www.ijecs.in
International Journal Of Engineering And Computer Science ISSN:2319-7242
Volume 6 Issue 6 June 2017, Page No. 21726-21728
Index Copernicus value (2015): 58.10 DOI: 10.18535/ijecs/v6i6.28

Secure Web Authentication Using OPASS to Prevent Secret Key Stealing

R. Nithyanandhan[1], Dr.G.Umarani Srikanth[2], Mr.S.Muthukumarasamy[3]
1 .Student,S.A.Engineering College, Chennai, India.,nithyanraghu@gmail.com
2. Professor & Hod, S.A.Engineering College, Chennai, India.
3. Assistant Professor, S.A.Engineering College, Chennai, India

Abstract— Text passwords have been adopted as the primary mean for user authentication in online websites. Humans are not experts in memorizing them, therefore they rely on the weak passwords. As they are the static passwords there are some adversary who can launch attacks to steal passwords, and suffers quitely from few security drawbacks: phishing, keyloggers and malware. This problem can be overcome by a protocol named oPass which leverages a user's cellphone and an SMS to thwart password stealing. Opass greatly avoids the man-in-middle attacks. In case of users lose their cellphones, this still works by reissuing the SIM cards and long-term passwords. This is a efficient user authentication protocol and is at affordable cost.

Keywords— security, password stealing , user authentication.

1.Introduction

1.1 General Information

One of the ancient way to prove identity or gain access to a resource is passwords. A password is nothing that consists to be of any secret word or string of characters that is used for authentication purpose. A typical computer user may require passwords for many purposes: logging in to computer accounts, retrieving the e-mail from servers, accessing programs, databases, networks, web sites, and even reading the morning newspaper online. In websites in order to maintain privacy to greater extent and provide high level of security we use passwords.

Over the past few decades, text password has been adopted as the primary mean of user authentication for websites. People select their username and text passwords when registering accounts on a website. In order to log into the website successfully, users must recall the selected passwords. As humans are not experts in memorizing passwords they easily forget the passwords and these users firstly often select weak passwords and reuse the same passwords across different websites. Routinely reusing passwords causes a domino effect; when an adversary compromises one password, they will exploit it to gain access to more websites. Second, typing passwords into untrusted computers suffers password thief threat. An adversary can launch several password stealing attacks to snatch passwords, such as phishing, keyloggers and malware.

The first commonly used method is the password-based user authentication can resist brute force and dictionary attacks if users select strong password to provide sufficient entropy. However, password-based user authentication has a major problem that humans are feel hard to keep those passwords in memory. Thus, most users would choose easy-to-remember passwords (i.e., weak passwords) even if they know the passwords might be unsafe. Another crucial problem is that users tend to reuse passwords across various websites. Password reuse causes users to lose sensitive information stored in different websites if a hacker compromises one of their passwords. This attack is referred to as the password reuse attack. The above problems are caused by the negative influence of human factors. Therefore, it is important to take human factors into consideration when designing a user authentication protocol.

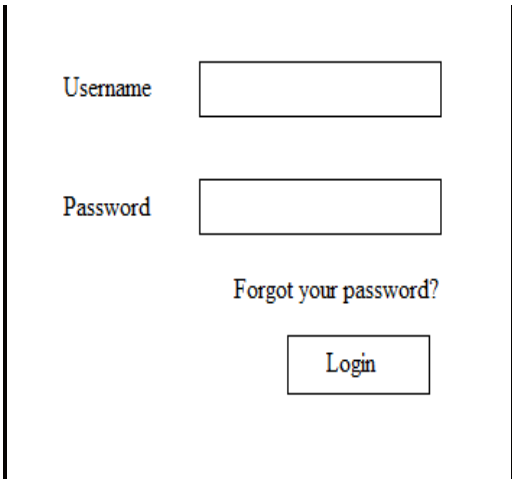

Fig 1:Password-based user authentication

II.Existing Security Measures

Inorder to reduce the negative influence of human factors in the user authentication procedure, the researchers have investigated a variety of technology. Since humans are more adept in remembering graphical passwords than text passwords , many graphical password schemes were designed to address human's password recall problem. Using password management tools is an alternative. These tools automatically generate strong passwords for each website, which addresses password reuse and password recall problems. The advantage is that users only have to remember a master password to access the management tool.

Despite the assistance of these two technologies graphical password and password management tool the user authentication system still suffers from some considerable drawbacks. Although graphical password is a great idea, it is not yet mature enough to be widely implemented in practice and is still vulnerable to several attacks. Password management tools work well; however, general users doubt its security and thus feel uncomfortable about using it. Furthermore, they have trouble using these tools due to the lack of security knowledge.

Besides the password reuse attack, it is also important to consider the effects of password stealing attacks. Adversaries steal or compromise passwords and impersonate users' identities to launch malicious attacks, collect sensitive

information, perform unauthorized payment actions, or leak financial secrets. Phishing is the most common and efficient password stealing attack.

