International Journal of Scientific Engineering and Research (IJSER)
www.ijser.in
ISSN (Online): 2347-3878, Impact Factor (2014): 3.05

Web Based Security Analysis of oPass Authentication System Using Mobile Application

Lata Borade[1], Deepak Chaudhary[2]

[1]M.Tech Student IET College, Alwar, Rajasthan, India
[2]Assistant professor of Computer Science and Engineering Dept., Alwar, Rajasthan India

Abstract: ***The main Objective 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.***

Keywords: Phishing, keylogger, 3G-Connection, SMS Channel, OTP

1. Introduction

Given the widespread use of password authentication in on-line correspondence, subscription services, and shopping, there is growing concern about identity theft. When people reuse their passwords across multiple accounts, they in-crease their vulnerability; compromising one password can help an attacker take over several accounts. Passwords are the most commonly used type of authentication on the Web, but they have many usability problems and security weaknesses. Password security depends on choosing passwords that are unique and hard to guess, yet long passwords can be difficult to remember and retype correctly. The passwords that are easiest to choose and memorize tend to be vulnerable to dictionary attacks, in which an attacker tries to guess the password by constructing likely possibilities from lists of words and common passwords. Changing passwords frequently helps to resist attack, but makes the task of memorizing passwords even harder. Using the same password or related passwords at multiple sites compromises password secrecy, yet memorizing a different password for every site imposes an unrealistic burden on human users. Password login forms are also vulnerable to phishing attacks, in which the user is fooled into entering a password at an imitation site. Some of the more sophisticated phishing attacks also corrupt or mimic parts of the browser‘s user interface to mislead the user about a site‘s true identity.

Graphical passwords are an alternative to text passwords, whereby a user is asked to remember an image (or parts of an image) instead of a word. They are motivated in part by the well-known fact that people have superior memorability for images, and the promise of their suitability for small devices such as smart phones. 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.

Humans have difficulty remembering complex or meaningless passwords. Pass Points involves a user creating a five-point click sequence on a background image. Scalable attacks require that the attacker collect sufficient "human computed" data for the target image, which is more costly for systems with multiple images. This

leads to ask whether more scalable attacks exist, and in particular, effective fully automated attacks An attacker may install a malicious program such as a keystroke logger that can observe and modify a legitimate software environment, compromise modifiable software such as the BIOS, or add malicious hardware such as a USB sniffer. Each of these attacks poses password stealing attacks.

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.

2. Existing System

Over the past few decades, text passwords have been adopted as primary means of user authentication for websites. Users select username & passwords while registering on websites. But to log onto that site next time, user has to recall that password.
If the user selects complex password, it can resist brute force & dictionary attacks. But because humans are not good at memorizing strings, most users would choose easy to remember passwords. Another crucial problem is that many users reuse the same password for many sites. Password reuse can cause a great loss because a hacker can compromise a weak site & use the password for other websites. This is

password reuse attack. Various schemes have been suggested till date for User Authentication. It included some Graphical Password Schemes as well.

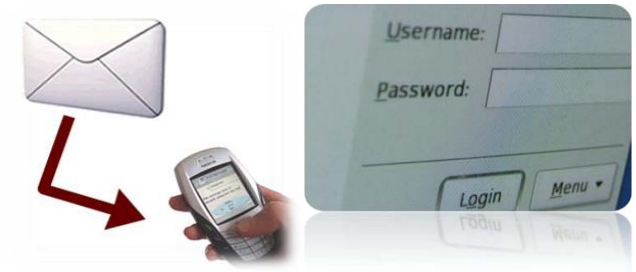
Although it's a great idea, it is not mature enough & is vulnerable to some attacks like guessing, shoulder surfing & spywares. Keylogging or key listening cannot crack them but we are not sure about mouse tracking spywares.

Another alternative to password security is to use Password Management Tools. These tools suggest long complex passwords while registering over websites & store them so that when you login next time, it can fill them automatically. The user just need to remember one Master Password & all other passwords are managed by the software. Some managers even facilitate carrying a copy in flash drives so as to use them on other computers. But users doubt its security & thus feel uncomfortable about using it.

Some researches focus on three factor authentication rather than password based to provide more reliable user authentication. Three factor authentication depends on what you know (e.g. password), what you have (e.g.ID cards) & who you are (e.g. fingerprint or iris).This requires comparatively high cost.

