MULTIFACTOR AUTHENTICATION AND RANDOM PASSWORD GENERATION TO PREVENT ATTACKS

R.Nisharanjani*

J.R. Thresphine**

ABSTRACT

Network safety engrosses the consent to get access to information in a network. Client prefers an ID and password or other substantiating information that permits them retrieve the data and programs within their mandate. Web-security is the wing of processor security explicitly associated to the Web. Its intention is to establish rules and measures to aid anti attacks. At the outset, Text passwords are most accepted custom of client endorsement on websites due to its ease and unfussiness. Conversely user's password are flat to be stolen and cooperated below different intimidation and risks. Secondly, to steer clear of these password attacks a technique oPass which controls mobile phone for login to the websites was used. However this technique was cost-effective merely in smart mobiles. To overwhelm these pressure, we suggest an approach of Multifactor authentication and random password generation which is further proficient and cost-conscious by the exercise of an usual mobile. Clients key in the username and long term password. Moreover,an image is worn as a password via Steganography . The Short term password is generated through long term password. This method eradicates Domino effect, Dictionary attacks, Brute force attacks, Password reuse attacks.

Key Terms— Web Security, Multifactor Authentication, Domino Effect, Dictionary Attacks, Brute Force Attacks, Password Reuse Attacks.

* M.Tech(CSE),Prist University

** A.P, Dept. Of .CSE, Prist University

1. INTRODUCTION

Beyond the years,Text passwords has been accepted as the principal standard for clients for websites. Browsers pick their username and text passwords when entering accounts on a website. In order to log into the website profitably, client must recollect the particular passwords. In general, password-based client verification can withstand brute force attacks and dictionary attacks if clients choose robust passwords to afford adequate entropy.

However, password-based client verification has a key challenge that individuals are not specialists in learning text series. Hence, most clients would prefer simple passwords (i.e., feeble passwords) even if they know that the passwords may be insecure. One more critical drawback is that clients be likely to reclaim passwords across different websites. Password reclaiming tends clients to be unable to find delicate data saved in different websites. If the hacker manages to find one of the passwords, this attack is known as the password reuse attack. These inconveniences are due to the harmful power of human issues. Hence, it is significant to consider the human issues when manipulating a client verification protocol**.**

Phishing is the most familiar and professional password stealing attack .Some enquiries concentrates on three-factor verification quite than password-based authentication to offer more trustworthy client verification. Three-factor authentication depends on password, proof and biometric. To permit the authentication, the client must enter a password and offer a pass code create by the proof (e.g., RSA SecureID), and check the client's biometric character (e.g., fingerprint or pupil). Three-factor authentication is an inclusive destructive means in opposition to password theft attacks, but it involves relatively increased cost.

Therefore, two-factor authentication is extra smart and realistic than three-factor authentication. Even though a lot of banks hold up two-factor authentication, it yet goes through the harmful power of human issues, such as the password reuse attack. In this thesis, we put forward a multifactor authentication protocol, which involves a long-term password. It is the only password required to be remembered by the clients. Using random password generation, a short-term password is generated. The Short-term password is received by the client's cellphone which is further proficient and cost-conscious by the exercise of an usual mobile.

Moreover, an image is worn as a password via Steganography besides the short-term password for added precautions**.** Hence, the main concept of Multifactor authentication and random password generation is to unbound the clients from having to memorize or enter whichever passwords into regular computers for authentication.

2. PROBLEM DEFINITION AND ASSUMPTIONS

In this section, we consider various methods of password stealing. Afterwards, we introduce the architecture of our Multifactor authentication and random password generation system and make some reasonable assumptions. People nowadays rely heavily on the Internet since conventional activities or collaborations can be achieved with network services (e.g., web service). Widely deployed web services facilitate and enrich several applications, e.g., online banking, e-commerce, social networks, and cloud computing. But user authentication is only handled by text passwords for most websites. Applying text passwords has several critical disadvantages.

First, users create their passwords by themselves. For easy memorization, users tend to choose relatively weak passwords for all websites. Second, humans have difficulty remembering complex or meaningless passwords. Some websites generate user passwords as random strings to maintain high entropy, even though users still change their passwords to simple strings to help them recall it. . Third,alternate two factor authentications using mobile phones are effective but are not economical .The reason for unreliability is ,they require a highly advanced smart mobile phones which are not at all economical. Eventhough all these facilities are available,the long-term passwords are under the risk of being thefted.

3. MULTIFACTOR AUTHENTICATION AND RANDOM PASSWORD GENERATION

Therefore, we proposed a user authentication, called Multifactor authentication and random password generation, to thwart the above attacks. This

paper includes the mechanism of Multifactor Authentication where the username and the long-term password is entered into the untrusted computers by the clients. The long-term password

entered generates the Short-term passwords for that particular session alone and it expires once the client logs out.

