ISSN No: - 2456- 2165

Forgot Password: A Double layer Security for Password Protection

Rakhee M[1], Sreelakshmi R[2], Varsha V Menon[3], Asha Elizabeth Varghese[4], Alka M Varghese[5]

Assistant Professor[1], Student[2,3,4,5]

***Abstract*—There are many new developments in the field of information technology offered to the people, but there are security related issues too that are not tackled well. One of the most important security features to be looked after are the passwords. It is important for all users to have a secure and unpredictable password. Since a cyber-attacker concentrates more on decrypting the password files, the maximum security should be provided and it should be in the highly encrypted form. Hence at the time of an unauthorized login, the original data should be kept hidden. For each user account, the legitimate password is stored as binary data in the password file along with a timestamp inserting special characters at certain positions as per the timestamp. Timestamps like system time are considered for the encrypting of the legitimate password, each time the user logs in. At every login session the encrypted password is updated in the password file in order to create an ambiguity for the cyber attacker and provide more protection to the user's account.**

***Keywords*— cyber-attacker, encryption, legitimate password, timestamp.**

I. Introduction

Disclosure of password files is a severe security problem that has affected millions of users and companies like Yahoo, RockYou, LinkedIn, eHarmony and Adobe, since leaked passwords make the users target of many possible cyber- attacks. These recent events have demonstrated that the weak password storage methods are currently in place on many web sites. Since we have so many passwords we often fall into the trap of either making the passwords too simple or use the same password for everything. Passwords are designed to make sure no one else can get into your accounts, if it is too easy/common hackers can try a number of common passwords and get in. If we use the same password for every site, it will also run the risk of opening up everything to attacks if someone figures out your only password. So we need a mechanism in which we can use same password for various accounts.

II. Literature Survey

Many researches have already worked for improving internet security of password. Herley and Florencio [4] proposed a method, in which malicious behavior on every incorrect or unauthorized login will be found out. This system helps to protect online banking accounts from brute-force attacks. For every single user false login attempts with few passwords will generate fake accounts so that malign behavior is caught.

Imran Erguler said how the honeyword is created and the password is stored in the form of honeywords in his paper "Achieving Flatness: Selecting the Honeywords from Existing User Passwords" [1]. The passwords are selected and checked if they match with honeyword or real password. The paper mainly focuses on the various methodology used for carrying out the process of generation of hashed password like Chaffing by tweaking, Chaffing-with-a-password-model, Chaffing with Tough Nuts and hybrid model. Only the false password file will be visible to the hacker which is the merit of that systems. But after the use of the system some drawback has occurred, like less authentication process. Honeyword i.e. false password forces the attacker to brute force the hashes one at a time, instead of attacking them as a group. He finally proposed a system of generating honeywords from the existing user passwords. The system architecture is shown in figure(1).

There is another system[3] which is a new way of protection for the password named Password Agent and the hashing technique followed is Random Salt hashing, this is the technique used for the mapping of the password when the user enters it in the require application. The password is divided into 2 parts the Repository &amp; the agent. The passwords are traced in a number of stages when the user is using the corresponding website from the loading on to the site, browsing in the site, login time, changing password, roaming situations, multiple accounts with the same username or password, change of password in the site, password format change. The security analysis is done in a wide range of techniques Unique Passwords, Offline Attacks, Compromised Plain-text Password, Compromised Site Password, Basic Phishing Protection, Advanced Phishing Protection, Shoulder Surfing Protection, Secured Remote Storage. The benefits of using these techniques are ease of site password updating, notification of protected sites, changing master password, site specific password requirements, minimal changes to browsing paradigm. The evaluation is done by the participants and the a tsk performed. There are limitations to the proposed technique such as the vulnerability to key loggers, the reliance on Salt Repository, and the usability limitations.

