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. 2, Issue. 8, August 2013, pg.174 – 180

RESEARCH ARTICLE

OPass: Attractive Presentation of User Authentication Protocol with Resist to Password Reuse Attacks

S. Megala Devi[1]**, M. Geetha**[2]

[1]Research Scholar, Department Of Computer Science, Vivekanandha College,
Tiruchengode, Tamil Nadu, India

[2]Assistant Professor, Department Of Computer Application, Vivekanandha College,
Tiruchengode, Tamil Nadu, India

[1] *megala8800@gmail.com;* [2] *geethkavi19@gmail.com*

Abstract— ***Passwords are the influential apparatus that tend to keep all data and information digitally safe. It is often notice that text password leftovers mostly popular over the other formats of passwords, due to the information that it is simple and convenient. However, text passwords are not always strong enough and are very easily stolen and changed under different vulnerabilities. Others can acquire a text password when a person creates a weak password or a password that is completely reused in many sites. In this condition if one password is stolen, it can be used for all the websites. This is called as the Domino Effect. Another risky environment is when a person enters his/her password in a computer that is not trust-worthy; the password is prone to stealing attacks such as phishing, malware and key loggers etc. In this paper, a user authentication protocol named Password is designed, that makes use of the customer's cellular phone and short message service to ensure protection against password stealing attacks. Password requires a unique phone number that will be possessed by each participating website. The registration and the recovery phases involve a telecommunication service provider. The main concept of the project is reducing the password reuse attack. We have implemented the one time password technology, and then reduce the password validity time. The performance had improved the security.***

Key Terms: - Encryption; Hash Function; Network Security; One-Time Password; Password Reuse Attack; Password Stealing Attack; User Authentication

I. INTRODUCTION

In order to log into the website successfully, users must recall these passwords. Generally, password based user authentication can resist brute-force and dictionary at-tacks if users select strong passwords. However, password-based user authentication has a major problem that humans are not experts in memorizing text strings. Thus, most users would choose easy-to-remember passwords (i.e., weak passwords) even if they know those 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.

Researchers have investigated a variety of technology to re-duce the negative influence of human factors in the user authentication procedure. Since humans are more adept in remembering graphical passwords than text passwords many graphical pass-word schemes were designed to address human's password re-call problem. Using password management tools is an alternative. These tools automatically generate strong passwords for each website, which addresses password reuse and password re-call 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 at-tack. Many previous studies have proposed schemes to defend against password stealing attacks.

Some researches focus on three-factor authentication rather than password-based authentication to provide more reliable user authentication. Three-factor authentication depends on what you know (e.g., password), what you have (e.g., token), and who you are (e.g., biometric). To pass the authentication, the user must input a password and provide a pass code generated by the, and scan her biometric features (e.g., finger-print or pupil). Three-factor authentication is a comprehensive defense mechanism against password stealing attacks, but it requires comparative high cost.

Thus, two-factor authentication is more attractive and practical than three-factor authentication. Although many banks 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.

A user authentication protocol named Procure pass which leverages a user's cellphone and short message service (SMS) to prevent password stealing and password reuse attacks. It is difficult to thwart password reuse attacks from any scheme where the users have to remember something. The main cause of stealing password attacks is when users type passwords to un-trusted public computers.

Therefore, the main concept of Procure pass is free users from having to remember or type any passwords into conventional computers for authentication. Unlike generic user authentication, procure pass involves a new component, the cell phone, which is used to generate one-time passwords and a new communication channel, SMS, which is used to transmit authentication messages.

II. RELATED WORK

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. Generally, password-based user authentication can resist brute force and dictionary attacks if users select strong passwords to provide sufficient entropy. However, password-based user authentication has a major problem that humans are not experts in memorizing text strings. 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 [1], [2]. In 2007, Florencio and Herley [3] indicated that a user reuses a password across 3.9 different websites on average. 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. Up to now, researchers have investigated a variety of technology to reduce the negative influence of human factors in the user authentication procedure. Since humans are more adept in remembering graphical passwords than text passwords [4], many graphical password schemes were designed to address human's password recall problem [5]–[9]. Using password management tools is an alternative [10]–[12]. 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 [13], [14] and is still vulnerable to several attacks [15]–[17]. 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 [18]–[20]. Phishing is the most common and efficient password stealing attack. According to APWG's report, the number of unique phishing websites detected at the second season of 2010 [(Q2, 2010)] is 97 388. Many previous studies have proposed schemes to defend against password stealing attacks. Some researches focus on three-factor authentication rather than password-based authentication to provide more reliable user authentication.

