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. 10, October 2013, pg.48 – 56

RESEARCH ARTICLE

Mobile Based User Authentication for Guaranteed Password Security Using key

B.Sivakumar[1], S.Venkatesan[2], Y.Kalifulla[3], D.Anandan[4]

[1,2,3,4] Assistant Professor, Veltech Multitech Dr.Rangarajan Dr.Sakunthala Engineering College, Chennai, India

sivablack@gmail.com [1], svsan81@gmail.com [2], kalifulla@gmail.com [3], anandandk@gmail.com [4]

Abstract—Text password is the most popular form of user authentication on websites due to its convenience and simplicity. However, users' passwords are prone to be stolen and compromised under different threats and vulnerabilities. Firstly, users often select weak passwords and reuse the same passwords across different websites. Routinely reusing passwords causes a domino effect; when an adversary compromises one password, she will exploit it to gain access to more websites. Second, typing passwords into untrusted computers suffers password thief threat. An adversary can launch several password stealing attacks to snatch passwords, such as phishing, key loggers and malware. In this paper, we design a user authentication protocol named oPass which leverages a user's cellphone and short message service to thwart password stealing and password reuse attacks. oPass only requires each participating website possesses a unique phone number, and involves a telecommunication service provider in registration and recovery phases. Through oPass, users only need to remember a long-term password for login on all websites. After evaluating the oPass prototype, we believe oPass is efficient and affordable compared with the conventional web authentication mechanisms.

Keywords— Network security; password reuse attack; password stealing attack; user authentication

---

I. INTRODUCTION

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. In 2007, Florencio and Herley 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 **[1]**, many graphical password schemes were designed to address Human's password recall problem. Using password management tools is an alternative. 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 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.

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 cellphone, which is used to generate one-time passwords and a new communication channel, SMS, which is used to transmit authentication messages. oPass presents the following advantages.

1) Anti-malware—Malware (e.g., key logger) that gathers sensitive information from users, especially their passwords are surprisingly common. In oPass, users are able to log into web services without entering passwords on their computers. Thus, malware cannot obtain a user's password from untrusted computers.

2) Phishing Protection—Adversaries often launch phishing attacks to steal users' passwords by cheating users when they connect to forged websites. As mentioned above, oPass allows users to successfully log into websites without revealing passwords to computers. Users who adopt oPass are guaranteed to withstand phishing attacks.

3) Secure Registration and Recovery—In oPass, SMS is an out-of-band communication interface. oPass cooperates with the telecommunication service provider (TSP) in order to obtain the correct phone numbers of websites and users respectively. SMS aids oPass in establishing a secure channel for message exchange in the registration and recovery phases. Recovery phase is designed to deal with cases where a user loses his cellphone. With the aid of new SIM cards, oPass still works on new cellphones.

4) Password Reuse Prevention and Weak Password Avoidance— oPass achieves one-time password approach. The cellphone automatically derives different passwords for each login. That is to say, the password is different during each login. Under this approach, users do not need to remember any password for login. They only keep a long term password for accessing their cellphones, and leave the rest of the work to oPass.

5) Cellphone Protection— an adversary can steal users' cellphones and try to pass through user authentication. However, the cellphones are protected by a long-term password. The adversary cannot impersonate a legal user to login without being detected.

II. BACKGROUND

oPass adopts the one-time password strategy therefore **[2]**, the strategy is given later. We also describe the secure features of SMS channel and explain why SMS can be trusted. Finally, we introduce the security of 3G connection used in the registration and recovery phases of oPass.

