ISSN: 2278-0181

User Authentication Protocol Resistant to Password Stealing and Reuse attacks

Mohan kumar S.S
M.Tech Student
Computer science & Engg.
KIT, Tiptur
mohangubbi@gmail.com

Rudresh N.C
M.tech Student
Computer science & Engg.
KIT, Tiptur
Rudreshsana@gmail.com

Kusuma R
Lecturer
Computer science & Engg.
KIT, Tiptur
Kusuma.r15@gmail.com

***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 pass-words 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. A user authentication protocol named oPass which leverages a user's cell phone 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, pass-word 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 [1],[2]. In 2007, Florencio and Herley[3] 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.

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 [4], many graphical password schemes were designed to address human's password recall problem [5]. 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.

A. Technologies

Despite the assistance of these two technologies—

- graphical password
- 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.

Besides the password reuse attack, it is also important to consider the effects of password stealing attacks. 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. Many previous studies have proposed schemes to defend against password stealing attacks.

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 Secure ID), 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.

A user authentication protocol named OPass which leverages a user's cell phone and short message service (SMS) to prevent password stealing and password reuse attacks. It is difficult to thwart password reuse attacks from any scheme where the users have to remember something. The main cause of stealing password attacks is when user 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 cell phone, which is used to generate one-time passwords and a new communication channel, SMS, which is used to transmit authentication messages.

B. Advantages of oPass

OPass presents the following advantages.

1) Anti-malware—Malware (e.g., key logger) that gather 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 cell phone. With the aid of new SIM cards, OPass still works on new cell phones.

4) Password Reuse Prevention and Weak Password Avoidance— OPass achieves one-time password approach. The cell phone 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 cell phones, and leave the rest of the work to OPass.

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

II. BACKGROUND AND RELATED WORK

OPass adopts the one-time password strategy the secure features of SMS channel and 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 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 [6] on input c.

$$\delta_0 = \mathcal{H}^N(c).$$

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

$$\delta_1 = \mathcal{H}^{N-1}(c).$$

Hence, the general formula is given as follows:

$$\delta_i = \mathcal{H}^{N-i}(c).$$

For security reasons, we use these one-time passwords in reverse order, i.e., using δ_{N-1}, then $\delta_{N-2}, \ldots \delta_0$. 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_s, and a random seed (Φ) generated by the server ID Note that function is a hash which is irreversible in general cryptographic assumption. Therefore, the bit length of is 256.

$$C = \mathcal{H}(P_u \| ID_s \| \Phi).$$

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 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 ARCHITECTURE OF OPASS SYSTEM

In this section consider various methods of password stealing. The architecture of OPass system and 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 [2]. This behavior causes a risk of a domino effect due to password reuse [1]. 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. Second, humans have difficulty remembering complex or meaningless passwords [4]. Some websites generate user passwords as random strings to maintain high entropy, even though users still change their passwords to simple strings to help them recall it. Florencio and Herley[3] indicated that users forget passwords a lot: 1.5% of Yahoo users forget their passwords every month. Some studies pay attention to password management. These approaches could mitigate this problem, but they also make the system more complicated to use. In addition, phishing attacks and malware are threats against password protection. Protecting a user's password on a kiosk is infeasible when key loggers or backdoors are already installed on it. Considering the current mechanisms, authenticating users via passwords is not a comprehensive solution.

Therefore, a user authentication, called OPass has proposed, 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 cell phones to avoid password stealing attacks. SMS is a suitable and secure medium to transmit important information between cell phones 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 cell phone. In OPass, each user simply memorizes a long-term password for access cell phone. The long-term password is used to protect the information on the cell phone from a thief.

