IOSR Journal of Computer Engineering (IOSR-JCE)
e-ISSN: 2278-0661,p-ISSN: 2278-8727, Volume 16, Issue 5, Ver. VIII (Sep – Oct. 2014), PP 56-60
www.iosrjournals.org

Secured Password Technique Using Devices

Mekha Mariyam Thomas,
Department of CSE, thomas.maria2@gmail.com, +918281330643

Abstract: *Text based password is most commonly used user authentication .To log on to websites, users must memorize the selected password. Password based authentication can resist brute force and dictionary attacks, if they select a stronger password but users often select weak password for their convenience and remembrance. They reuse password in different sites for simplicity, it would make the attacker to find their passwords in different sites. These are caused by the negative impact of human behavior. Typing password on untrusted computers suffers from stealing of password i.e. shoulder surfing. Then researchers have designed graphical password which made attackers to find out the commonly selective areas (Hotspots). Some researchers have focused on three-factor authentication for reliability and depends on password, token, biometric. For this authentication, the user must input a password and provide a pass code generated by the token, and scan her biometric features (e.g., fingerprint). This is a comprehensive defense mechanism against password stealing attacks, but it requires high cost. Another user authentication is Opass, which uses a cell phone to enter the password. The password that is entered by the user is converted to a one-time password and in this system it provides more security by enabling a encryption for the converted one-time password. By using the cell phone and providing an encryption, the security can be increased. This would reduce the user from remembering from many passwords and thus reduce the password stealing. The user can then successfully enter to their website and enjoy the accessibility. This reduces the negative influence of human factors compared to previous schemes, and is the first user authentication protocol to prevent password stealing (i.e., phishing, keylogger, and malware) and also prevent password reuse attacks simultaneously.*

Index Terms: *Password reuse attack, password stealing attack, user authentication, Hash function.*

I. Introduction

Over years text password has being commonly used user authentication. The primary medium of user authentication was text passwords. The users have to select a username and a password while registering and can login by using this username and password. Password based authentication can resist attacks like brute force and dictionary attack if users are selecting a stronger password but the main problem with the users is that they select weaker password for their remembrance even though they know that the password is unsafe. Another main problem is that they reuse password in different websites [1], [2]. Florencio and Herley[3] , in 2007 found that a user will reuse a password 3.9 different sites. Password reuse causes the information lose since if a hacker compromises in a password he would be able to find the data of different sites where the user uses the same password. Researchers have found many technique to overcome the problem of password stealing like graphical password [4] and password management tool [5]. These would automatically generate password which lead to password reuse and password recall problems. Although graphical password is a great idea it was not widely used [6] and still was under many attacks [7]. Password management tool worked well but users doubted its security. Another important issue is the password stealing attack, they impersonalize users identity and collect information and do unauthorized actions [8]. Phishing is the common attack. Many studies have being conducted to defend password stealing attack [9],[10].

Some researchers has focused on three phase authentication which is more reliable but it depends on password, token, biometric. First it check the user input, and provide a pass code generated by token and scan her biometric. It is comprehensive defense mechanism by it is of high cost. Two phase is more practical than three phase but it suffers from negative impact of user in most banking system two phase authentication is used but it suffers from password reuse attack. Another method is the user authentication called the opass [11] which leverages a user cell phone. A user can login to their websites by entering their username on the browser and typing their password on to their cell phones which would be converted to a one time password. And to provide a more secure system this provides a encryption for the converted one time password. So a more secure user authentication system is introduced in which, the user only have to remember a long term password for different sites.

The proposed system brings the following advantages:

1) Password Reuse Prevention and Weak password Avoidance - System uses the one-time password so each time the user login to their sites the system generates a different password. They have to remember only a single long term password for all their websites.
2) Anti- malware – Malware collect

3) sensitive information from users commonly their passwords. In this system leverages by typing their password on their cell phones rather than the site.

II. Related Work

Researchers had found a variety of methods to avoid the attacks like brute force, dictionary, phishing and so on. The solution leverages the negative influence of human factors such as password reuse and weak password problems.

To prevent the problems of user authentication M.wul [12] proposed a system on a trusted browser and a mobile device. To avoid the phishing attack a random session name is sent by SMS but it from proxy to device which was encrypted by A5/1 which was broken by Barkan and Biham [13]. , phishing is particularly a insidious problem, since trust forms the foundation for customer relationships, and phishing attacks undermine confidence in an institution. Phishing attacks succeed by exploiting a user's inability to distinguish legitimate sites from spoofed sites. The proposed system encrypts every data before transmission.