A. One-Time Password

The one-time passwords in oPass 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** SHA-256 **[3]**

$$\delta_0 = H^{n}(c) \qquad (1)$$

The next one-time password is obtained by performing 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 $\delta_{N-2\ldots,}$ δ_0. 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 (P_u), the identity of server ID (ID_s), and a random seed (φ) generated by the server.

$$\mathbf{c} = H(P_u || ID_s || \varphi) \qquad (4)$$

B. SMS Channel

SMS is a text-based communication service of telecommunication systems. oPass leverages SMS to construct a secure user authentication protocol against password stealing attacks. As we know, SMS is a fundamental service of telecom, which belongs to 3GPP standards. SMS represents the most successful data transmission of telecom systems; hence, it is the most widespread mobile service in the world. Besides the above advantages, we chose SMS channel because of its security benefits. Compared with TCP/IP network, the SMS network is a closed platform; hence, it increases the difficulty of internal

attacks, e.g., tampering and manipulating attacks. Therefore, SMS is an out-of-band channel that protects the exchange of messages between users and servers. Unlike conventional authentication protocols, users securely transfer sensitive messages to servers without relying on untrusted kiosks. oPass resists password stealing attacks since it is based on SMS channels.

C. 3G Connection

3G connection provides data confidentiality of user data and signal data to prevent eavesdropping attacks. It also provides data integrity of signal data to avoid tampering attacks. The confidentiality and integrity algorithms are f8 and f9, respectively. Algorithm f8 and f9 are based on a block cipher named KASUMI **[4]** where f8 is a synchronous binary stream cipher and f9 is a MAC algorithm. oPass utilizes the security features of 3G connection to develop the convenient account registration and recovery procedures. Users can securely transmit and receive information to the web site through a 3G connection

III. PROBLEM DEFINITION AND ASUMPTIONS

Now, we consider various methods of password stealing. Afterwards, we introduce the architecture of our oPass system and make some reasonable assumptions.

A. Problem Definition

People nowadays rely heavily on the Internet since conventional activities or collaborations can be achieved with network services (e.g., web service). Widely deployed web services facilitate and enrich several applications, e.g., online banking, e-commerce, social networks, and cloud computing. But user authentication is only handled by text passwords for most websites. Applying text passwords has several critical disadvantages. First users create their passwords by themselves. For easy memorization, users tend to choose relatively weak passwords for all websites. This behavior causes a risk of a domino effect due to password reuse. To steal sensitive information on websites for a specific victim (user), an adversary can extract her password through compromising a weak website because she probably reused this password for other websites as well.

Therefore, we proposed a user authentication, called oPass, to thwart the above attacks. The goal of oPass is to prevent users from typing their memorized passwords into kiosks. By adopting one-time passwords, password information is no longer important. A one-time password is expired when the User completes the current session. Different from using Internet channels, oPass leverages SMS and user's cellphones to avoid password stealing attacks. As we mentioned in Section II, we believe SMS is a suitable and secure medium to transmit important information between cellphones and websites.

Based on SMS, a user identity is authenticated by websites without inputting any passwords to untrusted kiosks. User password is only used to restrict access on the user's cellphone. In oPass, each user simply memorizes a long-term password for access her cellphone. The long-term password is used to protect the information on the cellphone from a thief.

B. Architecture of oPass and Its Assumptions

Fig. 1 describes the architecture (and environment) of the oPass system. For users to perform secure login on an untrusted computer (kiosk), oPass consists of a trusted cellphone, a browser on the kiosk, and a web server that users wish to access. The user operates her cellphone and the untrusted computer directly to accomplish secure logins to the web server. The communication between the cellphone and the web server is through the SMS channel. The web browser interacts with the web server via the Internet. In our protocol design, we require the cellphone interact directly with the kiosk. The general approach is to select available interfaces on the cellphone, Wi-Fi or Bluetooth.

