International Journal of Engineering Research and Development
e-ISSN: 2278-067X, p-ISSN: 2278-800X, www.ijerd.com
Volume 11, Issue 05 (May 2015), PP.24-28

M-Pass: Web Authentication Protocol

Ajinkya S Yadav[1], Prof.A.K.Gupta[2]
[1]*JSPM's, JSCOE Hadpasar, pune.*
[2]*JSPM's, JSCOE Hadpasar, pune.*

Abstract:- The password plays an important role for user authentication on computers. However, as users are required to remember more, longer, and changing passwords, it is evident that a more convenient and secure solution to user authentication is necessary. That system examines passwords, security tokens and biometrics-collectively calls authenticators-and compares these authenticators and their combinations. The design of a system in which a user's mobile device serves as a vehicle for establishing trust in a public computing kiosk by verifying the integrity of all software loaded on that kiosk. This procedure leverages several emerging security technologies, namely the Trusted Plat form Module, the Integrity Measurement Architecture, and new x86 support for establishing a dynamic root of trust. That system balances the desire of the user to maintain data confidentiality against the desire of the kiosk owner to prevent misuse of the kiosk.

Keywords:- Network Security, m-Pass, Phishing, authentication.

I. INTRODUCTION

Today's world rely on the internet and network services for using the various web services such as online banking, social networks, cloud computing. And for the security and authentication of user a text based password is primarily used. People select their username and text passwords when registering accounts on a website. In order to log into the website successfully, user must recall the selected passwords. 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. 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. Those problems caused by the negative influence of human factors.

The various technologies are invented 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, many graphical password schemes were designed to address human's password recall problem. An alternative approach is to use the password management tools. 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.

The password stealing attack is also creates the problem. 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. According to apwg's report the number of unique phishing websites detected at the second season of 2010 is 97 388.

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), 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 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 secure id. In addition, users easily forget to bring the token.

II. BACKGROUND

Mostly in today's Internet technology world the password are very important for using the latest web services hence the authentication is needed so the users are required to remember more, longer, and changing passwords, it is evident that a more convenient and secure solution to user authentication is necessary. That system examines passwords, security tokens and biometrics-collectively calls authenticators-and compares these authenticators and their combinations. Lawrence O'Gorman [8] examined their effectiveness against several attacks and suitability for particular security specifications such as compromise detection and nonrepudiation. Examples of authenticator combinations and protocols are described to show tradeoffs and solutions that meet chosen, practical requirements.

Many users fail to take adequate steps to protect their passwords. Often the cause is not a failure to understand that strong passwords are important, but rather frustration with the difficulty of doing the right thing. In the study J. Alex Halderman, Brent Waters, Edward W. Feltenwe [7] attempted to make strong password management more convenient. Whereas previous schemes were lacking in either transportability for mobile users or security against brute force attacks, our design achieves a balance of the two by using password strengthening techniques.

The findings by Shirley Gaw, Edward W. Felten [2] also indicated that the nature of online accounts and tools for managing passwords in online accounts enable poor password practices rather than discourage them. There is a gap between how technology could help and what it currently provides. Furthermore, they demonstrated that password reuse is likely to become more problematic over time as people accumulate more accounts and having more accounts implies more password reuse.

The data allows us to measure for the first time average password habits for a large population of web users. Many facts previously suspected, can be confirmed using large scale measurements rather than anecdotal experience or relatively small user surveys. Dinei Florencio and Cormac Herley studied and found [3] particularly confirm the conventional wisdom about the large number and poor quality of user passwords. In addition passwords are reused and forgotten a great deal. This allows estimating the number of accounts that users maintain the number of passwords they type per day, and the percent of phishing victims in the overall population.

The design of a system [7] in which a user's mobile device serves as a vehicle for establishing trust in a public computing kiosk by verifying the integrity of all software loaded on that kiosk. This procedure leverages several emerging security technologies, namely the Trusted Plat form Module, the Integrity Measurement Architecture, and new x86 support for establishing a dynamic root of trust. That system balances the desire of the user to maintain data confidentiality against the desire of the kiosk owner to prevent misuse of the kiosk. Scott Garriss, Ramon Caceres, Stefan Berger have demonstrated [7] the viability of the approach by implementing our system on commodity hardware. The delay incurred by the trust establishment protocol in the prototype is close enough to the range of delays reported as tolerable by users that are moderate engineering effort would result in a useable system. However, work is generally applicable to establishing trust on public computing devices before revealing any sensitive information to those devices.

III. 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 user's cell phones to avoid password stealing attacks. Compared to internet channels, it believes secure medium between cell phones and websites to transmit important information. 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 simplymemorize 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. To provide the authentication, user has to follow the steps of execution of the system, he needs to register himself on the website with unique credentials and set the long term password. After that user needs to login on to the website by using any browser providing only username not a password after submitting it user must provide his/her long term password from registered mobile. Server receives these credentials and validates all. If all credentials are get validated the user redirected to his/her webpage.

- **Registration Phase**

For registration it requires the users account ID (IDu) , the mobile no and the address of the web service which user wants to use (IDs). The mobile program sends IDu and IDs to the server Once the server received the IDu and the IDs, it can trace the user's phone number Tu.. After that server is used to distribute a

shared key Ksd which plays the role of third-party between the user and the server. To encrypt the password Pu with his cell phone.