Another well known approach is MP-Auth presented by Mannan and Oorschot [14]. Password based authentication is strengthened by inputting a long secret password over the trusted mobile device and before it is send to the untrusted kiosk it is encrypted by a preinstalled public key on a remote server. This encryption is done to protect the password from attacks from the untrusted kiosks. MP-Auth also suffers from password reusable vulnerabilities. It also assumes that the password and the account is secure. The user has to post his account and password such as in banks. Our system is protected from this by a secure one time password and an secure AES encryption.

Similarly another work by parno [15] used device as authentication token to construct an anti-phishing mechanism called phoolproof. To log on the website the user has to enter the issued public key and the username/password combination. It needs physical contact to check whether the account is secure and still possess the reusable problem.

Another work is Opass which leverages by using a mobile phone and the password which is entered in phone is converted to a one time password . In the proposed system the one time password so generated is encrypted by using the AES algorithm which gives more security to the password so generated by the user.

One-Time Password

The one-time passwords are generated by a secure one-way hash function. With a given input x, the set of onetime passwords is established by a hash chain through multiple hashing. To prepare N one time password. The password is produced by performing N hashes on input x

$$\delta_0 = H^N (x)$$

The next one-time password is obtained by performing (N-1) hashes

$$\delta_1 = H^{N-1} (x)$$

Hence, the general formula is given as follows:

$$\delta_i = H^{N-i} (x)$$

For security reasons, we use these one-time passwords in reverse order, i.e., using , δ_{N-1} then δ_{N-2} , ...0 . If an old one-time password is leaked, the attacker is unable to derive the next one. In other words, she cannot impersonate a legal user without the secret shared credential x . Besides, the input x is derived from a long-term password (P_u), the identity of server ID_s , and a random seed (∅)generated by the server

$X = H(P_u \| ID_s \| \emptyset)$

Note that function is a hash which is irreversible in general cryptographic assumption. In practice, is realized by SHA-256 [16] in oPass. Therefore, the bit length of x is 256.

III. Problem Definition And Architecture

This section deals with how the passwords are stolen which are entered by the user and then the architecture of the system can be described.

Problem Definition

Nowadays all the people greatly depend on internet for everything. They are facilitated with many technologies and several application on the internet like online banking, online shopping, e-commerce, cloud computing, etc. most of the users use text password and graphical passwords for most of the websites which has many disadvantages like stealing.

First of all users select their own password in which most of them select weak password like their date of birth or anything for them to memorize. And these passwords would be used by them for many websites. And this makes the hackers to find the password from one site and steal their sensitive information.

Secondly humans have difficulty in remembering strong passwords [4]. Some system generates their own password for individuals but the often change their password to simple one to memorize them. And these would lead to password reuse problem. Florencio and Herley [3] has found that users forget passwords a lot. Users may generate another account due to this problem. Password management [12],[34] has also paid attention a lot to the password problem. But it was more complicated to use. And if the graphical password is used to lead to the same click points called the hotspots such as if in a picture girls would probably select a flower or a doll likewise boys would select their interested areas which lead to the hotspot problem.

So a proposed system is introduced in which a more secure user authentication to thwart the attacks. The main goal of the system is to provide more security and make the users free from typing the password on the untrusted browser. And which provides a secure password mechanism by adopting one time password generation. The generated one time password is no longer existed. And this provides more security by encrypting the generated one time password, because during the travel through the network the password can be stolen since the one time password contains the password. A onetime password would be expired when the user completes the current session. Next time the user enters the site and type the long strong password another form of one time password would be generated. The user can log in to different sites by using this same type of password which the attacker cannot find since it is one time generated. In this system it provide a SMS channel and a users cell phone to avoid stealing of password. In this system the user only have to remember a long password and this is used to protect the information from a password thief.

