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. 6, June 2014, pg.674 – 680

RESEARCH ARTICLE

SWAP: Secure Web Authentication Protocol on Windows Mobile App

Sonal Fatangare [1], Archana Lomte [2]

[1]Department of Computer Engineering, Bhivrabai Sawant Institute of Technology and Research (W), Pune, India

[2]Department of Computer Engineering, Bhivrabai Sawant Institute of Technology and Research (W),Pune, India

[1] sonal_fatangare@rediffmail.com; [2] archanalomte@gmail.com

Abstract— Password Security is a major issue for operators and users of the website and its many applications. Among the complicated problems still efficiently addressed is identity authorization. Normal user uses text passwords for authentication which select while registering accounts on a website. If a user selects a weak password and uses that among different websites causes domino effect. The proposed system is a OTP user authentication protocol which leverages a user's cell phone and Web service to resist password stealing, password reuse and collision attacks. Through our system users only need to remember a long term password for login on all websites. It uses one time password strategy. SWAP (Secure Web Authentication Protocol) is efficient and affordable compared with the conventional web authentication mechanism. The design principle is to eliminate the negative influence of human factor as much as possible. It only requires each participating website possess a unique phone number and involves a registration and a recovery phase.

Keywords— Network security, Password reuse attack, one time password, user authentication

I. INTRODUCTION

The past two decades have seen a gigantic increase in the development and use of networked and distributed systems, providing increased functionality to the user and more efficient use of resources. The past few decades, text password has been used as the primary mean of user authentication for websites. A major problem of Password-based user authentication has humans are not experts in memorizing text strings.

1. In 2007, Florencio and Herley [1] indicated that on an average normal user reuses a password across 3.9 distinct websites. Because of password reuse users loses 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 evil fortune of human factors. Therefore, most important thing is to take human factors into consideration when designing a user authentication protocol.

2. When consideration of the password reuse attack, it is also important to think over the effects of password stealing attacks. Attacker steals or compromise passwords and impersonates users' identities to launch malevolent attacks, collect sensitive information, perform unauthorized payroll actions, or leak financial secrets [2]. Phishing is a way of attempting to acquire information such as usernames, passwords, and credit card details by masquerading as a trustworthy entity in an electronic communication. According to APWG's report [3],

97388 phishing websites detected at the second season of 2010. Most previous studies have proposed schemes to defend against password stealing attacks [4].

Our protocol is a user authentication protocol which advantages a user's cell phone and Web service (SMS) to prevent password robbery and password reuse attacks. It is difficult to prevent password reuse attacks from any scheme where the users have to memorize something. The main concept of proposed protocol is free users from having to remember or type any passwords into conventional computers for authentication. Unlike common user authentication, SWAP(Secure Web Authentication Protocol) involves a new component, the mobile phone, which is used to generate OTPs (one-time passwords) and a new communication channel, SMS, which is used to transmit authentication messages.

II. LITERATURE REVIEW

Up to now, researchers have investigated a variety of technology to reduce the negative influence of human factors in the user authentication procedure. Usually humans are more adept in memorizing graphical passwords than text passwords many graphical password schemes were designed to address human's password recall problem .

In 2004 Wu et al. [5] proposed an authentication protocol depending on a trusted proxy and user mobile devices for prevent compromising user credentials. Secure login is authenticated by a token (mobile device) on untrusted computers, e.g., systems. A random session name is sent by SMS from the proxy to the mobile device for thwart phishing sites.

In 2006 Barkan and Biham [6] has been broken algorithm A5/1 this algorithm creates SMS, which are encrypted with A5/1. But this system is also vulnerable to cell phone robbery. On the contrary, our protocol encrypts every SMS before sending it out and utilizes a long-term password to protect the cell phone.

In 2007 Mannan and Oorschot [7] presents MP-Auth protocol, which forces the input of a long-term text password through a trusted mobile device. Before sending the password to an untrusted system, the password is encrypted by using preinstalled public key on a remote server. MP-Auth is intended to protect passwords from attacks raised by untrusted systems, including key loggers and malware. MP-Auth suffers from password reuse vulnerability.

On the other side, some literature represents different approaches to prevent phishing attacks. In detail, we will review three typical OTP schemes.

