Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X

IJCSMC, Vol. 3, Issue. 3, March 2014, pg.976 – 981

RESEARCH ARTICLE

SECURED PASSWORD MANAGEMENT TECHNIQUE USING ONE-TIME PASSWORD PROTOCOL IN SMARTPHONE

R.Selva Bhuvaneshwari[1], P.Anuja[2]

[1]PG Scholar, Embedded system technologies, Regional centre of Anna University, Tirunelveli, India

[2]Lecturer, Department of EEE, Regional centre of Anna University, Tirunelveli, India

[1] bhuvi.indra20@gmail.com , [2] anujap788@gmail.com

Abstract— Graphical passwords and text passwords are most widely used primary user authentication for all websites due to its convenience and simplicity. These kinds of passwords are static in nature and hence it is easy for the attackers to hack using malicious programs and threats. The security drawbacks of the existing methods are phishing, keyloggers, malware, sniffing, spoofing, surfing and guessing. These problems can be overcome by using OTP protocol which is dynamic and also it greatly avoids man-in-the-middle attack, password reuse and password stealing attacks. The proposed method requires a long-term password for login and must be remembered. Finally, OTP is generated using MD5 algorithm. The authentication system is suggested for Android smart phones.

Keywords— One-Time Password (OTP), password stealing, password reuse, authentication

I. INTRODUCTION

Text passwords has been used for user authentication for websites which was traced back before past few decades while registering accounts on a website ,the user enters the username and text password. Once the account is created, he/she has to remember the password for logging into the website. As humans are not experts in memorizing text strings, weak passwords will be selected which leads to brute force and dictionary attacks and another problem is that the same password will be used for more than a website which causes password reuse attack. Another type of authentication is graphical passwords which use images or representation of images as passwords. Human brain is good in remembering picture than textual character. Password guessing resistant protocol is used which provides protection against keyloggers and spyware. The advantage is that for entering graphical passwords, computer mouse is used rather than the keyboard which protects the passwords from keyloggers. Although, graphical password is a great idea, it is not yet mature enough to be widely implemented in practice. Password management tool has also been used which automatically generates the strong passwords for each website, which prevents password reuse and password stealing attacks. The advantage is that the user has to remember the master password to access the management tool. If the user is having trouble in using the tool due to security knowledge which is considered as a drawback. Some researches focus on fourth-factor authentication rather than password-based authentication to provide more reliable user authentication. Three-factor authentication is a comprehensive defense mechanism against password stealing attacks but it requires high cost. Many banks support two-factor authentication but it suffers from password reuse attacks. In this paper, we propose a user authentication protocol which influences a user's cell phone and SMS to prevent password stealing and password reuse attacks. The OTP application was developed using eclipse tool and the android package should be installed in the cell phone which generates the one-time password. Each user simply memorizes the long-term password for access her cell phone. The LTP is used to protect the information on the cell phone from a thief.

II. ONE-TIME PASSWORD PROTOCOL

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

$$\mu_0 = H^N(c) \text{ ……………….(1)}$$

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

$$\mu_1 = H^{N-1}(c) \text{……………….(2)}$$

Hence the general formula is given by,

$$\mu_i = H^{N-i}(c) \text{ ……………….(3)}$$

For security reasons, we use these one-time passwords in shuffled or reverse order i.e., using μ_{N-1}, then μ_{N-2},…, μ_0. If an odd 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 c. Besides, the input c is derived from a LTP (P_u), the identity of server (ID_s), and a random seed (Ø) generated by the server.

$$C = H(P_u \parallel ID_s \parallel \text{Ø}) \text{ ………..(4)}$$

Note that function H is a hash which is irreversible in general cryptographic assumption. In practice, H is realized by SHA-256. Therefore the bit length of C is 256.

III. PROTECTION ASSESSMENT

Protecting user credentials on universal web access Kiosks is important since they are located everywhere, such as airport, lounges, hotel business centre and cafes. All sorts of attacks may happen in such setting including keyloggers, malware, and phishing. Hence we define a threat model of OPASS and demonstrate that it is secure later.