Moreover for improved security against the long-term password,an image is also given as a password which contains hidden information embedded in it using Steganography. The client can enter into the website only after entering both the long-term password and the image.This Multifactor authentication consists of separate modules for each and every operations.In this section, we introduce a method in which the user can authenticate over the data to prevent from attacks. This method contains four phases namely, password generation, security, attack prevention and recovery phases.

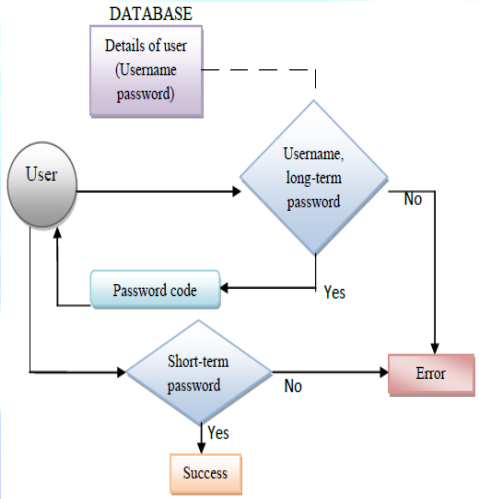

Fig 3.1: Overall Architecture

4. OVERALL ARCHITECTURE

Figure3.1 shows the description of each phases in the MAARG. Like standard web logins, it uses as a multi authenticator over the data. For multipurpose security, proposes generation of short term password and the data can be encrypted into the image using steganographical method. In the password generation phase, the user enters username and long-term password in the web logins. Then it creates random password that is used as a short term password for the user while entering into the browsing.

PHASE 1: PASSWORD GENERATION

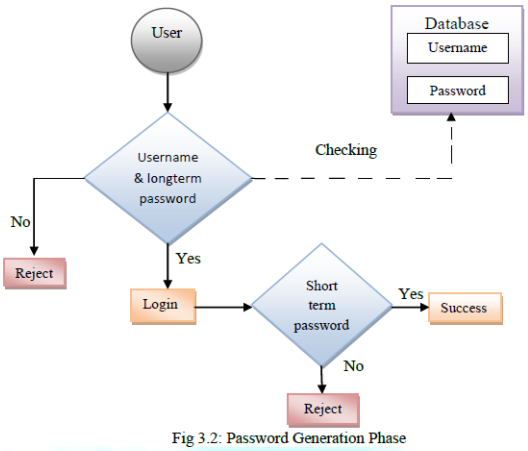

Fig 3.2: Password Generation Phase

In this phase we store the details of username and password in the database. User also clearly specifies their long-term password which will be used by user through the entire trusted browsing. It compares the given details of username and password with the details stored in the database. It will login if the details are correct. Then the short-term which should be changed for every successive login. trusted.

PHASE 2: **SECURITY PHASE**

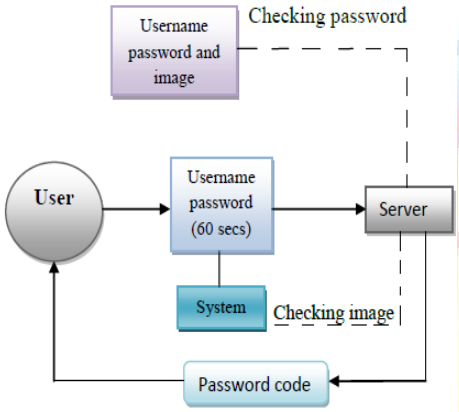

Fig3.3: Security Phase

In this phase security is enhanced by using the content based image retrieval method which uses steganographical algorithm. Once the long-term password is entered it checks for the image in the system by comparing with the image stored in the database . this phase is mainly used for the image checking and enters into the required website by generating the one time password.then

the password code is sent from the server to the users mobile indicating that authentication is completed successfully.

3.ATTACK PREVENTION

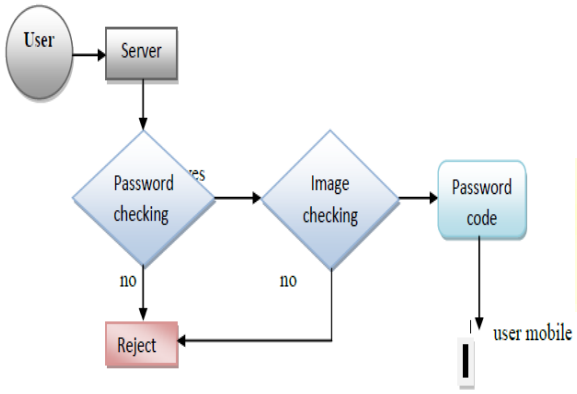

Fig 3.4: Attack Prevention Phase

This phase provides security to our data in many ways from the hacker from being hacked. If the hacker knows the long-term password of the user he can easily enter the website. Through he knows the long-term password; he needs to know the image which is also used as the password for login. Even though he knows the image he needs to know the password code of the mobile. So this is believed to be the security phase in this project in order to improve the security of the data from the hacker.