The first one is Lamport's Scheme [8]. In the scheme, a hash chain is formed as a secure hash function which is applied for hash function iteration to a secret key. In this scheme uses number of hash iteration authentication, the server sends a challenge to the user. Then calculates the OTP using a microcomputer and sends it to serve as a response. The identify of user is authenticated by Server with checking hash authentication.

The second one is Yeh–Shen–Hwang's Scheme [9], which is designed of Registration phase, Login phase and Authentication phase. In Registration phase, Sever issues a smart card to User. The card contains a pre-shared secret, a large random number (a permitted number of login times). Once receiving them, User can extract random number by performing XOR operation on secret and random number. Random number is hashed one time and compared with the secure hash function. The identity of Server is authenticated if they are same. Then User computes the initial password and send to User by maintain the private secret of User. In Login phase, Server sends challenge values to User. Similarly as in Registration phase, the identify of Server can be authenticated by User. Then Server responses Server with encrypted data; In Authentication phase, Server can obtains plaintext by performing the XOR operation on encrypted data Then plain text is hashed one time and compared with paintext−1. If they are same, the identity of User is authenticated by Server. After the successful authentication, Server and User replace new plain and cipher text with old respectively. However, it causes the stolen-verifier attack [10].

The third one is Eldefrawy et al.'s Scheme [11] using nested hash chains. There are two phases, which are Login and Authentication phase and Registration phase. In Registration phase, User and S share OTP seed and the authentication seed. User stores them in his token. In Login and Authentication phase Server sends the challenge values to User, where random integers generated by Server. The values are the challenge core. Once receiving them, User can check whether the identify of Server can be authenticated by User with positive results. After the successful authentication, User extracts challenges values. User calculates the OTP same procedure done at server. Then User responses Server after receiving the response, Server checks whether Plain text and OTP. If the two results are positive, the identify of User can be authenticated by Server. After the successful authentication, User and Server update respectively.

III. PROBLEM DEFINITION AND PROPOSED SYSTEM

A. Problem Definition

To develop proposed system, mobile phone application that uses One Time Password technique for secure communication between client and server. It is a Secure OTP generation using user authentication protocol

which leverages a user's Cellphone and Web service to thwart password stealing ,password reuse and collision attacks.

B. Architecture of Proposed System

Authentication ensures that system's resources are not obtained fraudulently by illegal users. Password authentication is one of the most convenient and simplest authentication mechanisms over untrusted networks. The problem of password authentication in untrusted networks is present in many application areas. Since computing resources have tremendously grown, password authentication is more frequently required in areas such as remote login, operation systems, computer networks, wireless networks and database management systems. When application uses to weak single-factor authentication, which many are more familiar with as the single static passwords still employed by most companies. The static passwords are easy to remember. However, when different systems have different passwords, then it can be difficult to remember and may have to be raising their vulnerability. Most often, static passwords are short and based on subjects close to the user—birthdays, partner names, children's names—and they are typically only letters. It is obvious others can access their personal accounts; otherwise we need to change the password repeatedly. To overcome these drawbacks new method is invented that is called "One Time Password (OTP)", which is valid for only one login session or transaction. This method allows the user to get login into the system by entering their password with OTP. In our proposed approach, after user enters the username and password web server generates the Encrypted OTP algorithm and sends it to the users mobile. It is an encrypted format, so users can't read it. Instead of that, user needs to forward that OTP with system logging password to the system. At the system end encrypted OTP is decrypted and verify the OTP, Password and mobile number for a particular username. In this approach user's information are verified in many levels. It avoids the unauthorized logging.

System architecture is same as oPass [12] architecture but our authentication protocol generates different OTP than oPass.

Firstly we will make a mobile application which will contain three main options or methods for the users:

1. Registration phase
2. Login phase
3. Recovery phase

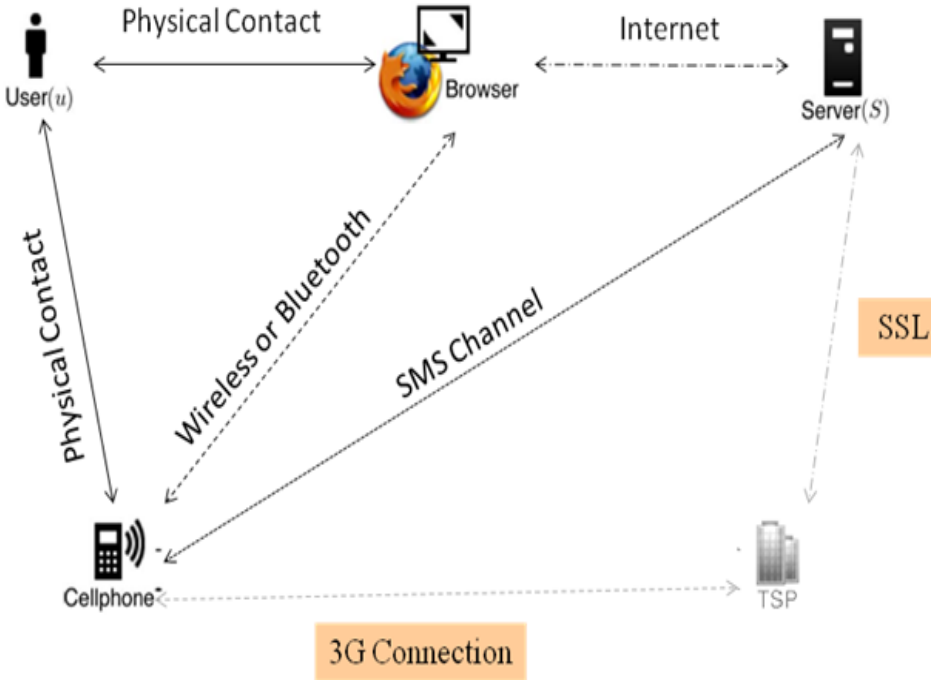

Fig. 1. System Architecture

We have to design an application server which will act as a third-party to distribute the key as well as to trace the unique Id of the web server. Firstly user will send a message containing his/her information like unique ID, server domain/URL, and contact number according to SIM to application server which will in turn send this information to the Web server (URL provided by user). After we receive a message from server then only we will be able to communicate with the web server.

TABLE 1.
NOTATIONS OF AUTHENTICATION PROTOCOL

Name	Description
Sid	Sever identity
Tu	User telephone number
Φ	Random seed
N	Per-define length of hash chain
Nz	Nonce generated by any entity z
Pu	Long term password of user
Ksd	Shared secret key of AES
C	Secrete shared credential between mobile and server
||	Concatenation
H(0)	Hash function H*with input 0
IV	Initialization Vector
*Hash Function is SHA-512	

To develop all this we are going to use SOAP web services. After we get the unique ID of server we have to send a message called as Registration message to the server which will contain all the user credentials. These credentials are encrypted by using HMAC algorithm and the key which application server will distribute between the client and server. A user can login to a particular site if he/she is registered to that site.

Registration is the first and the most important step which user has to perform. Fig. 2 depicts the registration phase. The purpose of this phase is to allow a user and a server to negotiate a shared secret to authenticate succeeding logins for this user.

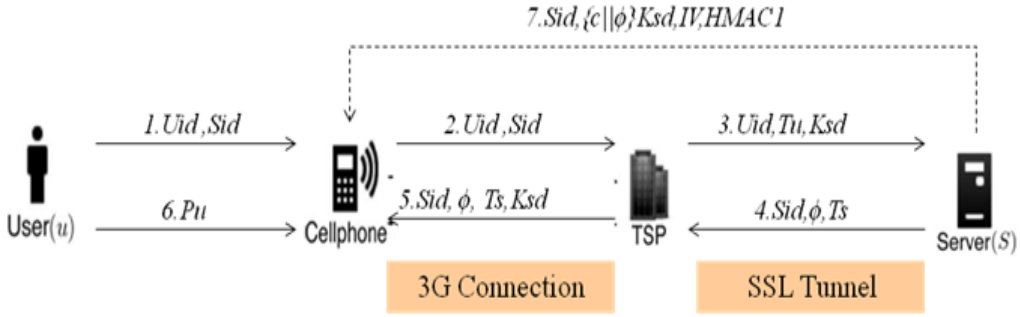

Fig. 2. Registration Phase

Secondly we have to implement login phase. In login phase actual process of OTP generation will take place. At beginning of login phase the user sends a request to the server through an untrusted browser (on a kiosk). The user uses his/her cellphone to produce a one-time password, and deliver necessary information encrypted with to server via an SMS message. Based on previously shared secret credential, server can verify and authenticate user based on. Fig. 3 shows the detail flows of the login phase.