A. Threat model

In our setting, attackers can intercept, eavesdrop and manipulate any message transmitted over the internet and other wireless networks. The attacker can also spoof an SMS to cheat websites. The computer which a user uses to log into websites is considered untrusted. Attackers can install malwares and setup a backdoor to collect a user's sensitive information (e.g., password). The attacker's goal is to masquerade itself as a legitimate user and to gain access to websites without being detected. The methods of gaining access can be classified into two categories based on the attacker's targets which are user and web server.

1)User side:

In this category, the malicious threat is originated from user side. Password stealing is an effective method to complete the attacker's goal. The attacker can launch phishing attacks such as phishing websites and phishing e-mails, to swindle passwords out of users. A user's computer probably installs some malwares (e.g., keylogger and Trojan horses). Furthermore, as we mentioned earlier, users always choose weak passwords which are vulnerable to dictionary attacks. Users also suffer from password reuse attacks. In OPASS the attacker can steal a user's cell phone to log on websites.

2) Server side:

The malicious threat in this category is different from user side. Attackers exploit vulnerabilities of OPASS to pass the authentication without being detected by the websites for e.g., the attackers can intercept and manipulate messages to launch reply and SMS spoofing attacks.

IV. SYSTEM ARCHITECTURE

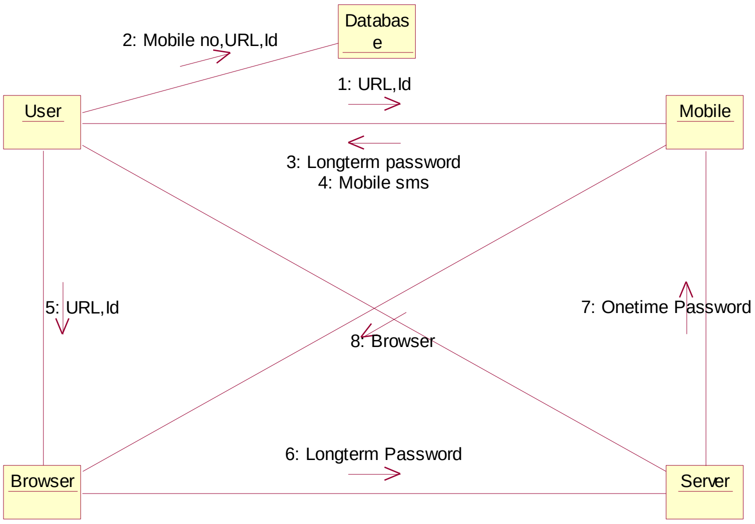

Fig.1 Collaboration diagram of OPASS system

The diagram of the OTP protocol explains that it is used to greatly reduce from malware and phishing attacks. It provides security at local and remote location. And has improved unique identity and level security. The generation of OTP is valid only for 30sec or to the maximum of 1 minute.

B. Phases of OPASS

1. Registration Phase

The basic and initial step to be followed is the registration phase. The user enters all the required details which is stored in the server database. Hence it is used to find whether the user is authenticated.

2. Confirmation Phase

The registration details are to be updated at the server database as a unique user account. It is impossible to generate two user accounts for the same SIM number. This acts as a main quality of the generated application.

3. Login Phase

The login phase begins when the user sends a request to the server through an untrusted browser. The user is free from entering the password in any browser so that it greatly avoids the MITM attack. The major activity of the login phase is directing the server to identify the user by launching an application in the user's cell phone.

4. Recovery phase

Recovery phase is designated for some specific conditions. For e.g., a user may lose her cell phone. The protocol is able to recover the setting on the new cell phone assuming still uses the same SIM number (apply a new SIM card with old phone number). Once the user installs the program on their new cell phone, automatically can launch the program to send a recovery request with their account ID.

5. GSM modem implementation

GSM modem is a specialized type of modem which accepts a SIM card, and operates over a subscription to a mobile operator, just like a cellphone. Importing the common driver and connecting the modem to the PC with serial port. When the user sends the request to the server with the help of GSM modem, a web service is being sent to the users cellphone which automatically triggers the application asking the LTP. This is very helpful to users because they are intimated if any outsiders login without their knowledge.

