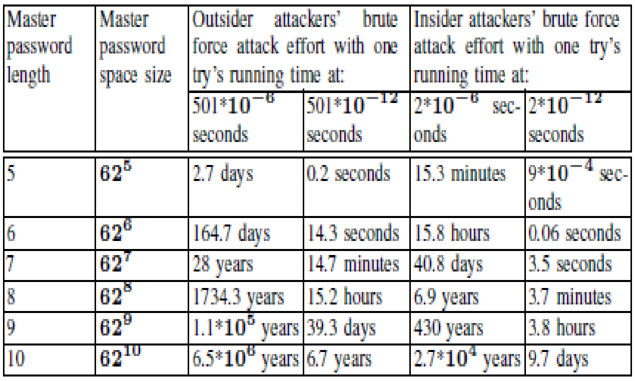


Figure 2: Fuzzy commitment scheme for biometric template protection

Rui Zhao et. al[3] gives the security analysis of two password manager currently used. LastPass and RoboForm both are browser are cloud based password manager. They both save password local drive in cache file or text file and also on cloud. Fig 3.



Master password length	Master password space size	Outsider attackers' brute force attack effort with one try's running time at:		Insider attackers' brute force attack effort with one try's running time at:	
		$501*10^{-6}$ seconds	$501*10^{-12}$ seconds	$2*10^{-6}$ sec-onds	$2*10^{-12}$ seconds
5	62^5	2.7 days	0.2 seconds	15.3 minutes	$9*10^{-4}$ sec-onds
6	62^6	164.7 days	14.3 seconds	15.8 hours	0.06 seconds
7	62^7	28 years	14.7 minutes	40.8 days	3.5 seconds
8	62^8	1734.3 years	15.2 hours	6.9 years	3.7 minutes
9	62^9	$1.1*10^5$ years	39.3 days	430 years	3.8 hours
10	62^{10}	$6.5*10^6$ years	6.7 years	$2.7*10^4$ years	9.7 days

Figure 3: The average brute force attack effort on the Master password for lastpass.

Table 1: Comparison of Different Password Storing techniques.

Author	Research paper title	Technique/method	characteristics
S. Agholor[1]	A Secured Mobile-Based Password Manager	Use mobile phone to store password	Provide more effective security than other. It is also resistant shoulder surfing.
Hao Fang[2]	SESS: A Security-Enhanced Secret Storage Scheme for Password Managers	Security-Enhanced Secret Storage Scheme	Provide soundness and password-privacy against malicious adversaries. Resist offline dictionary attacks.
Bian Yang [3]	Cloud Password Manager Using Privacy-Preserved Biometrics	Cloud based plus addition biometric feature	Authentication process takes place in the client end which is highly privacy-respected.
Rui Zhao, Chuan Yue [4]	A Security Analysis of Two Commercial Browser and Cloud Based Password Managers	Local drive in cache file and on cloud	Did not need to remember password. Easy to use.

3. Comparative Study

In this section, we compare some existing method or technique to store password for authentication of user with security. Mobile based password manager uses mobile device to store password. there is no existing Password Manager that uses the Modified Levenshtein Distance to check the similarity between the user chosen password and the generated faux passwords in order to make identification of real password is very difficult. None of the existing Password Managers to the best of our knowledge stores its datain a Decentralized File Format architecture.

Storing password in pendrive through mobile based, local drive and cloud based password manager with proposed system and hence, it allows one to fills in your username and password data automatically, usually via a browser extension. Passwords are just one piece of the puzzle in combating identity theft. The other pieces are strong antivirus software, firewalls, and using a VPN, but when the only method for controlling access to your personal information is a strong password, the best thing we can do is to be aware of the security risks, maintain strong passwords and adding one more factor of physical device such as pendrive . So using pendrive stored password for identification and authentication of user's account also increases the security.

4. Problem Statement

Many users tend to use easy remember password and they can be crackable. Some research show that mostly user use password which is less than 9 characters which can be attacked by attacker easily and guessing attack is more common . User also seems to make some of rules and advises concerning the security. Another problem that sometime users reuse the same password for the multiple online account So, in order to prevent this problem the proposed system use pendrive as key for login to account that helps you organize all the passwords.

5. Conclusion

This survey gives the brief overview of password storage methods and security. We studied different mechanism to store password for user and how their security is improved. In this, there are 3 basic methods to store password securely with its user. It gives idea about how password related problem of user can be solved by storing and managing with appropriate account instead of remembering or using one password to all account.

References

[1] S. Agholor, A.S. Sodiya, A. T. Akinwale, 0. J. Adeniran,”A Secured Mobile-Based Password Manager "; 2015IEEE International Conference.

[2] Hao Fang, Hu Aiqun, Le Shi and Tao Li,”SESS: A Security-Enhanced Secret Storage Scheme for Password Managers"; 2015 IEEE.

[3] Bian Yang, Huiguang Chu, Guoqiang Li, Slobodan Petrovic, Christoph Busch,”Cloud Password Manager Using Privacy-Preserved Biometrics"; 2014 IEEE International Conference on Cloud Engineering.

[4] Bian Yang, Huiguang Chu, Guoqiang Li, Slobodan Petrovic, Christoph Busch,”Cloud Password Manager Using Privacy-Preserved Biometrics "; 2014 IEEE International Conference on Cloud Engineering.Linhong

[5] Rui Zhao, Chuan Yue, Kun Sun,” A Security Analysis of Two Commercial Browser and Cloud Based Password Managers”; BioMedCom 2013.

[6] “LastPass Password Manager.” https://lastpass.com/. “RoboForm Password Manager.” http://www.roboform.com/.

[7] “LastPass, Online Password Manager, May Have Been Hacked,” http://www.pcworld.com/article/227223/LasPass Online Password Manager May Have Been Hacked.html.

[8] Amir Herzberg and Ahmad Jbara, “Security and Identification Indicators for Browsers against Spoofing and Phishing Attacks,200