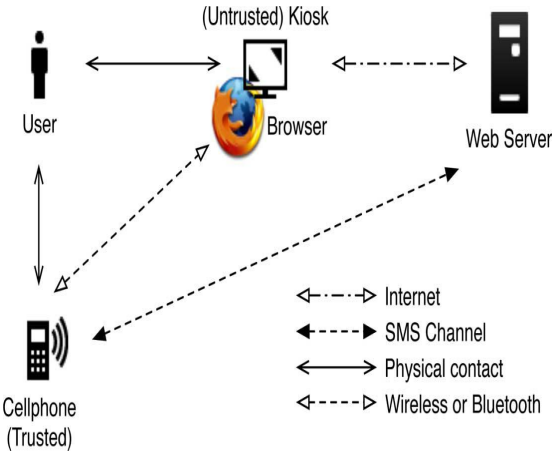

Fig 3: Architecture of oPass

The assumptions in oPass system are as follows.

1) Each web server possesses a unique phone number. Via the phone number, users can interact with each website through an SMS channel.

2) The users' cellphones are malware-free. Hence, users can safely input the long-term passwords into cellphones.

3) The telecommunication service provider (TSP) will participate in the registration and recovery phases. The TSP is a bridge between subscribers and web servers. It provides a service for subscribers to perform the registration and recovery progress with each web service. For example, a subscriber inputs her id ID and a web server's id ID to start to execute the registration phase. Then, the TSP forwards the request and the subscriber's phone number T_U to the corresponding web server based on the received ID.

4) Subscribers (i.e., users) connect to the TSP via 3G connections to protect the transmission.

5) The TSP and the web server establish a secure sockets layer (SSL) tunnel. Via SSL protocol, the TSP can verify the server by its certificate to prevent phishing attacks. With the aid of TSP, the server can receive the correct T_U sent from the subscriber.

6) If a user loses her cellphone, she can notify her TSP to disable her lost SIM card and apply a new card with the same phone number. Therefore, the user can perform the recovery phase using a new cellphone.

IV. OPASS

In this section, we present oPass from the user perspective to show operation flows. oPass consists of *registration*, *login*, and *recovery* phases. We introduce the details of these three phases respectively.

A. Overview

Fig. 2 describes the operation flows of users during each phase of oPass. Unlike generic web logins, oPass utilizes a user's cellphone as an authentication token and SMS as a secure channel. Different from regular login processes, additional steps are required for oPass and are marked in back rectangles in Fig. 2. In the *registration* phase, a user starts the oPass program to register her new account on the website she wishes to visit in the future. Unlike conventional registration, the server requests for the user's account id and phone number, instead of password.

After filling out the registration form, the program asks the user to setup a long-term password. This long-term password is used to generate a chain of one-time passwords for further logins on the target server. Then, the program automatically sends a registration SMS message to the server for completing the registration procedure. The context of the registration SMS is encrypted to provide data confidentiality. oPass also designed a *recovery* phase to fix problems in some conditions, such as losing one's cellphone.

Contrasting with general cases, *login* procedure in oPass does not require users to type passwords into an untrusted web browser. The user name is the only information input to the browser. Next, the user opens the oPass program on her phone and enters the long-term password; the program will generate a one-time password and send a login SMS securely to the server. The login SMS is encrypted by the one-time 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. The message is used to ensure that the website is a legal website, and not a phishing one. Protocol details of each phase are provided as follows. Table I shows the notations used in the oPass system.