PHASE 4: RECOVERY PHASE

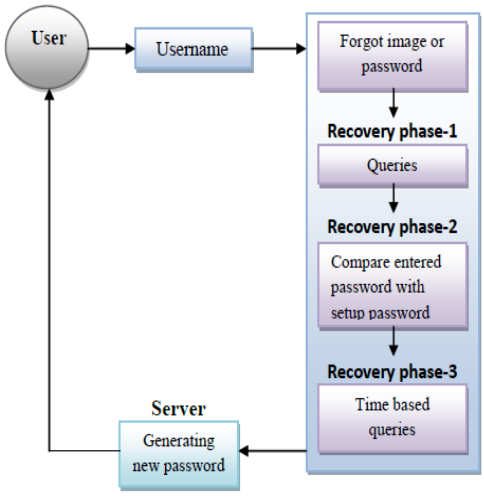

Fig 3.5: Recovery phase

If the user tends to forget the password or loss of an image, this recovery phase is used in order to recover the forgot password. The recovery phase-1 performs the operation of displaying the queries given by the user at the time of registration. The user answers the queries and recovery phase-2 performs the operation of checking the answers with the stored answers in the database. After successfully completing the recovery phases it helps to allow the user to change the password.

5. FUTURE WORK

An amount of preceding scholars have presented to safeguard clients' credentials from phishing attacks in client verification. The presented systems controls variable techniques. Still, these results were short in view of the harmful power of human issues, such as password reuse and weak password crisis. Even more protected against the rivalries from the theft of the password, situations may occur of tracing the original image due to carelessness of the clients'.

6. CONCLUSION

In this paper, we propose Multifactor Authentication and Random Password Generation which is an efficient password management technique to remove password reuse attacks, where the username and the long-term password is entered into the untrusted computers by the clients. The long-term password entered generates the Short-term passwords for that particular session alone and it expires once the client logs out.Moreover for improved security against the long-term password,an image is also given as a password which contains hidden information embedded in it using Steganography. The client can enter into the website only after entering both the long-term password and the image. This image is used for additional security in order to wipe out the stealing of the long-term password.

7. REFERENCES:

[1]Hung-Min Sun, Yao-Hsin Chen, and Yue-Hsun Lin ”oPass: A User Authentication Protocol Resistant to Password Stealing and Password Reuse Attacks” vol. 7, no. 2, april 2012.

[2] S. Chiasson, A. Forget, E. Stobert, P. C. van Oorschot, and R. Biddle,“Multiple password interference in text passwords and click-based graphical passwords,” in *CCS ’09: Proc. 16th ACM Conf. ComputerCommunications Security*, New York, 2009, pp. 500–511, ACM.

[3] K.-P. Yee and K. Sitaker, “Passpet: Convenient password management and phishing protection,” in *SOUPS ’06: Proc. 2nd Symp. Usable PrivacySecurity*, New York, 2006, pp. 32–43, ACM.

[4] K. M. Everitt, T. Bragin, J. Fogarty, and T. Kohno, “A comprehensive study of frequency, interference, and training of multiple graphical passwords,” in *CHI ’09: Proc. 27th Int. Conf. Human Factors Computing Systems*, New York, 2009, pp. 889–898, ACM

[5]P. van Oorschot, A. Salehi-Abari, and J. Thorpe, “Purely automated attacks on passpoints-style graphical passwords,” *IEEE Trans. Information Forensics Security*, vol. 5, no. 3, pp. 393–405, Sep. 2010.

[6]M. Weir, S. Aggarwal, M. Collins, and H. Stern, “Testing metrics for password creation policies by attacking large sets of revealed passwords,” in *Proc. 17th ACM Conf. Computer Communications Security*, New York, 2010, pp. 162–175, ACM.

[7]M. Mannan and P. van Oorschot, “Using a personal device to strengthen password authentication from an untrusted computer,”*Financial Cryptography Data Security*, pp. 88–103, 2007.

[8]C. Yue and H. Wang, “SessionMagnifier: A simple approach to secure and convenient kiosk browsing,” in *Proc. 11th Int. Conf. Ubiquitous Computing*, 2009, pp. 125–134, ACM.