2.1 Three Factor Authentication(TFA)

Some researches focus on TFA rather than password-based authentication to provide more reliable user authentication. The TFA takes advantage of a combination of three major factors of authentication which includes verification by something a user knows (such as a password), something the user has (such as a smart card or a security token), and something the user is (such as biometrics).

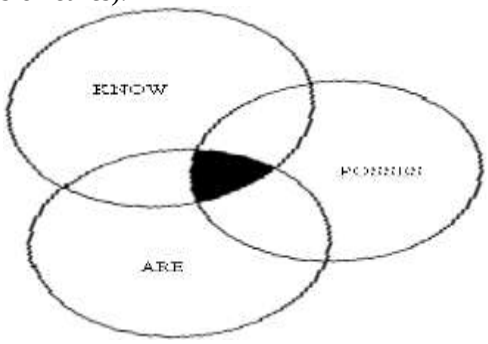

Fig 2:Three Factor Authentication

To pass the authentication, the user must input a password and provide a pass code generated by the token (e.g., RSA SecureID), and scan her biometric features (e.g.,fingerprint). This provides superior security. The major drawback is though it provides high level security, because of its increased complexity and of comparatively high cost, this cannot be adopted in all environments.

2.2 Two Factor Authentication

To resolve this a more attractive and practical approach Two-factor authentication (2FA) is adopted which requires the presentation of two or more of the three authentication factors: a knowledge factor ("something the user knows"), a possession factor ("something the user has"), and an inherence factor ("something the user is").Although there are many banks that support two-factor authentication, it still suffers from the negative influence of human factors, such as the password reuse attack. Users have to memorize another four-digit PIN code to work together with the token, for example RSA SecureID. In this method also to remember the tokens is very difficult.

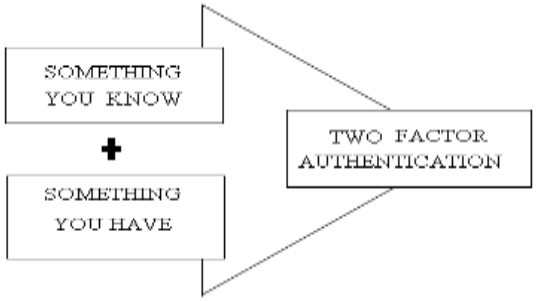

Fig 3: Two Factor Authentication

III.OPASS

A user authentication protocol named oPass which leverages a user's cellphone and short message service (SMS) to prevent password stealing and password reuse attacks. The most difficult is to thwart password reuse attacks from any protection scheme where the users have to bring something for every transaction. The main cause of stealing password attacks is when users type passwords to untrusted public computers.

Therefore, the main concept of oPass is free users from having to remember or type any passwords into conventional computers for authentication. Unlike generic user authentication, oPass involves a new component, the cellphone, which is used to generate one-time passwords and a new communication channel, SMS, which is used to transmit authentication messages to maintain a high level of security.

3.1 Phases In OPASS

The opass prototype is dealing with the following modules which gives the clear cut description :

- Registerring Phase.
- Check Point Phase.
- Entry Phase.
- Application Launching Phase.
- Message Channel.
- Recovery Request Phase.

3.1.1 Registerring Phase

The basic and initial step to be followed is the registration phase. The user initially enters all the required details to be stored in the server database so that whenever the user interacts with the server it is useful to verify and find whether the user is the genuine user. Based upon the preshared secret credential the user is authenticated by the server.

3.1.2 Check Point Phase

The registered details is to be updated at the server database as a unique user account. No two user accounts for the same SIM number cannot be generated. This acts as a main quality of the generated application.

3.1.3 Entry Phase

The login phase begins when the user sends a request to the server through an untrusted browser (on a kiosk). The user is free from entering the password in any browser so that it greatly avoids the man in the middle attacks. The major activity of the login phase is directing the server to identify the user by launching an application in the users cell phone.

3.1.4 Application Launching Phase

When the user sends the request to their favorite server with the help of GSM modem a web service is being send to the users cellphone which automatically triggers the application asking the long term password. This is very helpful to user because they are intimated if any outsiders login without their knowledge.

3.1.5 Message Channel

If the using user is a legitimate user, the application will be asking for the details. Then the user enters ID (account id prefered) and ID (usually the website url or domain name) to the program. The mobile program sends ID and ID to the telecommunication service provider (TSP) through a 3G connection to make a request of registration.

3.1.6 Recovery Request Phase

Recovery phase is introduced for some specific conditions; for example, a user may lose her cell phone. The protocol is able to recover oPass setting on the new cell phone assuming ,still uses the same phone number (apply a new SIM card with old phone number).Once user installs the oPass program on their new cellphone, automatically can launch the program to send a recovery request with their account ID and requested server ID to predefined TSP through a 3G connection.