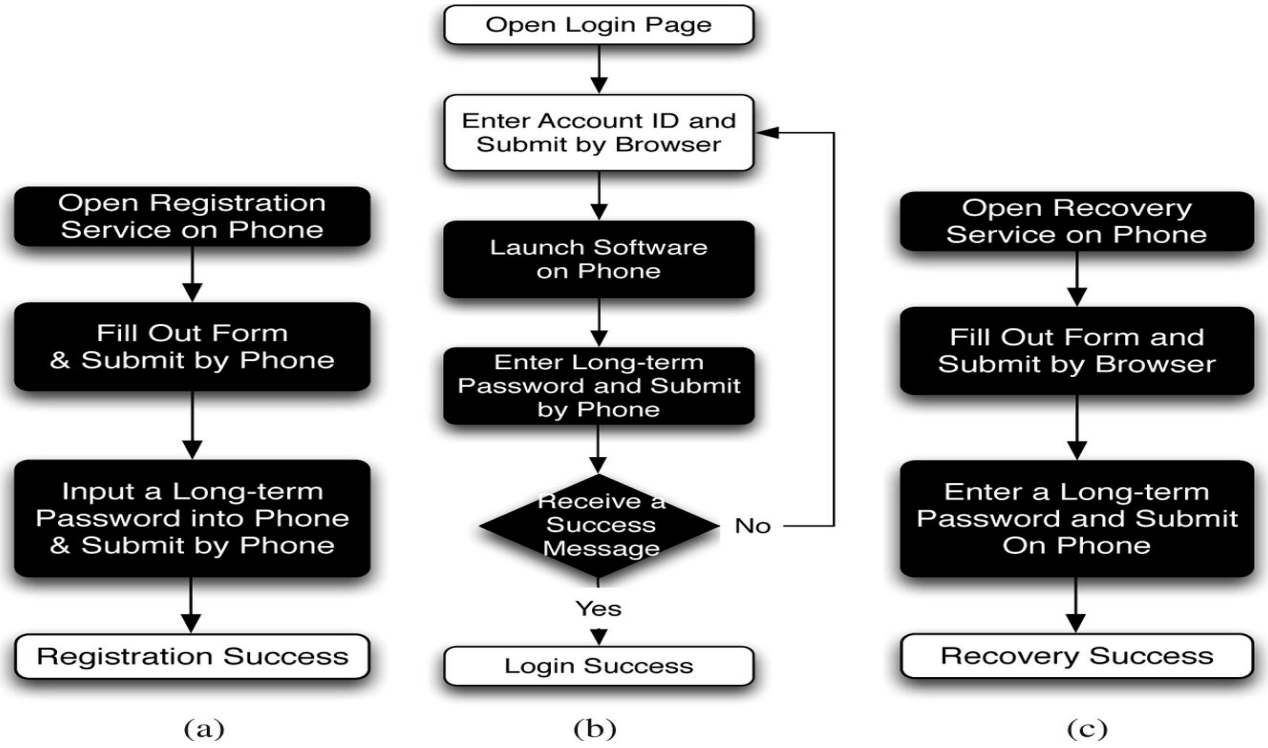

Fig 2**:**Operation flows for user in each phase of oPass system respectively. Black rectangles indicate extra steps contrasted with the generic authentication system: registration, (b) login, and (c) recovery

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 oPass program installed on her cellphone. She enters ID (account id she prefers) and ID (usually the website URL or domain name) to the program. The mobile program sends ID and ID to the telecommunication service provider (TSP) through a 3G connection to make a request of registration **[5]**.

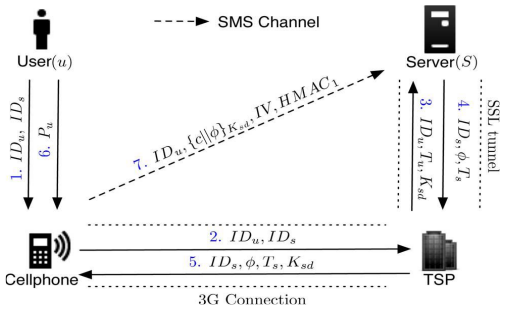

Fig 3: Procedure of registration phase.

C. Login Phase

The *login* phase begins when the user sends a request to the server through an untrusted browser (on a kiosk). The user uses her cell phone to produce a password, and deliver necessary information encrypted with to server via an SMS message. Based on preshared secret credential, server can verify and authenticate.