Three-factor authentication depends on what you know (e.g., password), what you have (e.g., token), and who you are (e.g., biometric). 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 or pupil).Three-factor authentication is a comprehensive defense mechanism against password stealing attacks, but it requires comparative high cost. Thus, two-factor authentication is more attractive and practical than three-factor authentication. Although many banks thus, two-factor authentication is more attractive and practical than three-factor authentication. Although many banks 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 addition, users easily forget to bring the token. In this paper, we propose 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. In our opinion, it is difficult to thwart password reuse attacks from any scheme where the users have to remember something. We also state that 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 cell phone, which is used to generate one-time passwords and a new communication channel, SMS, which is used to transmit authentication messages.

III. FURTHER DISCUSSION

A. *Issues of Phone Number Authenticity*

Phone number is a critical factor of oPass since we adopt the SMS channel for message exchanging. The potential issue is how users ensure that the phone number received is actually from the desired website rather than a forged phishing website. To address this difficulty, registration and recovery phases involve a telecommunication service provider (TSP). We assume that TSP provides a service (e.g., cell phone application) to support registration and recovery procedures of oPass. Users input the identity of the desired websites to the TSP's service. TSP will establish an SSL tunnel with the website before forwarding messages sent from users to it. Based on the SSL protocol, TSP can verify the website's certificate to prevent phishing attacks. Therefore, we can ensure that the phone number is actually from the correct website rather than phishing websites. In addition, the SSL tunnel provides data confidentiality. The communication interface between cell phone and TSP is 3G. 3G provides data confidentiality to protect the messages exchange. Hence, the secret key can be securely distributed by the TSP to both the cell phone and the server for registration use. A malicious user cannot decrypt other users' registration SMS unless he compromised there. This mechanism guards against insider attacks. Another potential issue about the phone number is that websites may change their telecom service provider.

B. *One-Time Password Refreshment*

The hash chain of a one-time password will be consumed entirely. We introduce parameter to solve this problem. The server checks the status of hash chain after receiving a legal login SMS. If the rest of the one-time passwords are less than , the server sends a new seed to the cell phone at Steps 6) and 7) of the login procedure Once the cell phone gets the new seed, it computes a new credential and sends it to the server through the SMS channel. Hence, the user and the server will use the new hash chain for the next login. This facility can be automatically completed without user effort.

C. *Resistance to Phishing Attacks*

Although we setup a reasonable assumption: user cell phones should be malware-free, the long-term password still suffers from phishing attack by means of a browser in the cell phone. Via social engineering, the user might input his long-term password into a malicious web site through the cell phone's browser. Even though an attacker can obtain, oPass is still secure since the attacker has no enough information to recompute the credential. Message is only transmitted by the server in the registration and recovery phases; most important of all, the transmission through SSL tunnel and 3G connection ensures data confidentiality and privacy.

D. *Password Reuse*

Password reuse is a serious problem in the present user authentication systems. To repair this problem, oPass adopts an OTP approach. Even if the long-term password is used for every account, the OTP approach still ensures that all logins are independent. Based on the design, is one of inputs to compute the credential. Ideally, different web servers randomize different to compute distinct. Then distinct derives distinct OTP sequence for login. Therefore, oPass users do not reuse same passwords for different accounts since generated OTP sequences guarantee randomness for each login. 5) Weak Password: Regarding the weak password problem, users tend to pick weak passwords because the passwords are easy to remember. In oPass system, a user just remembers a long-term password for all accounts. Unfortunately, user behavior is not easy to change. To help users, oPass adopts a checker to evaluate the security strength of passwords in the registration phase. If the selected password cannot satisfy the preferred security, oPass would suggest a random strong password or allow the users picking a new one again.

