Secure Login for Websites: A User Authentication Protocol to Resist Password Stealing and Reuse Attacks

Rashmi S Suvarna
Department of Computer Science and Engineering
Sahyadri College of Engineering and Management
Mangalore-575007

Pavan Kumar V
Asst. Prof. Department of CSE
Sahyadri College of Engineering and Management
Mangalore-575007

***Abstract*— A Password is a secret word that must be used to gain access on websites. There are various types of password like Graphical passwords, text passwords etc, in which text password is most popular user authentication on websites. As Text password is simple and easy to use but it still suffers from different threats and it also can be stolen. Most of the users use the weak passwords or use same password over many websites. If hackers get one of the passwords from the websites, they try to use those passwords across the different websites to gain access. Another risk is that when a person enters his/her password in an untrusted computer then the password is prone to stealing attacks such as phishing, malware and key loggers etc. In proposed system, A user authentication protocol named SecurePass which involves a user's cell phone and a short message service to prevent password stealing and password reuse attack. SecurePass requires a unique phone number that will be possessed by each participating website. Here a telecommunication service provider is involved during the registration and the recovery phases and users just have to remember the long term passwords for secure login. Thus we believe that SecurePass is more efficient user authentication protocol that prevents password stealing and reuse attacks.**

Keywords—Password reuse attack; Password Stealing attack; OTP; User Authentication

I. INTRODUCTION

Password security is most important on network system. Many types of passwords like text password, graphical password can be used and there are different number of factors can be used for user authentication like-Single password can be used to login into website, Two factor authentication depends on what you know (e. g. password) and what you have (e. g. token), Three factor authentication depends on what you know (e. g. password), what you have (e. g. token) and who you are (e. g. Biometric). Among all text password is most commonly used for user authentication on different websites. By selecting username and password one can register their account on website. And to successfully login on a website user must recall that password. If selected password is robust, then different attacks that reveal password can be avoided. But if selected password is weak, it can be vulnerable to various types of attacks. If same password is used across different websites and if adversary compromise one of their password, they will exploit it to gain access to more websites. This causes user to lose sensitive information from different websites. This attack is known as Password Reuse attack [1][2]. Another problem is Password stealing attack leads to major problems in web environment. Password stealing can be done in several ways they are key loggers, phishing attack etc., basically password are encrypted using hashed function and stored into the database. Eavesdroppers easily identify and decrypt those hashed password. The above problems are mainly caused by the negative influence of human factors.

According to the researchers humans are quite a good expert in remembering something which is represented in pictorial format, thus graphical password schemes were designed to overcome the text password schemes [3], [4] to address human recall problem. There is also an alternative method where password management tool is used [5]. These tools automatically generate strong passwords for the users for each websites, which eliminates password reuse and password recall problem. The advantage of this password management tools is that user has to remember only a master password for accessing the tool. But Graphical password user authentication is still not yet mature and there are considerable amount of graphical password attacks [6]. Password management tool works well but still users have trouble in these tools due to their lack of knowledge of using it. Some researchers tend to focus on the three-factor authentication procedure rather than the password user authentication for more reliable user authentication. It is base on what you know (i.e., password), what you have (i.e., token), what you are (i.e., biometric). For this type of authentication the user has to input their password and provide a pass code generated by the token (e.g., RSA SecureID [12]), and scan their biometric feature usually their fingerprint. Even though it gives security for the user authentication mechanism, it requires a high cost for applying it in practice. Thus two-factor authentication is more practical than the three- factor authentication. Many support two-factor authentication which still suffers from negative influence of human factors and also the password stealing attacks. So as to overcome this user must remember another four-digit PIN code to work together with the token for authentication. A user authentication protocol named SecurePass which uses user's cellphone and a short message service (SMS) to prevent password stealing and reuse attacks. The main cause of password stealing is by entering the username and the

password in untrusted computers or websites. Unlike other user authentication systems the user doesn't have to enter their password in the browser. Instead a new component is used, users cellphone for enter the password and a new communication channel SMS is used to transmit the authentication messages.

A. Background

Some of the features of the SMS channel and why SMS can be trusted and also the security of the 3G connection which is used in registration and recovery phases of the authentication system.

- **One time password**

  The One-time passwords in SecurePass 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 *N* one-time passwords, the first of these passwords is produced by performing *N* hashes on input c.

$$\delta_0 = H^N(c) \qquad (1)$$

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

$$\delta_1 = H^{N-1}(c) \qquad (2)$$

  Hence, the general formula is given as follows:

$$\delta_i = H^{N-i}(c) \qquad (3)$$

  For security reasons, we use these one-time passwords in reverse order, i.e., using δ_{N-1} then δ_{N-2} . . . . δ_0. Even if an old password is hacked, the attacker is unable to drive the next one. In other words, she cannot impersonate a legal user without the secret shared credential. The input is derived from a long-term password P_u, the identity of server (ID_s), and a random seed ϕ generated by the server.

$$c = H(P_u \| ID_s \| \phi) \qquad (4)$$

- **SMS Channel**

  SMS is a fundamental text based communication service provides by the telecommunication system which belongs to 3GPP standards. Also SMS is a successful data transmission techniques used by the telecom systems, hence it is widely spread across the world. This authentication protocol uses the SMS channel for a secure user authentication to provide password stealing attacks. Unlike TCP/IP, SMS is a closed platform, thus increasing the difficulties for internal attacks like tampering and manipulating attacks. Therefore SMS channel is an out-of-band communication channel which is use to transmit secured messages between the users and the servers without entering the passwords in untrusted kiosks.