B. Architecture of oPass and its Assumptions

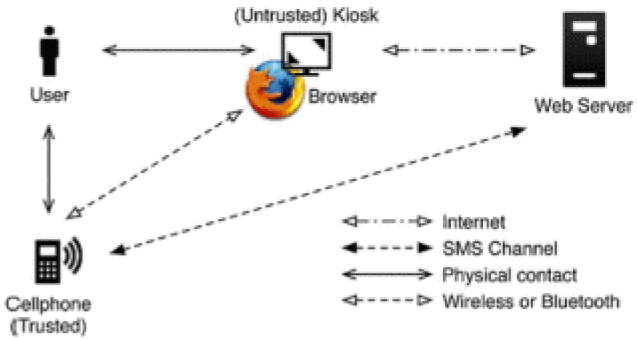

Fig 1. *Architecture of oPass system*

Figure. 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 cell phone, a browser on the kiosk, and a web server that users wish to access. The user operates cell phone and the untrusted computer directly to accomplish secure logins to the web server. The communication between the cell phone 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 cell phone interact directly with the kiosk. The general approach is to select available interfaces on the cell phone, Wi-Fi or Bluetooth.

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' cell phones are malware-free. Hence, users can safely input the long-term passwords into cell phones.

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_u and a web server's ID_s 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 cell phone, 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 cell phone.

IV. OPASS

OPass from the user perspective to show operation flows. OPass consists of *registration*, *login*, and *recovery* phases.

A. Overview

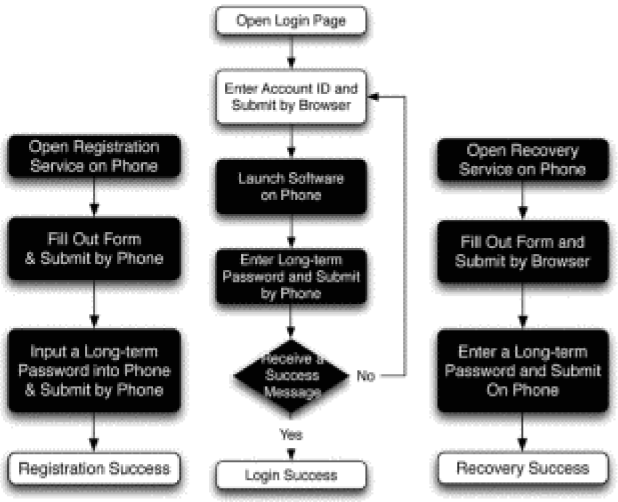

Figure. 2. Operation flows for user in each phase of OPass system respectively. Black rectangles indicate extra steps contrasted with the generic authentication system: (a) registration, (b) login, and (c) recovery.

Fig 2 describes the operation flows of users during each phase of OPass. Unlike generic web logins, OPass utilizes a user's cell phone 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 Figure. 2. In the *registration* phase, a user starts the OPass program to register thier new account on the website user 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 cell phone.

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 cell phone 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. Above Table 1 shows the notations used in the OPass system.

B. Registration phases

Figure. 3 depicts the *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 OPass program installed on her cell phone. 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. Once the TSP received the ID_u and the ID_s, it can trace the user's phone number based on user's SIMcard.

TABLE I
NOTATIONS

Name	Description
ID_x	Identity of entity x.
T_y	Entity y's phone number.
ϕ	random seed
N	Pre-define length of hash chain ($\{\delta_0 \sim \delta_{N-1}\}$).
n_z	Nonce generated by entity z.
P_u	User u's long-term password.
K_{sd}	Shared secret key between cellphone and the server.
c	Secret shared credential between cellphone and the server.
δ_i	i^{th} one-time password.
$\|\|$	concatenate operation.
$\{\}_k$	symmetric encryption[1] with key k.
$\mathcal{H}(\circ)$	Hash function $\mathcal{H}$[2] with input $\circ$.
IV	Initialization vector of AES-CBC.
$HMAC_1$	The HMAC-SHA1 digest of $ID_u\|\|IV\|\|\{c\|\|\phi\}_{K_{sd}}$ under the K_{sd}.
$HMAC_2$	The HMAC-SHA1 digest of $ID_u\|\|IV\|\|\{n_d\|\|n_s\}_{\delta_i}$ under the δ_i.
$HMAC_3$	The HMAC-SHA1 digest of $ID_u\|\|IV\|\|\{c\|\|n_s\}_{\delta_{i+1}}$ under the δ_{i+1}.

[1]Symmetric encryption algorithm in oPass is AES-256.

[2]Hash function is SHA-256.