Architecture of the system

The architecture of the system is shown in Fig.1. To login securely this system consists of a cell phone, a browser, and a web server that users wish to access. The cell phones and the untrusted computer directly accomplish login securely to the web servers. The communication between the cell phone and the browser is through a secure SMS channel. Using the internet the web browser and the web server interact

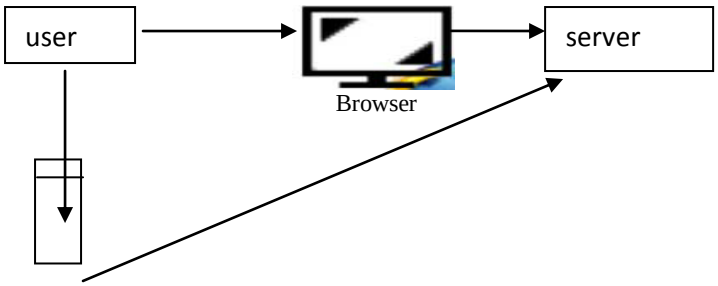

Fig 1: Architecture of the System

Steps involved in the Proposed System

1. During the registration process, the user registers their username on the browser.
2. The user can enter the password on the phone .
3. Then he can log in the website by using this password.
4. These passwords would generate as one time password and can enter the site

During registration the user has to specify the users id and url to the cell phone . This would be send to a TSP and TSP send the user id and phone number to the sever. Server sends back the url and this would send to the cellphone and the user can then enter the password on the phone. Cell phone then communicates the server through a secure SMS channel.The password entered would be converted to a one time password and is encrypted by using AES algorithm and send to the server. So a third party won't be able to hack the password and these one time password would be expired after this session. If the user wants to enter again to this website, he would enter the password on to the phone and this would generate another one time password. To provide more security this one time password is encrypted by using AES encryption. So our proposed system would provide more security.

Fig. 2 describes the operational flows of users during each phase of the system. Unlike other web logins, this system utilizes a user's cell phone as an authentication token and an SMS as a secure channel. In the registration *phase*, a user starts the program by registering her new account on the website. Unlike other conventional registration, the server requests for the user's account id and phone number, instead of password. The entered long term password is used to generate a chain of one-time passwords for further logins on the target server. Then, the program automatically sends a registration message to the server for completing the registration procedure. The context of the registration is encrypted to provide data confidentiality. Login procedure in our system does not require users to type passwords into an untrusted web browser. The only information input to the browser is the username. Next, the user opens the program on her phone and enters the long-term password;

the program will generate a one-time password, encrypt it and send securely to the server. The login is encrypted by the one-time password. And these are encrypted by using AES algorithm for more security.
and cafes. Attacks like keylogger, malware, and phishing would take place. so a threat model is implemented that is more secure.

Threat Model

Attackers can interrupt any messages over the internet and network. Attacker can spoof message send through GPRS to cheat the users. The computer which is used is untrusted so attackers can install malwares and collect the sensitive data. The attacker's goal is to gain access to websites and this can be classified in two categories based on attacker target i.e. user and server. Since these messages are encrypted and send it cannot be accessed by the attacker.

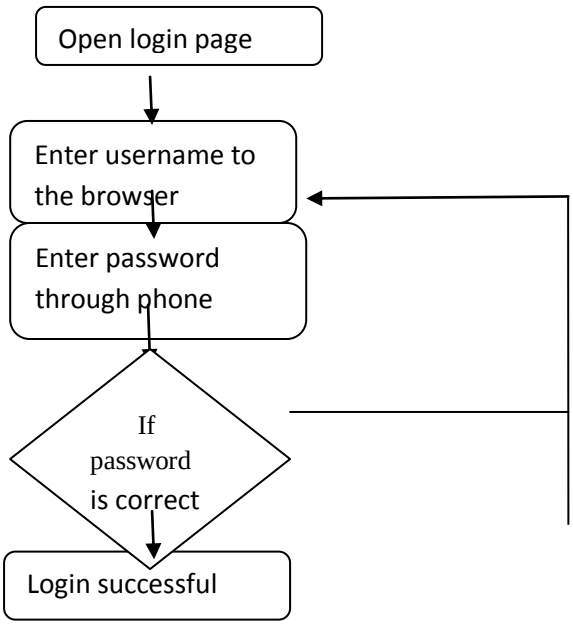

Fig 2: Login process of the system

.