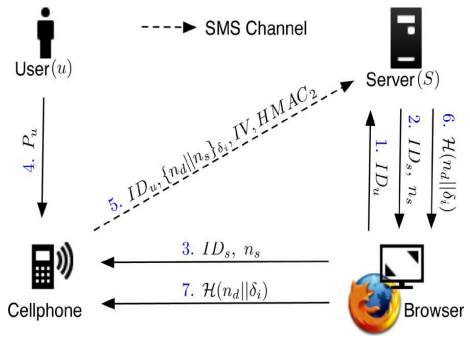

Fig 4: Procedure of login phase

D. Recovery Phase

Recovery phase is designated for some specific conditions; for example, a user may lose her cell phone. The protocol is able to recover oPass setting on her new cell phone assuming she still uses the same phone number (apply a new SIM card with old phone number).Once user installs the oPass program on her new cellphone, she can launch the program to send a recovery request with her account ID and requested server ID to predefined TSP through a 3G connection.

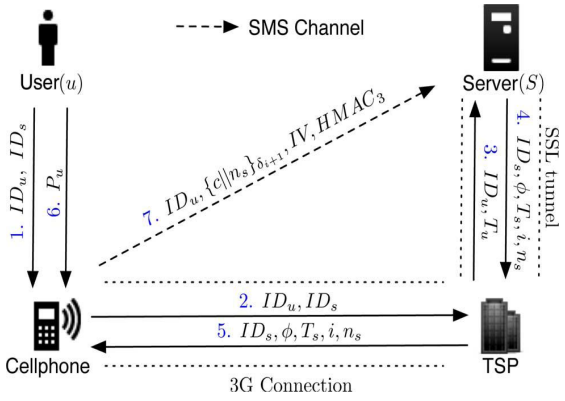

Fig 5**:** Procedure of recovery phase

E. Performance Evaluation

The average time of registering is 21.8 s and the SMS delay time is 9.1 s. Based on our observation, the SMS overhead is the major factor of the *registration* phase (about 41%). Because the

GSM modem in our evaluation is a cheap device, we believe that the performance can be improved when we utilize a more powerful GSM modem.

TABLE I
PERFORMANCE OVERHEAD IN OPASS

	Registration		Login	
	SMS delay	total	SMS delay	total
Avg. time (s)	9.1	21.8	8.9	21.6
(min, max) (s)	(6, 12)	(11, 59)	(7, 12)	(17, 32)
σ	1.72	14.05	1.45	4.05

V. CONCLUSION

In this paper, we proposed a user authentication protocol named oPass which leverages cellphones and SMS to thwart password stealing and password reuse attacks. The telecommunication service provider participates in the registration and recovery phases. Through oPass, each user only needs to remember a long-term password which has been used to protect her cellphone. Users are free from typing any passwords into untrusted computers for login on all websites. Compared with previous schemes, oPass is the first user authentication protocol to prevent password stealing (i.e., phishing, key logger, and malware) and password reuse attacks simultaneously. The reason is that oPass adopts the one-time password approach to ensure independence between each login. To make oPass fully functional, password recovery is also considered and supported when users lose their cellphones. The average time spent on registration and login is 21.8 and 21.6 s, respectively. The performance of login of oPass is better than graphical password schemes, for example, Pass faces. The login time of Pass faces is from 14 to 88 s, which is longer than oPass. Therefore, we believe oPass is acceptable and reliable for users. The login success rate is over 90%, except for a few typing errors. Consequently, they all agreed oPass is more secure than the original login system.

REFERENCES

[1] S. Chiasson, A. Forget "Click-based graphical passwords," in CCS '09: Proc. 16th ACM Conf. Computer Communications Security, New York, 2009, pp. 500–511, ACM.

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

[3] H. Gilbert and H. Handschuh, "Security analysis of SHA-256 and sisters," in *Selected Areas Cryptography*, 2003, pp. 175–193, Springer.

[4]TS 35.202: Specification 3GPP Confidentiality Integrity Algorithms Document 2: KASUMI Specification 3GPP [Online]. Available: http:// www.3gpp.org/

[5] H. Krawczyk, "The order of encryption and authentication for protecting communications (or: How secure is SSL?)," in *Advances Cryptology— CRYPTO 2001*, 2001, pp. 310–331.