Table 1 Notations

The TSP also plays the role of third-party to distribute a shared key between the user and the server. The shared key K_{sd} is used to encrypt the registration SMS with AES-CBC. The TSP and the server will establish an SSL tunnel to protect the communication. Then the TSP forwards ID_u,T_u and K_{sd} to the assigned server S. Server Swill generate the corresponding information for this account and reply a response, including server's identity ID_s, a random seed Φ, and server's phone number T_s. The TSP then forwards ID_s, Φ,T_s and a shared key K_{sd} to the user's cell phone. Once reception of the response is finished, the user continues to setup a long-term password P_u with her cell phone. The cell phone computes a secret credential by the following operation:

$$C = \mathcal{H}(P_u || ID_s || \Phi).$$

To prepare a secure registration SMS, the cell phone encrypts the computed credential with the key and generates the corresponding MAC, i.e., HMAC. HMAC-SHA1 takes input user's identity, cipher text, and IV to output the MAC.

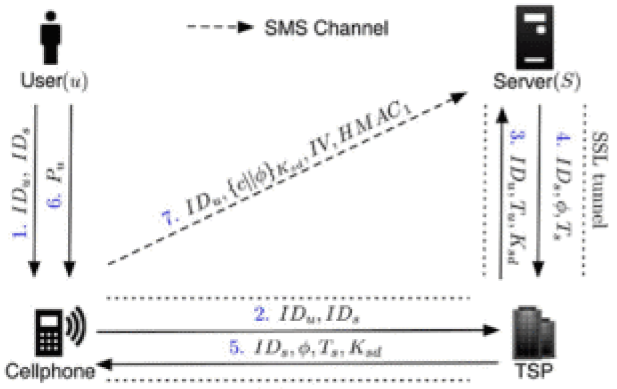

Fig 3. *Procedure of registration phase*

Then, the cell phends an encrypted registration SMS to the server by phone number T_s as follows:

$$\text{Cell phone} \xrightarrow{SMS} \text{S:ID}_u, \{c||\Phi\}K_{sd}, \text{HMAC}_1$$

Server S can decrypt and verify the authenticity of the registration SMS and then obtain with the shared key. Server also compares the source of received SMS with to prevent SMS spoofing attacks. At the end of registration, the cell phone stores all information {IDs,T_s, Φ,i} except for the long term password P_u and the secret. Variable indicates the current index of the one-time password and is initially set to 0, the server can authenticate the user device during each login. After receiving the message, the server stores {IDs,T_s, c,Φ,i} and then completes the registration.

C. *Login phase*

The *login* phase begins when the user u sends a request to the server S through an untrusted browser (on a kiosk). The user uses her cell phone to produce a one-time password, e.g., δ_i and deliver necessary information encrypted with δ_i to S server via an SMS message. Based on pre shared secret credential, server can verify and authenticate user u based on δ_i. Figure. 4 shows the detail flows of the login phase.

The protocol starts when user wishes to log into her favorite web server (already registered). However, begins the login procedure by accessing the desired website via a browser on an untrusted kiosk. The browser sends a request to S with u's account ID. Next, server supplies the ID and a fresh nonce to the browser. Meanwhile, this message is forwarded to the cell phone through bluetooth or wireless interfaces. After reception of the message, the cell phone inquires related information from its database via ID, which includes server's phone number and other parameters.

The next step is promoting a dialog for her long-term password. Secret shared credential can regenerated by inputting the correct on the cell phone. The one-time password for current login is recomputed using the following operations

$$C = \mathcal{H}(P_u || ID_s || \Phi).$$
$$\delta_i \leftarrow \mathcal{H}^{N-1}(c).$$