IV. Security Analysis

Protecting user credentials on web access browsers is important since they are located everywhere, such as airport lounges, book publishing, business centre

Table I:Comparison of the proposed system with the other conventional systems

	Attack Prevention			*Requirements*	
	Phishing	*KeyLogger*	*Password Reuse*	*Proxy*	*Malware free mobile*
MP-Auth	*Prevents*	*Prevents*			*Needed*
Phoolproof	*Prevents*	*Prevents*			*Needed*
M.wu	*Prevents*	*Prevents*		*Needed*	*Needed*
Proposed System	*Prevents*	*Prevents*	*Prevents*	*Needed*	*Needed*

Weak password

The weak password problem, means the users tends to select weak passwords because the passwords are easy for them to remember so in our system the system itself would generate a password.

Attacks on Login

The attacker can launch attacks to masquerade itself as a legitimate user without being detected, during login process. The attacker cannot obtain a one-time password for login even if he builds a spoof website to launch a phishing attack. So phishing attack cannot take place in the new system. In this system, users type their accounts into the browser and enter their long-term passwords into the mobile phones. System achieves a one-time password to prevent password reuse attacks. Even if a attacker steals a user's cell phone and tempts to log into a website that the user has visited, he cannot login since he does not know the user's long-term password, so he cannot generate a one-time password for the next round.

V. Conclusion

A user authentication protocol, which leverages cell phones to thwart password stealing and password reuse attacks. Each website possesses a unique phone number. The design principle is to eliminate the negative impact of human behaviour as much as possible. In this the user has to remember only a long-term password which is entered in the phone and type their username on their website. Users don't need to type their password on the website so the password is secured. Compared to other schemes this system is the first user authentication system to prevent password stealing (i.e., phishing, keylogger, and malware) and password reuse attacks simultaneously. One time password is used so that it ensure independence between logins.

References

[1] B. Ives, K. R. Walsh, and H. Schneider, "The domino effect of password reuse," *Commun. ACM*, vol. 47, no. 4, pp. 75–78, 2004.

[2] S. Gawand E. W. Felten, "Password management strategies for online accounts," in *SOUPS '06: Proc. 2nd Symp. Usable Privacy . Security*,New York, 2006, pp. 44–55, ACM..

[3] D. Florencio and C. Herley, "A large-scale study of web password habits," in *WWW '07: Proc. 16th Int. Conf. World Wide Web.*, New

[4] 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. Computer Communications Security*, New York, 2009, pp. 500–511, ACM.

[5] S. Wiedenbeck, J. Waters, J.-C. Birget, A. Brodskiy, and N. Memon, "Passpoints: Design and longitudinal evaluation of a graphical password system," *Int. J. Human-Computer Studies*, vol. 63, no. 1–2, pp. 102–127, 2005.

[6] S. Wiedenbeck, J. Waters, L. Sobrado, and J.-C. Birget, "Design and evaluation of a shoulder-surfing resistant graphical password scheme," in *AVI '06: Proc. Working Conf. Advanced Visual Interfaces*, New York, 2006, pp. 177–184, ACM.

[7] B. Pinkas and T. Sander, "Securing passwords against dictionary attacks in *CCS '02: Proc. 9th ACM Conf. Computer Communications Security*, New York, 2002, pp. 161–170, ACM.

[8] J. Thorpe and P. C. van Oorschot, "Graphical dictionaries and themem space of graphical passwords," in *SSYM'04: Proc. 13th Conf. USENIX Security Symp.*, Berkeley, CA, 2004, pp. 10–10, USENIX Association.

[9] 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.

[10] T. Holz, M. Engelberth, and F. Freiling, "Learning more about the underground economy:Acase-study of keyloggers and dropzones," *Proc. Computer Security ESORICS 2009*, pp. 1–18, 2010.

[11] Hung-Min Sun, Yao-Hsin Chen, and Yue-Hsun Lin, "Opass:A User authentication protocol resistant to password stealing and password reuse attacks.

[12] M.Wu, S. Garfinkel, and R. Miller, "Secure web authentication with mobile phones," in *DIMACS Workshop Usable Privacy Security Software*, Citeseer, 2004.

[13] E. Barkan and E. Biham, "Conditional estimators: An effective attack on A5/1," in *Selected Areas in Cryptography*. NewYork:Springer, 2006, pp. 1–19.

[14] 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.

[15] B. Parno, C. Kuo, and A. Perrig, "Phoolproof phishing prevention," *Financial Cryptography Data Security*, pp. 1–19, 2006.

[16] H. Gilbert and H. Handschuh, "Security analysis of SHA-256 and sisters", in selected area cryptography,2003,pp:175-193, springer.