II. RELATED WORK

In 2004, M. Wu, S. Garfunkel, and R. Miller proposed a solution to the problem of phishing attacks using a mobile phone as a hand-held authentication token.A security proxy which allows the system to be used with unmodified third-party web services. The main goal is to create a system that is both secure and highly usable. The security of the proposed system depends on the SMS that is encrypted using A5/1 algorithm. The drawback was that A5/1 has been broken by Barkan and Biham in 2006 [9].And also they are vulnerable to the mobile phone theft.

Mannan and Oorschot in 2007 proposed a protocol named MP-Auth, a user authentication protocol [8]. MP-Auth forces the input of a long-term secret (typically a user's text password) through a trusted mobile device, to strengthen password-based authentication in untrustworthy environment. This protocol prevents passwords from being attacked i.e keylogger , malware but it still suffered from reuse attacks and another drawback is that account and passwords are created through physical contact i.e banks request users to send passwords through postal service or account personally.

Parno [10] proposed a mobile device as authentication tokens to build an anti-phishing mechanism is called Phool proof. Here users have to log in through issued public key and account/password combination. The drawback was that it was vulnerable to reuse problem. Another approach to prevent from phishing attack was Session Magnifier [11] that enables an extended browser on a mobile device and a regular browser on a public computer to collaboratively secure a web session. Session Magnifier separates user access to sensitive inter-actions (online banking).

III. DESIGN METHODOLOGY

User authentication protocol SecurePass, designed to generate different random passwords for each login to avoid recall problems and password reuse problems for the users. The figure 1 shows the architecture of SecurePass.

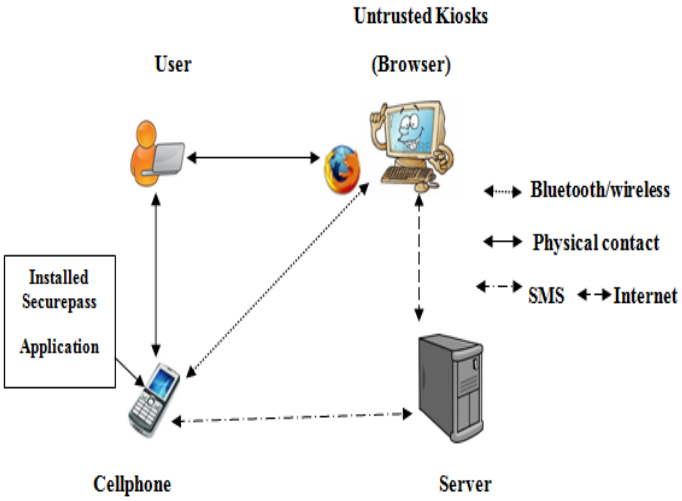
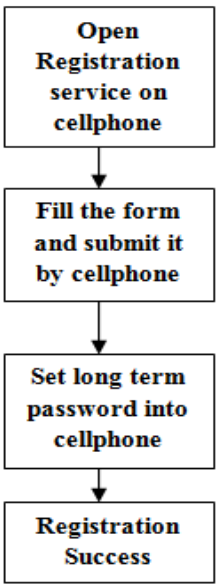


Figure 1: Architecture of SecurePass

A protocol SecurePass requires the only user's unique mobile number. SecurePass generates random one time passwords for each login. Telecommunication service provider (TSP) is involved in registration, login and recovery phase. In the registration phase, starting SecurePass program on their mobile, user must provide their personal information with unique phone number. This personal information is stored into the database and one long term password generated is also stored in database in encrypted format. In login phase, user need to provide the only the username as input to the system. User get random one time password generated by the web server after providing the long term password in mobile application. This one time password are created by using hash algorithm and stored in encrypted format. In the recovery phase, if user loses his mobile then the protocol is able to recover the user setting for the new phone. Setting can be recovered by using two things such as mobile number and long term password.