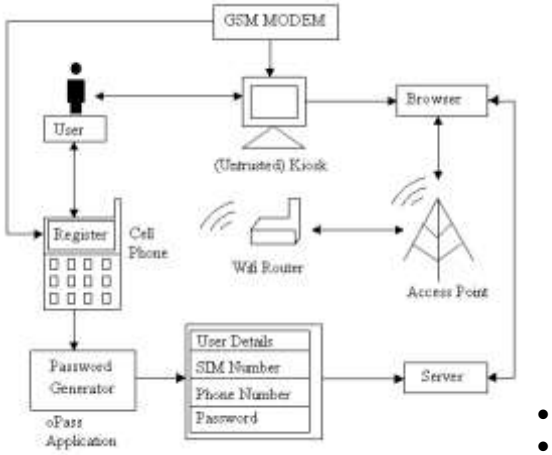

Fig 4: OPASS System Architecture

IV.**Architecture**

The Architecture diagram of oPass system tells that it is used to greatly reduce from malware and phishing. Provides security at local and remote site. And has improved unique identity. The oPass also provides high level security which is at affordable cost. Also the usage of OTP (One Time Password) is valid only for 30sec or to the maximum of1minute.

Therefore hacking of the OTP is useless. Hence the features of adopting the OTP,SMS Channel and 3G Connection are to be given as:

4.1.1 OTP

The one-time passwords in oPass are generated by a secure one-way hash function. With a given input , the set of onetime passwords is established by a hash chain through multiple hashing. Assuming we wish to prepare one-time passwords, the first of these passwords is produced by performing hashes on input

1. The next one-time password is obtained by performing hashes
2. Hence, the general formula is given as follows:
3. For security reasons, we use these one-time passwords in reverse order, i.e., using , then . 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 . Besides, the input is derived from a long-term password , the identity of server ID , and a random seed generated by the server ID
4. Note that function is a hash which is irreversible in general cryptographic assumption. In practice, is realized by SHA-256 in oPass. Therefore, the bit length of is 256.

4.1.2 Message Channel

SMS is a text-based communication service of the telecommunication systems. The oPass leverages SMS to construct a secure user authentication protocol against password stealing attacks. As SMS is a fundamental service of telecom, which belongs to 3GPP standards. SMS represents the most successful data transmission of telecom systems; hence, it is the most widespread mobile service in the world.

SMS network is a closed platform; hence, it increases the difficulty of internal attacks, e.g., tampering and manipulating attacks. Therefore, SMS is an out-of-band channel that protects the exchange of messages between users and servers. Unlike conventional authentication protocols, users securely transfer sensitive messages to servers without relying on untrusted kiosks. oPass resists password stealing attacks since it is based on SMS channels.

.

4.1.3 Connection Through 3G/2G

Both 3G or 2G. connection provides data confidentiality of user data and signal data to prevent eavesdropping attacks. It also provides data integrity of signal data to avoid tampering attacks. The confidentiality and integrity algorithms are f8 and f9, respectively. Algorithm f8 and f9 are based on a block cipher named KASUMI where f8 is a synchronous binary stream cipher and f9 is a MAC algorithm. oPass utilizes the security features of 3G connection to develop the convenient account registration and recovery procedures. Users can securely transmit and receive information to the web site through a 3G connection.

4.1.4 Application Boon

- Confidentiality of information
- Integrity of data
- Reliability
- Authentication
- Independence between each login
- Avoids Man-in-middle attacks

V.Conclusion

The oPass technology described is simple and effective way to keep the plain text passwords out of hands of adversary groups. There is a chance of man-in middle attacks in case of the one time password (OTP) generated by the browser and hence the hackers easily trap them. So oPass application generates the password in the users cellphone and it establishes a direct connection to the server. Also the high sms delay compared to the total execution time is greatly reduced. oPass is a user authentication protocol which is highly secure and efficient compared to the traditional web authentication protocols. For the future work this can be implemented in the banking sectors to maintain a user secure environment, IMEI number and selection of random images on both the side can also be included to maintain the security.

VI. **Reference**

[1] I. Jermyn, A. Mayer, F. Monrose, M. K. Reiter, and A. D. Rubin, "The design and analysis of graphical passwords," in SSYM'99: Proc. 8th Conf. USENIX Security Symp., Berkeley, CA, 1999, pp. 1–1, USENIX Association.

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

[4] D. Florencio and C. Herley, "A large-scale study of web password habits," in WWW '07: Proc. 16th Int. Conf. World Wide Web., New York, 2007, pp. 657–666, ACM.

[5] 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. 662 IEEE TRANSACTIONS ON INFORMATIONFORENSICS AND SECURITY, VOL. 7, NO. 2, APRIL.