M-Pass: Web Authentication Protocol Resistant to Malware and Phishing

Ajinkya S. Yadav
M.E.student, Department of Computer Engineering.
Pune University, Pune

A. K .Gupta
Professor, Department of Computer Engineering
Pune University, Pune.

ABSTRACT
In this digital world all information and data is kept safe by passwords. The simple and convenient format of password is in the form of text. But, text passwords are not always strong enough and under different vulnerabilities they are very easily stolen and changed. When a person creates a weak password or same password is reused in many sites it may be possible that others can acquire that password. If one password is stolen, then it is possible that it can be used for all the websites. This phenomenon is known as the Domino Effect. Another possible risky attacks are related to phishing, malware and key loggers etc. A protocol is designed which makes use of the user's customer's mobile i.e. cellular phone and SMS (short message service) to ensure protection against password stealing attacks. This user authentication protocol is named as m-Pass. The unique phone number is required which will be possessed by each participating website. The telecommunication service provider plays important role in the registration and the recovery phases. The main theme is to reduce the password reuse attack. It works with one time password technology, and results in reduction of the password validity time. The results show improvement in performance of the security**.**

Keywords
Network Security, m-Pass, Phishing, authentication

1. INTRODUCTION
Internet and network services play vital role in today's digital world. The various web services are like online banking, social networks, cloud computing. For the security and authentication purpose of user needs a password. Mostly text based password is used. While registering accounts on a website, user selects his username and text password. In order to log into the website successfully, user must recall the selected passwords. To provide sufficient entropy, if users select strong passwords, then user authentication based on password can resist attacks like brute force attack and dictionary attack. However, a major problem is, password based user authentication involves humans and they are not experts in memorizing text strings. So the weak passwords (i.e. easy-to-remember passwords) would be chosen by most users even if they know the passwords might be unsafe. It is found that, the users tend to reuse passwords across various websites. This is another crucial problem. Reuse of Password causes users to lose sensitive information stored in different websites, if a hacker compromises one of their passwords. This attack is said to be the password reuse attack. Such problems are caused by the negative influence of the human factors. The various technologies are invented to reduce the negative impact of the human factors in the user authentication procedure. Since humans have adept nature in remembering graphical passwords than text passwords, there were many techniques related to graphical password designed to notify human's problem of password recalling [6]. Making use of password management tools is an alternative approach. These tools can be used to automatically generation of the strong passwords for each website. It points out problems of password reuse and password recall problems. Due to this, users have to remember only one master password to access the management tool; this is an advantage [2].The another attack is related to the password stealing. Adversaries steal or compromise passwords. They may impersonate users' identities to collect sensitive information, to launch malicious attacks, perform unauthorized payment actions and they may leak financial secrets. The most common and efficient password stealing attack is Phishing. Some researches focus on three-factor authentication rather than password-based authentication to provide more reliable user authentication. The previously three-factor authentication system depends on what user knows i.e. password, what user have i.e., token, and who user is i.e., biometric). To pass on the authentication function, the user must have to input a password and provide a pass code generated by the token (e.g., RSA), and scan his biometric features (e.g., fingerprint or pupil). Three-factor authentication is a comprehensive defense mechanism against the attacks like password stealing, however it requires comparative high cost. Compared to three-factor authentication, two-factor authentication is more attractive and practical. Although two-factor authentication is supported by many banks, it still suffers from the bad influence of human factors, like the password reuse attack. Another factor is, users have to memorize another four-digit PIN code to work together with the token, for example RSA Secure ID. The proposed system gives a web authentication protocol (m-Pass) which combines the user's cell phone and short message service (SMS) to prevent the password reuse and password stealing attacks. The proposed system state that the main cause of stealing password attacks is when users type passwords to untrusted public computers. The main concept of m-Pass is to free users from having to remember or type any passwords into conventional computers for authentication. The authentication system i.e. M-Pass involves a new instrument, i.e. the cell phone, which is used to generate one-time passwords. It has a new communication channel, i.e. SMS, which is used to transmit authentication messages. m-Pass presents the following advantages.