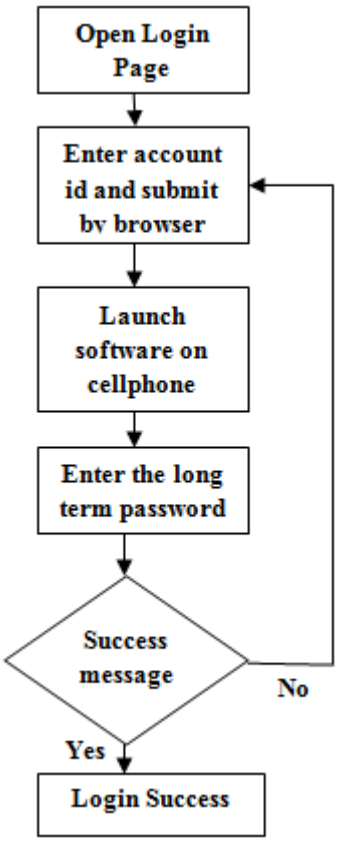
A. Registration Phase



The aim of this phase is to allow a user and a server to negotiate a shared secret to authenticate succeeding logins for this user. The user begins by opening the SecurePass program installed on her cellphone. She enters ID_u (account id she prefers) and ID_s (usually the website URL or domain name) to the program. The mobile program sends ID_u and ID_s to the telecommunication service provider (TSP) through a 3G connection to make a request of registration [1]. As soon as the response is received, the user then continues setting up a strong long-term password P_u with the required cellular phone.

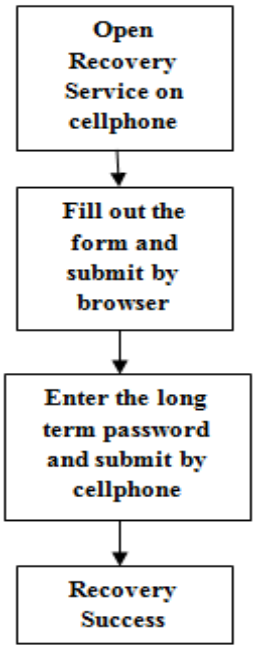
B. Login Phase

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 user's cell phone.



Once the long term password is entered, one time password is generated and send a login SMS securely to the server. The login SMS is encrypted by the onetime password. Finally, the cellphone receives a response message from the server and shows a success message on her screen if the server is able to verify her identity and this ensures that the website is a legal website.

C. Recovery Phase



Recovery phase is designated for some specific conditions; for example, a user *u* may lose her cellphone. The SecurePass is able to recover the setting on new cellphone assuming User still uses the same phone number (apply a new SIM card with old phone number). Once user installs the SecurePass program on new cellphone, then launch the program to send a recovery request with account ID_u and requested server ID_s to TSP.

Name	Description
ID_u	Identity of user
ID_s	Identity of Server
P_u	Long term password
Φ	Random Seed
$\|$	Concantination op.
H (o)	Hash function with o
N	Predefined length of Hash chain {}
δ_i	$_w$ ith one time password
C	Secret shared credential between cellphone and the server.

Table 1 show notation used:

D. Application

- Confidentiality of Information
- Avoids Man-in-middle Attacks
- Authentication
- Independence between login

IV. CONCLUSION

In proposed system, A user authentication protocol named SecurePass which leverages cellphones and SMS to thwart password stealing and password reuse attacks.. The design principle of SecurePass is to eliminate the negative influence of human factors as much as possible. Through SecurePass, each user only needs to remember a long-term password which has been used to protect cellphone. Users don't have to type any passwords into untrusted computers for login on all websites. SecurePass is the first user authentication protocol to prevent password stealing (i.e., phishing, keylogger, and malware) and password reuse attacks simultaneously. The reason is that SecurePass adopts the one-time password approach to ensure independence between each login. To make SecurePass fully functional, recovery phase is also considered and supported when users lose their cellphones. They can recover our SecurePass system with reissued SIM cards and long-term passwords. Because of the co-ordination of the system and cellphones to protect login service of all websites, so the proposed scheme is efficient.

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] 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.

[4] 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.

[5] 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.

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

[7] TS 35.201: Specification 3GPP Confidentiality Integrity Algorithms Document 1: f8 and f9 Specification 3GPP [Online]. Available: http://www.3gpp.org/

[8] M. Mannan and P. van Oorschot, "Using a personal device to strengthen password authentication from an untrusted computer," *Financial Cryptography Data Security*, pp. 88–103, 2007.

[9] E. Barkan and E. Biham, "Conditional estimators: An effective attack on A5/1," in *Selected Areas in Cryptography*. NewYork:Springer, 2006, pp. 1–19.

[10] B. Parno, C. Kuo, and A. Perrig, "Phoolproof phishing prevention," *Financial Cryptography Data Security*, pp. 1–19, 2006.

[11] C. Yue and H. Wang, "SessionMagnifier: A simple approach to secure and convenient kiosk browsing," in *Proc. 11th Int. Conf. Ubiquitous Computing*, 2009, pp. 125–134, ACM.

[12] H.M.Sun, Y.H.Chen, Y.H.Lin, "oPass: A User Authentication Protocol Resistant to Password Stealing and Password Reuse Attacks", IEEE Transactions on Information Forensics and Security, vol.7, no.2, April 2012.