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

$$C= H(Pu \| IDs \| ø).$$

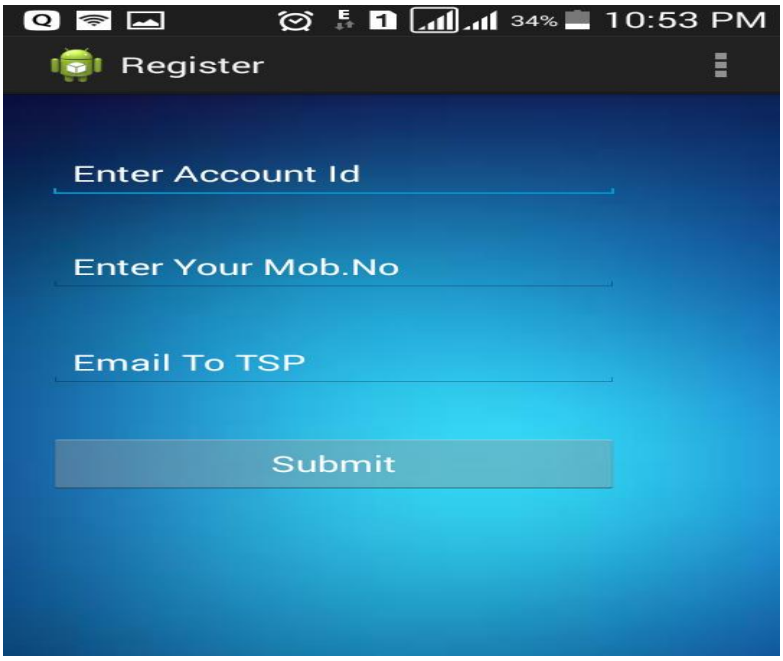

Fig.2. Registration phase

- **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 provide a long term password. 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. The verified users redirected to the home page automatically.
The password for current login is recomputed using the following operations:

$$C= H(Pu \| IDs \| ø).$$
$$δi= Hn-i(c).$$

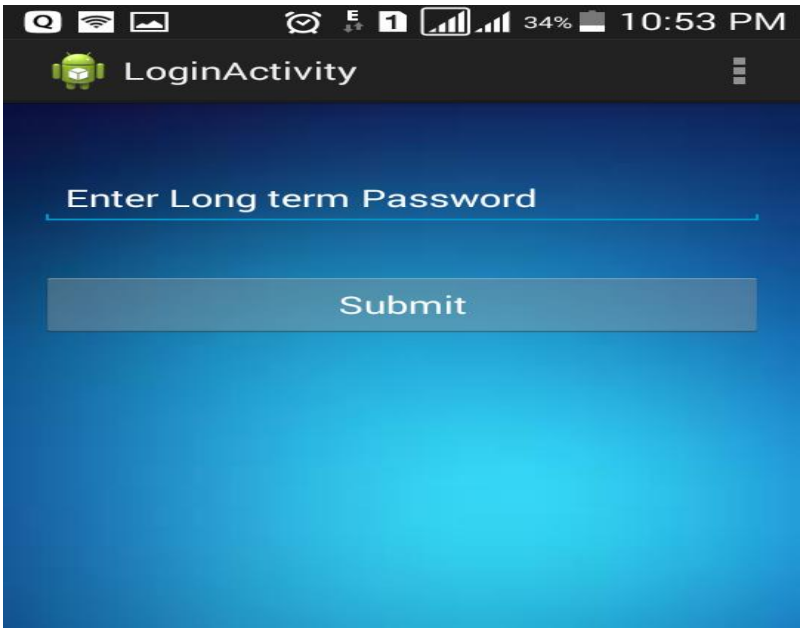

Fig.3. Login phase

- **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 IDs and requested server. As mentioned before, IDs can be the domain name or URL link of server. Similar to registration, TSP can trace his phone number Tu based on his SIM card and forward his account IDs and the Tu 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 IDu exists, the information used to compute the secret credential c will be fetched and be sent back to the user.

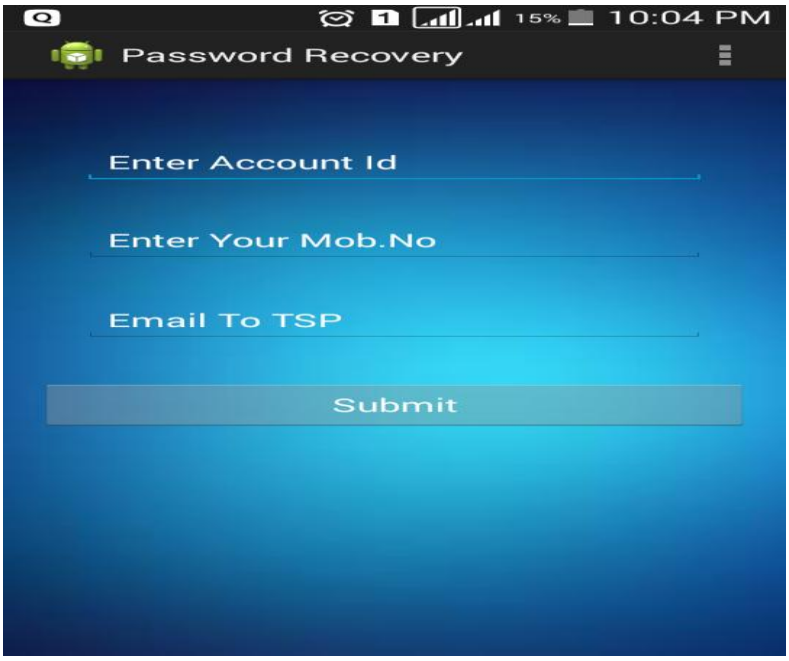

Fig.4. Recovery phase

IV. RESULTS

The following table shows the time required for registration and login phase

	Registration Time in Min	**Login Time in Min**
Avg time	4.1	3.5
Min, max	(3,6)	(3,7)

V. CONCLUSIONS

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.

ACKNOWLEDGMENT

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.

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.