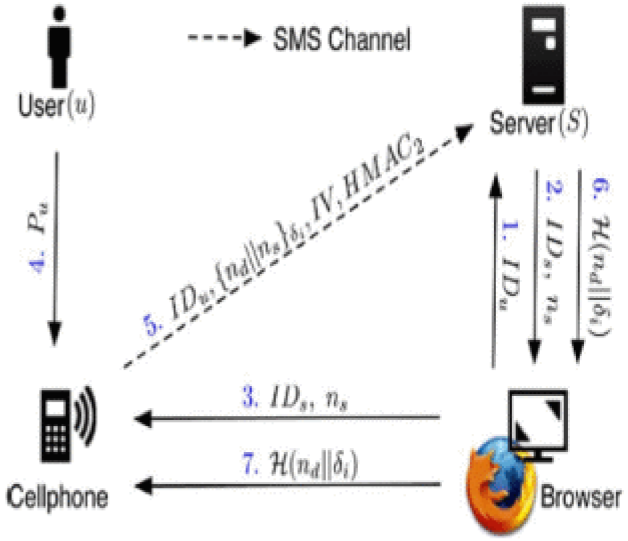

Fig 4. *Procedure of login phase*

ID is only used for this login (the login after user registered) and is regarded as a secret key with AES-CBC. The cell phone generates a fresh nonce. To prepare a secure login SMS, the cell phone encrypts n_s and n_d with δ_i and generates the corresponding MAC, i.e., HMAC. The next action on the cell phone is sending the following SMS message to server:

$$\text{Cell phone} \xrightarrow{SMS} \text{S:ID}_u, \{n_d||n_s\}\ \delta_i, \text{HMAC}_2.$$

Cell phone SMS ID HMAC After receiving the login SMS, the server recomputes to decrypt and verify the authenticity of the login SMS. If the received equals the previously generated, the user is legitimate; otherwise, the server will reject this login request. Upon successful verification, the server sends back a success message through the Internet, $\mathcal{H}(P_u||\ \delta_i)$, to the user device. The cell phone will verify the received message to ensure the completion of the login procedure. The last verification on the cell phone is used to prevent the phishing attacks and the man-in-the-middle attacks. If the verification failed, the user knows the failure of login, and the device would not increase the index. If the user is successfully log into the server, index is able to automatically increased i=i+1, in both the device and the server for synchronization of one-time password. After N-1 rounds, the user and the server can reset their random seed Φ by the *recovery* phase to refresh the one-time password.

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 cell phone, she can launch the program to send a recovery request with her account ID_u and requested server ID_s to predefined TSP through a 3G connection. As we mentioned before, ID_s can be the domain name or URL link of server S. Similar to registration, TSP can trace her phone number T_u based on her SIM card and forward her account ID_u and the T_u to server S

through an SSL tunnel. Once server S receives the request, S probes the account information in its database to confirm if account is registered or not. If account ID_s 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 and replies a message which consists of ID_s, Φ, T_s, i and n_s . This message includes all necessary elements for generating the next one-time passwords to the user u.

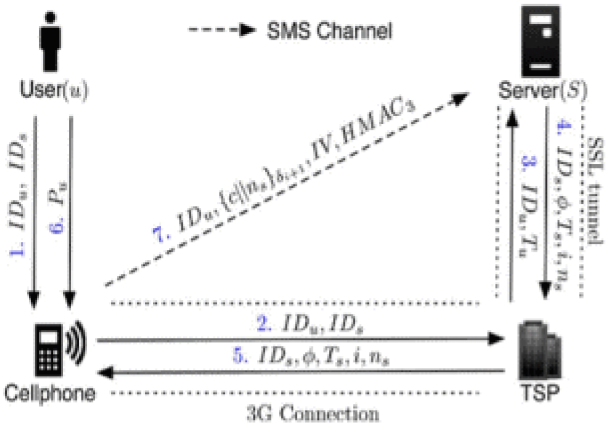

Figure 5. Procedure of recovery phase

When the mobile program receives the message, like registration, it forces the user u to enter her long-term password to reproduce the correct one-time password δ_{i+1} (assuming the last successful login before u lost her cell phone is δ_i). During the last 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 δ_{i+1} and decrypts this message to ensure that user is already recovered. At this point, her new cell phone is recovered and ready to perform further logins. For the next login, one-time password δ_{i+2} will be used for user authentication. Figure. 5 shows the detail flows of *recovery* phase.

V. CONCLUSION

A user authentication protocol named OPass which leverages cell phones and SMS to thwart password stealing and password reuse attacks. We assume that each website possesses a unique phone number. We also assume that a telecommunication service provider participates in the registration and recovery phases. The design principle of OPass is to eliminate the negative influence of human factors as much as possible. Through OPass, 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. 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 cell phones. They can recover our OPass system with reissued SIM cards and long-term passwords.

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] 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] 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.

[5] 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, USENI Association.

[6] 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.