1) Anti-malware—Malware (e.g., key logger) gathers sensitive information from users, like their password [1]. In m-Pass, users are able to log into web services without entering passwords on their computers. Due to this change, malware is not able to obtain a user's information like password from untrusted computers.

2) Phishing Protection— Phishing attacks are launched by adversaries to steal users' passwords by cheating users when they connect to forged websites. M-Pass successfully allows users to log into the websites without disclosing or revealing passwords to computers. Users who adopt m-Pass are guaranteed to prevention of phishing attacks.

3) Password Reuse Prevention and Weak Password Avoidance— m-Pass achieves one-time password approach. For

each login, the cell phone automatically derives different passwords; i.e. the password is different during each login [3]. In this approach, users do not need to remember any password for login. They only keep a long term password for accessing their cell phones, and leave the rest of the work to m-Pass.

4) Cell phone Protection—An adversary can breach user authentication by stealing user's cell phones. However, the cell phones are protected by a long-term password. The adversary cannot impersonate a legal user to login without being detected.

2. LITERATURE SURVEY

The previous studies shows how different researchers made work on have to protect user secret information or credentials from phishing attacks in user authentication. The proposed systems leverage variable technologies, for example, mobile devices,including the trusted platform module (TPM), or public key infrastructure (PKI). However, these solutions were short of considering the human's bad influence, such as password reuse and weak password problems. A well-known approach is MP-Auth protocol presented by Mannan and Oorschot in 2007 [9]. To strengthen password-based authentication in untrusted environments, MP-Auth forces the input of a long-term secret (mostly a user's text password) through a trusted mobile device [1]. Before sending the password to an untrusted kiosk, the password is encrypted by the already installed public key on a remote server. MP-Auth is intended to guard passwords from attacks raised by untrusted kiosks, which may include key loggers and malware. In spite of that, MP-Auth suffers from password reuse vulnerability. An attacker can compromise a weak server, e.g., a server without security features, to obtain a user's information and exploit it to gain his access rights of different websites. On another side, MP-Auth assumes that password and account system setup is secure. Then it is necessary that users should setup an account and password via physical contact, like banks which are requiring users to initialize their account personally or send passwords though postal service. In m-Pass, it addresses above weakness and removes this assumption. M-Pass system attains one-time password approach to diminish the password reuse problem, and involves a TSP to ensure that the registration and recovery phase is secure. Parno utilized mobile devices i.e. cellphones as an authentication tokens to build an anti-phishing mechanism, named as Phoolproof, between mutual authentication between users and websites. While logging on to the website, a user should provide the issued public key and username/password combination. But previous study shown that Phoolproof is still vulnerable to the problems like password reuse. It needs physical contacts to ensure that account setup is secure. On the contrary, some research represents different approaches to prevent phishing attacks. Session Magnifier enables the browser on a mobile device which is extended and a regular browser on a public computer. It creates collaboratively a secure web session. User access to sensitive interactions is separated by Session magnifier from regular interactions. For important communication, the content is sent to the extended browser on the user's mobile device for further confirmation from a user. Another avenue is adopting TPM. The author [4] designed a bump in the ether (BitE) based on TPM. Via BitE, user inputs are protected under an encrypted tunnel. This tunnel is in between the mobile device and on a TPM-equipped untrusted computer where the application running . Many of recent systems require involvement of users in certificate confirmation (UICC) in order to setup a secure SSL tunnel.

3. PROPOSED SYSTEM

The proposed user authentication system, called as m-Pass, to thwart the attacks like Phishing, Malware etc. The goal of m-Pass is to prevent users from typing their memorized passwords into kiosks. By using one-time passwords, which reflects that password information is no longer important. When the user completes the current session, the one-time password is expired. Instead of using Internet channels, m-Pass leverages SMS and user's cell phones to avoid password stealing attacks. Compared to internet channels, it believes SMS is a suitable and secure medium between cell phones and websites to transmit important information. Based on SMS, a user identity on untrusted kiosk is authenticated by websites without inputting any passwords. Use of the password is only to restrict access on the user's cell phone. In m-Pass, each user needs to simply memorize a long-term password for access his cell phone. The long-term password is used to protect the information on the cell phone from a thief.