V. ATTACKS AND REMEDIES

1. Registration

The main task of the registration phase is to generate a shared credential c for computing one-time passwords between users and websites. The shared credential should be kept to guard OPASS from attacks. We also make the assumption that the attacker cannot obtain the LTP(P_u) because it is directly typed into the malware-free cellphone by the user.

2. Attacks and remedies on Login

In the login protocol, the attacker can launch attacks to masquerade itself as a legitimate user without being detected. The attacker has no way of obtaining a one-time password μ_i for login even if she builds a spoof website to launch a phishing attack because the μ_i is treated as a secret key for encryption and is never transmitted. The attacker also cannot recover the μ_i from the encrypted login SMS. Hence phishing attacks do not work under this application. In OPASS , users type their LTP into their cell phones. A kiosks is installed with malwares or keyloggers to steal user passwords is also useless. The application achieves a OTP approach to prevent against password reuse attack. If an attacker steals a user's cellphone and attempts to log into a website that the victim has visited, she will not succeed because she does not know the user's LTP, so she cannot generate a legal OTP for the next round. If an attacker eavesdropped a user's login SMS, she can masquerade the user to deliver the same login messages to the web server. Nevertheless, login will fail, because the stolen login SMS has already been used for login. Even if the attacker interrupts the login procedure after obtaining the login SMS, login will still fail, because the nonce generated by the server does not match.

Another threat is man-in-the-middle (MITM) attack. In order to launch a MITM attack, an attacker must fully control (i.e., interception, eavesdropping and manipulation) all transmission channels. Suppose the attacker launches an MITM attack between the server and browser, the server will detect the MITM attack once it receives a login SMS from the legitimate user. Hence OPASS resists MITM attacks.

3. Attacks and remedies on recovery

Potential threat in the recovery protocol is whether an attacker who stole a user's cellphone can succeed in guessing the correct LTP. This attack is referred to as the password guessing attack. The attacker may try to guess the user's LTP to compute OTP for login. She only has to masquerade as a normal user and execute the recovery procedure. After receiving the message via server, the attacker enters a guessed password and computes a candidate OTP μ_i. The attacker then transmits a login SMS to the server. However, the attacker has no information to confirm whether or not the candidate is correct. Therefore, the protocol prevents a password guessing attack.

VI. CONCLUSION

We have proposed a user authentication technique that can be used to prevent from password stealing and password reuse attacks by installing the applications on the Android smartphone. This system possesses a unique phone number and the user has to remember the LTP that they enter which protects the cellphone. This system also has a recovery procedure when the user loses the cellphone. The proposed system is more efficient since there is independence between each login. We have planned to add-up extra authentication using front camera of the Android smartphone with iris pattern recognition in the future.

REFERENCES

[1] Y.S.Gawand, E.W.Felten, "*Password management strategies for online accounts*", in SOUPS '06:Proc: 2nd symposium.Usable privacy, security, New York, 2006, pp.44-55, ACM.

[2] R.Dhamija, J.D.Tygar, and M.Hearst, "*Why phishing works*", in CHI '06: Proc: SIGCHI conf. Human factors computing systems, New York, 2006, pp. 581-590 ACM.

[3] J.Thorpe and P.Van Oorschot, "*Towards secure design choices for implementing graphical passwords*", presented at the 20th Annu. Computer security applications, conf. 2004.

[4] D.S.Jestel et al. "*survey on awareness and security issues in password management strategies*", IJCSNS, vol.10, no.4, April, 2010.

[5] T.Chippy and R.Nagendran, "*Defenses against large scale online password guessing attacks by using persuasive click points*", IJCAE, vol.03, no.03, Issue:01, March 2012.

[6] J.M.McCune, A.Perrig, and M.K.Reiter. *Seeing-is-believing: Using camera phonea for human-verifiable authentication*. In IEEE symposium on security and privacy, pages 110-124, 2005.

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

[8] S.Chiasson, and 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, NewYork, 2009, pp. 500-511, ACM. 662 IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY, Vol.7, no.2, April.

[9] J.Brainard, A.Juels,R.L. Rivest, M.Szydlo and M.Yung, "*Fourth-Factor Authentication: Somebody You Know*", ACM CCS, 168-78, 2006.