IV. Performance Analysis

The analysis is conducted in order to identify the effectiveness of SCTPOpass.20 persons are selected and asked to work on the application and the time required to send the SMS during the registration and login phase is noted.

Table I Performance Analysis Of Registration Process

Registration Process	SMS Delay	Total
OPass	9.1	21.8
SCTPOpass	8.3	20.1

Table II .Performance Analysis Of Login Process

Login Process	SMS Delay	Total
OPass	8.9	21.6
SCTPOpass	8.2	19.9

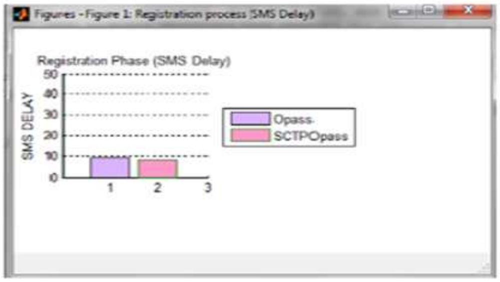

Fig.6. SMS Delay Of Registration Process

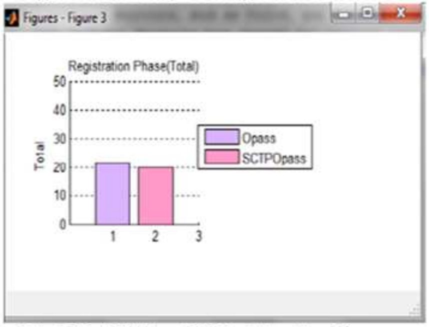

Fig.7.Total Time Of Registration Process

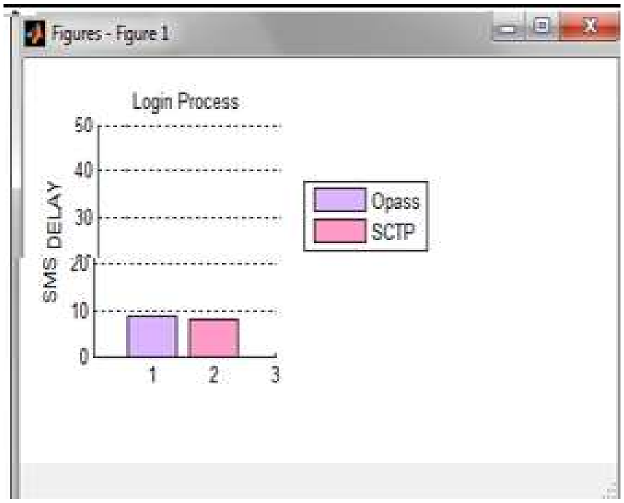

Fig.8. SMS delay of login process

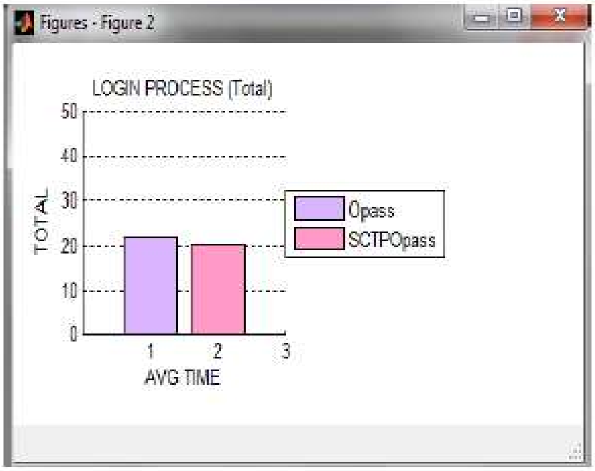

Fig.9.Total Time of Login Process

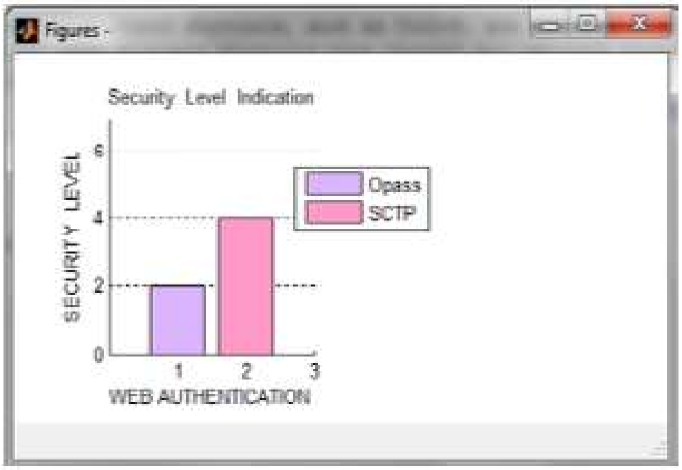

Fig.10.Security Level Indication.