Figure 1 describes the architecture (and environment) of the m-Pass system. To perform secure login on an untrusted computer (kiosk), m-Pass consists of a trusted cell phone, a browser on the kiosk, and a web server that users wish to access. To accomplish secure logins to the web server, the user operates his cell phone and the untrusted computer directly. The communication is possible through the SMS channel. The web browser interacts with the web server via the Internet. In our protocol design, it requires the cell phone interact directly with the kiosk. The basic way is to select available interfaces on the cell phone, SMS.

The system has following phases; Registration Phase, Login Phase and Recovery Phase.

3.1 Registration Phase

In this phase, the user and a server negotiate a shared secret to authenticate succeeding logins for this user. The m-pass program installed on his cell phone is opened by the user. The user enters ID_u (account id she prefers) and IDs to the program. The mobile program sends ID_u and ID_s to the telecommunication service provider (TSP). This is done through a 3G connection which makes a request of registration. Once the TSP received the ID_u and the IDs, it can trace the user's phone number T_u based on SIM card used by user. After that TSP is used to distribute a shared key K_{sd} which plays the role of third-party between the user and the server. To encrypt the registration SMS with AES-CBC, the shared key is used. To protect the communication, the TSP and the server S will establish an SSL tunnel. Then the TSP forwards ID_u, K_{sd}, T_u , and to the assigned server S. Server will generate the corresponding information for this account a response, including server's identity IDs , a random seed ø, and server's phone number T_s . The TSP then forwards ID_s , ø ,Ts , and a shared key K_{sd} to the user's cell phone. After reception of the response is finished, the user continues to setup a long-term password P_u with his cell phone.

Table 1. Comparison of M-Pass with previous techniques

	Attack Prevention			Requirements				
	Phishing	Key logger	Password reuse	UICC	Physical account setup	Logical account setup	On-device secret	Malware free mobile
m-pass	●	●	●			●		●
MP-Auth	●	●		●	●			●
Phoolproof	●	●		●	●		●	●
Session magnifier		●					●	●
BitE		●					●	●

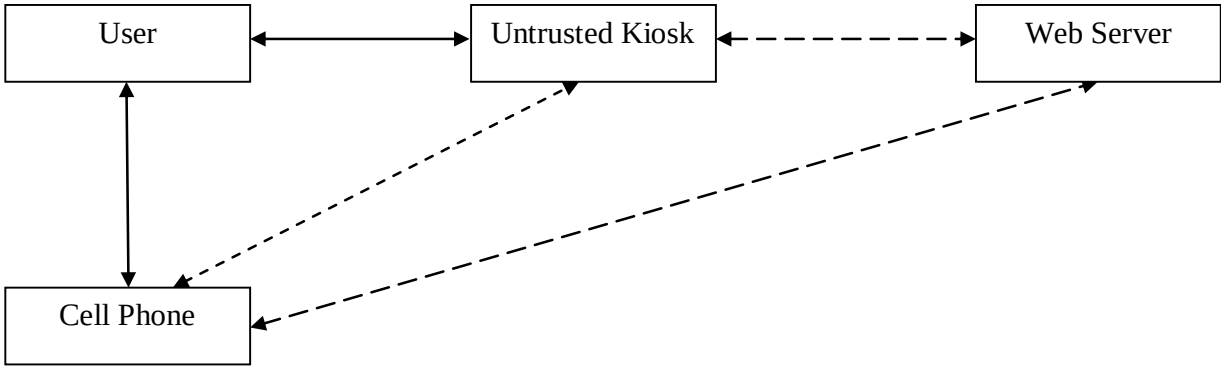

Fig.1. Architecture of m-Pass system

The cell phone computes a secret credential C by the following operation:

$$C= H(P_u \| ID_s \| ø).$$

3.2 Login Phase

The login begins when the user u sends a request to the server S through an untrusted browser (on a kiosk). The user uses his cell phone to produce a one-time password, e.g., δi. Then delivers necessary information encrypted with δi to server S via an SMS message. Server S can verify and authenticate user u based on δi, based on pre shared secret credential C, The protocol is started when the user u wishes to log into his already registered favourite web server S. However, user u begins with the login procedure by accessing the specific website via a browser on an untrusted kiosk. Then the browser sends a request to S with u's account ID_u. Next, server S supplies the IDs and fresh nonce ns to the browser. Meanwhile, this message is forwarded to the cell phone through SMS or wireless interfaces.

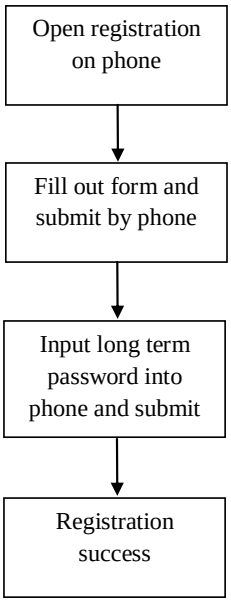

Fig.2. Registration phase

After receiving the message, the cell phone inquires related information from its database via IDs, which includes server's phone number and other parameters. The next step is promoting a dialog for the long-term password. Secret shared

information can regenerate by providing the correct on the cell phone. The OTP i.e. one-time password for current login is recomputed using the following operations:

$$C= H(P_u \| ID_s \| ø).$$

$$\delta i= H^{n-i}(c).$$

3.3 Recovery Phase

The recovery phase is designated for some specific conditions; for example, a user u may lose his cell phone. The protocol is able to recover m-Pass setting on his new cell phone assuming he still uses the same phone number (apply a new SIM card with old phone number). After the user u installs the m-Pass program on his new cell phone, he can launch the program to send a recovery request with his account ID_s and requested server ID_s through the 3G connection is to predefined TSP.

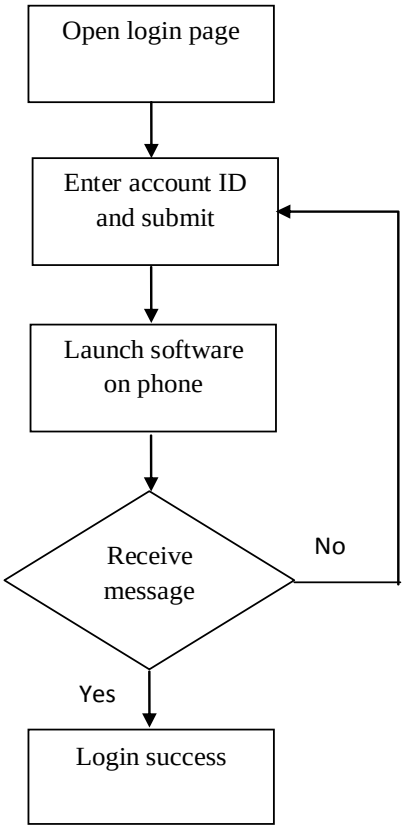

Fig.3. Login phase

As mentioned before, ID_s can be the domain name or URL link of server. Similar to registration, TSP can trace his phone number T_u based on his SIM card and forward his account ID_s and the T_u to server through an SSL tunnel. Once server S receives the request, S probes the account information in its database to confirm if account u is registered or not. If account ID_u exists, the information used to compute the secret credential c will be fetched and be sent back to the user. The server S generates a fresh nonce n_s and replies a message which consists of ID_s, ø , T_s , i , and S . The message includes all important fieldss for generating the next one-time passwords to the user u. When the mobile program receives the message, like registration, to reproduce the correct one-time password δi_{+1}, it forces the user u to enter his long-term password [7]. During the final step, the user's cell phone encrypts the secret credential c and server nonce n_s to a cipher text. The recovery SMS message is delivered back to the server S for checking. Similarly, the server S computes δi_{+1} and decrypts this message to ensure that user u is already recovered. At this point, his new cell phone is recovered and ready to perform further logins in the system. Continuing for the next login, one-time password is used for the user authentication.