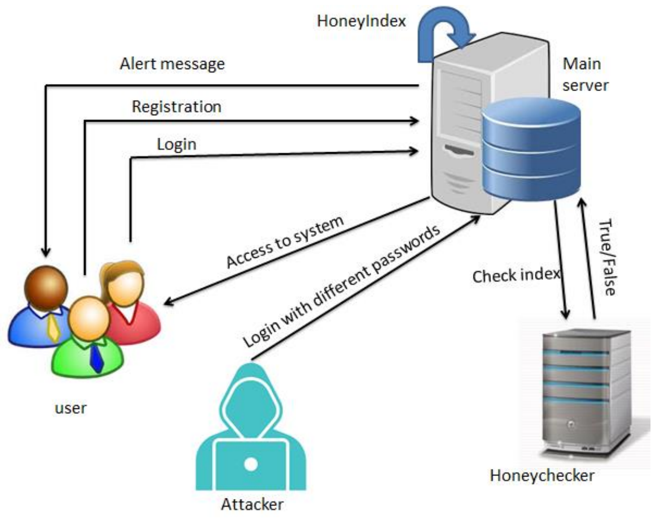

FIG 1. SYSTEM ARCHITECTURE

III. PROPOSED WORK

Password files have got a lot of security problem that has affected millions of users as well as many companies. Password file is generally stored in encrypted format, if a password file is stolen or theft by using the password cracking techniques, it is easy to capture most of the plain text and encrypted passwords. First passwords must be protected and secured by using the appropriate algorithm. And a secure system should detect the entry of unauthorized users in the system.

A cyber-attacker who steals a file of hashed passwords cannot be sure if it is the real password or a honey word for any account. The main disadvantage of using honey words is that large storage space is needed to store the honey words generated by the system. Here, we propose a system where the passwords are encoded using timestamps. Here, timestamps refer to the time between the log in and log out of the user from the account. Every log in and log out of the user to the account updates the password file. Therefore, it may be difficult for a cyber-attacker to use the passwords in the encrypted format and then use them to log in to an account. The attackers need to decrypt the password file. The decryption process can only be carried out using certain algorithms.

The main aim behind the development of this project is to give more security on passwords so that the original password is not available in the database.

IV. PROBLEM STATEMENT

While logging into several services in public, we may have to expose our passwords to unknown parties unconsciously. People with malicious intent could watch the whole authentication procedure and use our personal assets. And also, the difficulties faced to memorize extra information during authentication.

V. IMPLEMENTATION

The work is implanted on a Municipal Co-operation Office work, the documents need to be kept safe so the files corresponding to each user is protected by encoding the one to one password of the user as per the login time and logout time i.e. the encoding of the password is done by calculating the timestamp-a sequential key is used for encoding and as the next layer of protection the password file which hold the password information of all the users are kept encrypted with a random key generation and this file can only be decrypted only if the key is known. The algorithm used for encrypting & decrypting of file is AES algorithm hence a symmetric form of cryptography is used in this system. The work is divided into following different modules.

A. *Module Description*

1. REGISTRATION

User initially registers their details such as their personal details along with a username and password. After registration user can directly login to the application.

2. Login

At the time of login the username and password entered by the user is checked with the original username and password which is entered by the user at the time of registration. But at each logout time the password in the database is updated and at each log in time the user need to enter the timestamp which is received through their mail id. The database contains the encoded password which is generated using that timestamp. For comparison the password in the database need to be decoded using the same.

3. ENCODING

After each logout the password is updated and encoded with the help of the generated timestamp. The time of the login and log out session are stored in the database. The timestamp is generated by taking the difference between the log in time and the log out time. The encoded password is then encrypted using RSA algorithm. The encrypted password is stored in the database and the timestamp is mailed to the user which is used for the next log in.

4. DECODING

At the time of each login the user need to enter the timestamp which is received through their email. The entered timestamp will be compared with the timestamp which is stored in the database. The encrypted password should be decrypted using RSA algorithm and finally decoded for every log in using the timestamp.

VI. FUTURE IMPLEMENTATION

For the existing system, the text passwords are stored in the form as entered by the user. Here, we propose a system where the password is encrypted and encoded and stored in the password file. This creates difficulty for the cyber attacker to access the password stored in the password file. The hackers may find it difficult to guess, decode and decrypt the passwords stored in the file. There are certain algorithms that are used for the encoding and encryption of the password which is unknown to the cyber attacker and the decrypting algorithm is different from the encoding algorithm and therefore making it a mess for them. There are timestamps inserted at different positions of the passwords that are stored in the password file. Thus the passwords will be different from the exact password when stored in the password file in encrypted form. For every log in of the user, the password will be decrypted and checked with the entered password. If there is a match, then the login will be reflected as successful. But, there is security is provided for the system, when another user who knows your password logs in. The third party can thus access your credentials. This could be solved by the implementation of graphical password. This could act as a extra layer of protection to your account. Therefore the user can log in to their account with the help of graphical passwords. The system describes that the user can provide at least three pictures or videos during the time of registering to the account and then select few cells, say three cells from every picture that they have uploaded, which is shown in fig (2).