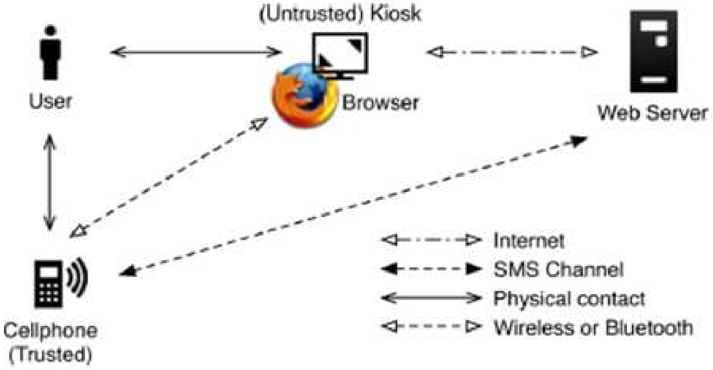

Fig. 1. Architecture of oPass system.

V. CONCLUSION

A user authentication protocol named oPass which leverages cell phone and SMS to thwart password stealing and password reuse attacks. OPass assume that each website possesses a unique phone number. It also assume that a telecommunication service provider participants in the registration and recovery phases. The design principle of oPass is to eliminate the negative influence of human factors as much as possible. Through oPass, each user only needs to remember a long-term password which has been used to protect their cell phone. Users are free from typing any passwords into untrusted computers for login on all websites. OPass is efficient for website authentication to prevent phasing, key logger and malware. SMS delay could increase the execution time and reduce the performance. The performance of oPass can be improved by Round Robin DNS with the help of simultaneous response from the server for multiple users at a time. Internet relay chat protocol can be used for synchronous conferencing of SMS service. There by communication overhead can be reduced because of many transactions.

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 York, 2007, pp. 657–666, ACM.

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

[6] A. Perrig and D. Song, “Hash visualization: A new technique to improve real-world security,” in Proc. Int.Workshop Cryptographic Techniques E-Commerce, Citeseer, 1999, pp. 131–138.

[7] J. Thorpe and P. van Oorschot, “Towards secure design choices for implementing graphical passwords,” presented at the 20th. Annu. Computer Security Applicat. Conf., 2004.

[8] 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.

[9] 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.

[10] 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.

[11] J. A. Halderman, B. Waters, and E. W. Felten, “A convenient method for securely managing passwords,” in WWW ’05: Proc. 14th Int. Conf World Wide Web, New York, 2005, pp. 471–479, ACM.

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

[13] S. Chiasson, R. Biddle, and P. C. van Oorschot, “A second look at the usability of click-based graphical passwords,” in SOUPS ’07: Proc. 3rd Symp. Usable Privacy Security, New York, 2007, pp. 1–12, ACM.

[14] 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.

[15] J. Thorpe and P. C. van Oorschot, “Graphical dictionaries and thememorable space of graphical passwords,” in SSYM’04: Proc. 13th Conf. USENIX Security Symp., Berkeley, CA, 2004, pp. 10–10, USENIX Association.

[16] J. Thorpe and P. C. van Oorschot, “Human-seeded attacks and exploiting hot-spots in graphical passwords,” in SS’07: Proc. 16th USENIX Security Symp. USENIX Security, Berkeley, CA, 2007, pp. 1–16, USENIX Association.

[17] 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.

[18] 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.

[19] C.Karlof,U. Shankar, J. D.Tygar, andD.Wagner, “Dynamic pharming attacks and locked same-origin policies for web browsers,” in CCS ’07: Proc. 14th ACMConf. Computer Communications Security, NewYork, 2007, pp. 58–71, ACM.