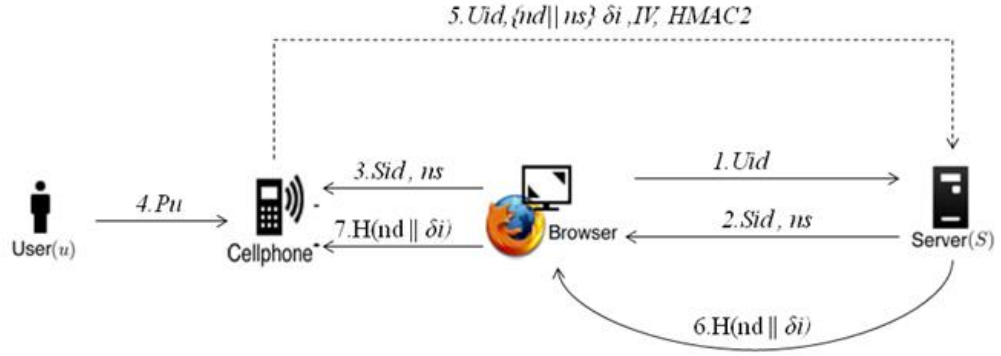

Fig. 3. Login Phase

Recovery phase comes into picture when the user loses his or her Cell phone. The protocol is able to recover setting on his/her new cell phone assuming he/she still uses the same phone number (apply a new SIM card with old phone number). Fig. 4 shows the detail flows of the Recovery phase.

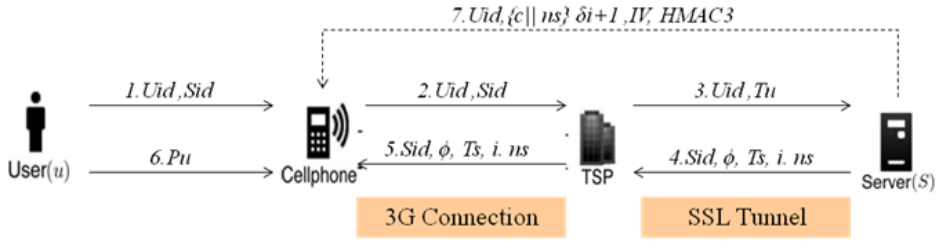

Fig. 4. Recovery Phase

IV. METHODOLOGY

The methodology used in this paper for OTP generation is that HMAC algorithm has been studied using different SHA-512 algorithm. The algorithms are evaluated using the OTP validity. Authentication is that the claimant "proves" its identity to the verifier by providing its uniqueness or timeliness guarantee to the knowledge of a secret known to be associated with itself during the authentication protocol.

A. OTP (One Time Password)

The one-time passwords in our system are generated by a secure one-way hash function. With a given input c, 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

$$\delta_o = H^N(c) \quad \text{..... (1)}$$

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

$$\delta_1 = H^{N-1}(c) \quad \text{..... (2)}$$

Hence, the general formula is given as follows:

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

For security reasons, we use these one-time passwords in reverse order, i.e., using δ_{N-1} , then δ_{N-2}, ……, δ_o. If an old 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 long-term password Pu , the identity of server Sid , and a random seed ϕ generated by the server

$$c = H(Pu||Sid||\phi) \quad \text{... ... ... (4)}$$

Note that function H is a hash which is irreversible in general cryptographic assumption. In practice, H is realized by SHA-512. Therefore, the bit length of is 512.

B. Web Service

Web service is a method of communication between two electronic devices over the web (internet). The W3C defines a "Web service" as a software system designed to support interoperable machine-to-machine interaction over a network". It has an interface described in a machine-process able format (specifically Web Services Description Language, known by the acronym WSDL). Other systems interact with the Web service in a manner prescribed by its description using SOAP messages, typically conveyed using HTTP with an XML serialization in conjunction with other Web-related standards."

A Web service is a unit of managed code that can be remotely invoked using HTTP, that is, it can be activated using HTTP requests. So, Web Services allows you to expose the functionality of your existing code over the network. Once it is exposed on the network, other application can use the functionality of your program. Web Services uses SOAP over HTTP protocol for the communication, so you can use your existing low cost internet for implementing Web Services. This solution is much less costly compared to proprietary solutions like EDI/B2B. Beside SOAP over HTTP, Web Services can also be implemented on other reliable transport mechanisms like FTP etc.