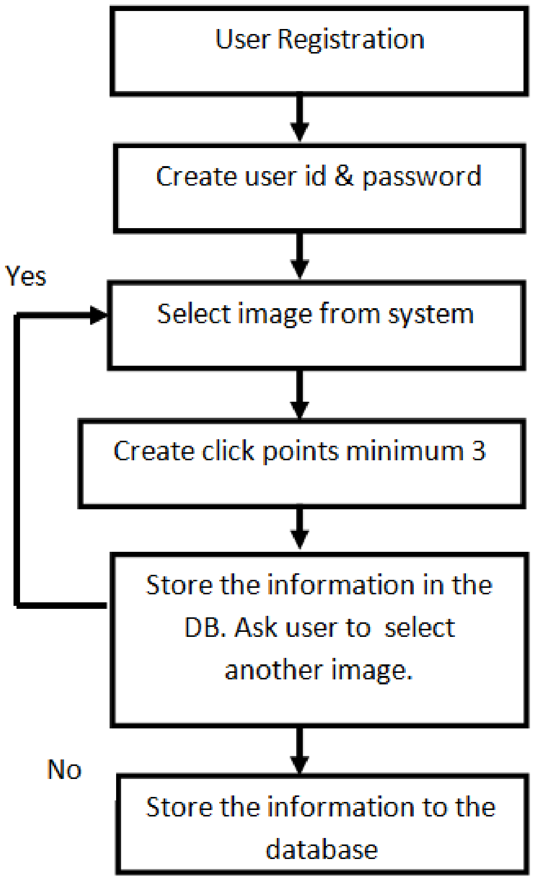
User Registration
Create user id & password
Yes
Select image from system
Create click points minimum 3
Store the information in the DB. Ask user to select another image.
No
Store the information to the database

Fig.(2) User Sign Up Process

If the user has uploaded a video other than picture the user can select several instances of the video as a key. These pictures or videos should be selected by the user during the login. If the selected pictures are exactly same as that of the pictures uploaded during the registration, then a matrix known as the Pass Matrix will appear on the selected pictures and request the user to select the cells that they have selected during the registration process. If the user fails to select the right images during the log in time, then the user account will be locked and an OTP number could be send to the mobile number of the user by which they have registered. This acts as an extra layer of security to the user account.

VII. Conclusion

In this paper, it is designed a suitable method to avoid password cracking. The principle idea of double layered password security of the system can be used as platform in institutes or organizations anywhere where credential data is secured using password. It also helps to monitor administrative processes and evaluate the performance to take decision for improvement. We proposed this system because of the demerits in honeyword security system ,as number of honeywords increases storage cost of system will increase.

Acknowledgment

First and the foremost we would like to thank Lord Almighty for helping me do this project and completing it on time. We are really grateful to all the members who helped us directly or indirectly with their constant encouragement and support throughout the completion, especially for the useful suggestions and corrections given during our works. We would also like to thank all the authors and the anonymous reviewers for their comments and the views on the topic that helped us improve the quality of the work. I express my heartfelt veneration to all who had been helpful and inspiring throughout this endeavor.

References

[1] Imran Euguler, "Achieving Flatness: Selecting the Honeywords from Existing User Passwords," *IEEE Tranactions. on Dependable and Secure Computing*, vol. 13, No 2, March/April 2016.

[2] Miss. Saraswati B.Sahu and Angad singh, "Secure User Authentication & Graphical Passwordusing Cued Click-Points", *International Journal of Computer Trends and Technology(IJCTT), Vol. 18, No. 4,December 2014* .

[3] Benjamin Strahs, Chuan Yue, and Haining Wang, "Secure Passwords Through Enhanced Hashing," *Department of Computer Science The College of William and Mary Williamsburg,* VA 23187, USA, {bgstra,cyue,hnw}@cs.wm.edu.

[4] C. Herley and D. Florencio, "Protecting financial institutions from brute-force attacks," in SEC'08, 2008, pp. 681–685.

[5] M. Weir, S. Aggarwal, B. de Medeiros, and B. Glodek, "Password Cracking Using Probabilistic Context-Free Grammars," in Security and Privacy, 30th IEEE Symposium on. IEEE, 2009, pp. 391–405.

[6] Prof.Vina M.Lomte, Kiran R.Pawar, Rushikesh M.Shivsharan,Kiran V.Swami, and Akshay A.Vishwasrao,

"Efficient approach for High Level Security using Honeyword," International Journal of Engineering Sciences and Research Technology, October 2015.

[7] Rahul Jambhale,Sagar Ombale, Prof. Deepa Manoj," Solicited Honeyindexed Password of an Universal Set of Honeyindex Using Shuffling Technique Ensuring Safty of Files in Distributed Envi- ronment ",International Journal of Current Trends in Engineering Research. (IJCTER) Volume 2 Issue 6, June 2016.