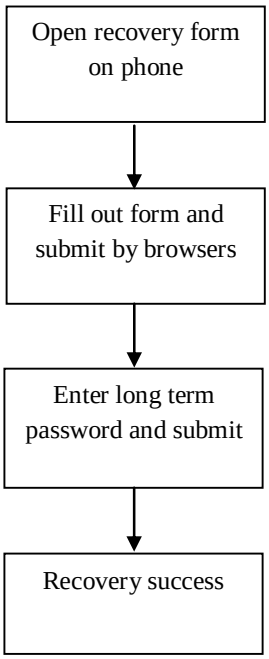

Fig.4. Recovery phase

4. RESULTS

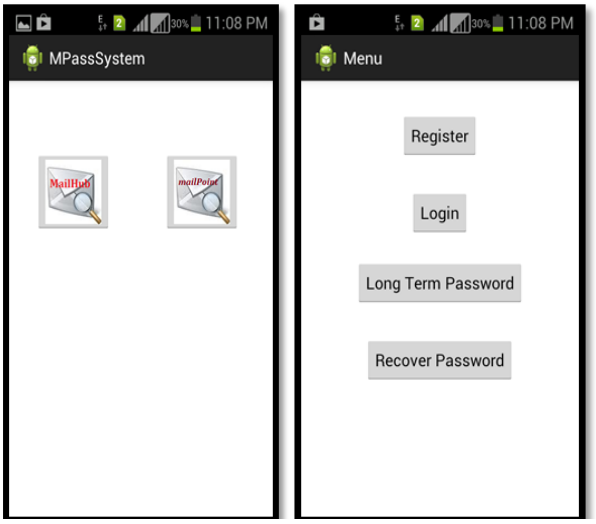

Fig.5. Results

As shown in Fig.5, the proposed system of m-Pass is implemented. In the system, the Registration and Login phase have been shown which guides to user for the authentication service protocol which creates OTP i.e. One Time Password.

6. CONCLUSION

A user authentication protocol i.e. m-Pass leverages cell phones and SMS to prevent password stealing and password reuse attacks. The assumption it makes is that each website possesses a unique phone number. The important principle of the proposed system i.e. m-Pass is to eliminate the negative influence of human factors as much as possible. Because of m-Pass, each user only needs to memorize the long-term password which has been used to protect his cell phone. Users are free from typing any passwords into untrusted computers for the sake of login on all websites. Compared with previous schemes, m-Pass is the first user authentication protocol to prevent password stealing and password reuse attacks simultaneously. The reason is that the m-Pass adopts the one-time password way to ensure independence between each and every login. Password recovery is also considered to make m-Pass fully functional. When users lose their cell phones password recovery plays it's role.

7. ACKNOWLEDGEMENT

It is a pleasure for me to thank many people who in different ways have supported and guided me. I would like to thank my Guide, Prof. A. K. Gupta; PG coordinator, Prof. M. D. Ingle, all my teachers, Principal Dr. M. G. Jadhav. I would also like to express my gratitude to all my colleagues for their support, co-operation, my family and friends for their sincere interest in my study and their moral support.

8. REFERENCES

[1] Hung-Min Sun, Yao-Hsin Chen, and Yue-Hsin Lin "oPass: A User Authentication Protocol Resistant to Password Stealing and Password Reuse Attack", in *IEEE Transaction Vol 7, No.2, April 2012.*

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

[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

[6] 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.

[7] 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..

[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] Mohammad Mannan, University of Toronto, Canada, and P.C. van Oorschot, Carleton University, Canada "Leveraging Personal Devices for Stronger Password Authentication from Untrusted Computers"

[10] 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.