C. 3G Connection

3G connection provides data confidentiality data integrity. It is telecommunication networks support services therefore we used for communication between mobile and telecommunication service provider. 3G networks offer greater security than their 2G predecessors. By allowing the UE (User Equipment) to authenticate the network it is attaching to, the user can be sure the network is the intended one and not an impersonator. Our protocol utilizes the security features of 3G connection to develop the convenient account registration and recovery procedures. Through a 3G connection, users can securely transmit and receive information to the web site.

V. COMPARISONS

The SHA-512 algorithm used in this paper for OTP generation therefore it differentiate to other schemes as follows.

TABLE 2.
COMPARISONS AMONG OTHER SCHEMES.

Scheme	Attacks Prevention			
	Phishing	**keylogger**	**Password reuse**	**Collision**
SWAP Scheme	Yes	Yes	Yes	Yes
oPass[12]	Yes	Yes	Yes	No
Eldefrawy et al.'s Scheme[11]	Yes	Yes	Yes	No
Yeh–Shen–Hwang's Scheme [9]	Yes	Yes	No	No
Lamport's Scheme [8]	Yes	Yes	No	No

VI. CONCLUSIONS

As discussed above in paper, the report proposed a user authentication protocol which leverages cell phones and Web service to prevent password stealing, password reuse and collision attacks. Here assume that each website possesses a unique phone number and telecommunication service provider participates in the registration and recovery phases.

The design principle of system is tried to eliminate the negative influence of human factors as much as possible. Through SWAP (Secure Web Authentication Protocol), each user only needs to remember a long-term password which has been used to protect cell phone. Users are free from typing any passwords into untrusted computers for login on all websites.

Advantages:

The proposed system presents the following advantages:

1) Unique OTP
2) OTP is valid for specific time
3) Anti-malware
4) Phishing Protection
5) Secure Registration and Recovery
6) Password Reuse Prevention and Weak Password Avoidance
7) Cell phone Protection

Therefore, our user authentication protocol is acceptable and reliable for users, and more secure than the original login system.

ACKNOWLEDGMENT

It gives us immense pleasure and satisfaction to express our heart-felt gratitude towards Head of the Department, Prof.Gayatri Bhandari for the constant support and encouragement they provided during the preparation of the paper.

REFERENCES

[1] 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.

[2] 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.

[3] Phishing Activity Trends Rep., 2nd Quarter/2010 Anti-Phishing Working Group [Online].Available: http://www.antiphishing.org/.

[4] S. Garriss, R. Cáceres, S. Berger, R. Sailer, L. van Doorn, and X. Zhang, "Trustworthy and personalized computing on public kiosks,"in Proc. 6th Int. Conf. Mobile Systems, Applications Services, 2008,pp. 199–210, ACM.

[5] M.Wu, S. Garfinkel, and R. Miller, "Secure web authentication with mobile phones," in *DIMACS Workshop Usable Privacy Security Software*,Citeseer, 2004.

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

[7] 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.

[8] L. Lamport, "Password authentication with insecure communication,"*Commun. ACM*, vol. 24, pp. 770–772, Nov. 1981.

[9] T.C. Yeh, H.Y. Shen, J.J. Hwang, "A secure one-time password authentication scheme using smart cards," *IEICE Trans. Commun.* E85 (2002) 2515–2518.

[10] W.C. Ku, H.C. Tsai, M.J. Tsaur," Stolen-verifier attack on an efficient smartcard-based one-time password authentication scheme", IEICE Trans. Commun.E87-B (8) (2004) 2374–2376

[11] M.H. Eldefrawy, M.K. Khan, K. Alghathbar,, "One-time password System with infinite nested hash chains," *Commun. Comput. Inf. Sci. 122 (2010) 161–170.*

[12] *Hung-Min Sun, Yao-Hsin Chen, and Yue-Hsun Lin, "oPass:A User Authentication Protocol Resistant to Password Stealing and Password Reuse Attacks," IEEE TRANSACTIONS ON FORMATION FORENSICS AND SECURITY, VOL. 7, NO. 2,APRIL2012*

[13] TS 23.040: Technical Realization Web service (SMS) GPP[Online].Availablehttp://www.3gpp.org