3. Proposed System

oPass is an User Authentication Protocol which leverages a user's cell phone & SMS service to prevent password reuse & password stealing attacks. The main cause why password stealing attacks succeed is because users have to type them in untrusted computers. Therefore, the main concept of oPass is to free users from having to remember or type any passwords into conventional computers for authentication. The user's cell phone is used to generate one time passwords & a new communication channel – SMS is used to transmit authentication messages. Because of one time passwords (OTP) the user is not required to memorize any passwords & there is no problem if the attacker knows this password as the password expires after one login session.



4. Background

oPass adopts the one-time password strategy

4.1. 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 N performing hashes on input c.

$$\delta_0 = \mathcal{H}^N(c). \tag{1}$$

The next one-time password is obtained by performing Hashes

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

Hence, the general formula is given as follows

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

4.2. 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.

4.3 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 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.

5. oPass Architecture

In oPass, a user is required to only memorize one long-term password to access his cell phone. For users to perform secure login on an untrusted computer (kiosk), oPass consists of a trusted cell phone, a browser on kiosk & the server he wishes to log into. The communication between cell phone & web server is through SMS channel. The browser interacts with web server via the internet. In our protocol, we require cell phone to interact directly with the kiosk. The general approach is to select available interfaces like Wi-Fi or Bluetooth.

The main Objective 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.

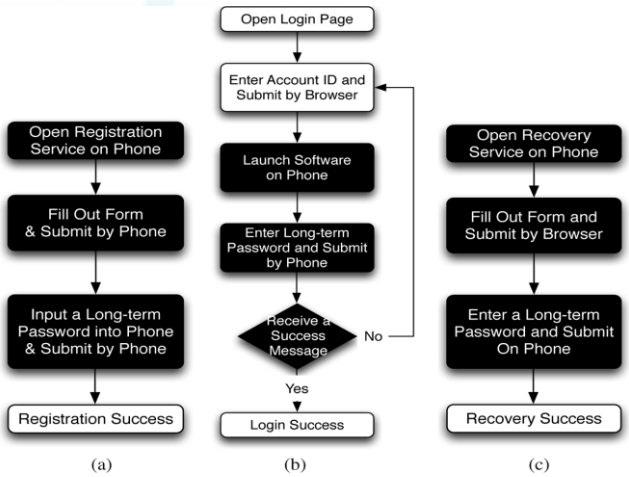
Figure 1: Architecture of oPass system

The assumptions in oPass system are as follows.

1) Each web server possesses a unique phone number via phone number, users can interact with each website through SMS channel.
2) The user's 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 and a web server's ID to start to execute the registration phase. Then, the TSP forwards the request and the subscriber's phone number 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 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.

5.1 oPass

oPass consists of registration, login, and recovery phases. We introduce the details of these three phases respectively. Figure 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. 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.



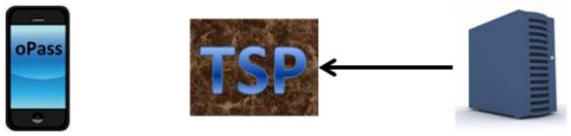
Figur 2: Operation flows for user in each phase of oPass system respectively.

5.2 Registration Phase

The user begins by opening the oPass program on her cell phone. User enters IDu (account id she prefers) & IDs (web site URL) to the program. The TSP plays the role to distribute a shared key (Ksd) between the user & the server. The key is used to encrypt the SMS with AES-CBC. (Advanced Encryption Standard Cipher Block Chaining).

TSP forwards user id (IDu), user number (Tu) & shared key (Ksd) to the server (s). Server generates corresponding

information about the account & replies with server ID (IDs), a random seed ϕ & servers phone number (Ts).



TSP then forwards server ID (IDs), a random seed ϕ, server's phone number (Ts) & a shred key Ksd to user's cell phone.

The user will now set up a long-term password Pu for her cell phone. The phone computes a secret credential c using Pu, IDs & ϕ.The cell phone then encrypts the credential c with key Ksd & generates corresponding MAC i.e. HMAC1.

The cell phone now sends an encrypted registration SMS to server phone number Ts which consists of user ID , c, ϕ, IV & HMAC1. Server decrypts this SMS to obtain c, key Ksd & sends an acknowledgement to user cell phone. In the end, cell phone stores server ID, server number, ϕ & i. _ŕ is current index of OTP. After SMS from above step, server stores user ID, user number, c, ϕ & i. This completes registration.

5.3 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 his cellphone to produce a one-time password and deliver necessary information encrypted with to server via SMS message. Based on pre shared secret credential server can verify and authenticate user based on 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 with account ID. Next, server supplies the ID and a fresh nonce to the browser. Meanwhile, this message is forwarded to the cellphone through Bluetooth or wireless interfaces. After reception of the message, the cellphone 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 regenerate by inputting the correct on the cellphone. The cellphone generates a fresh nonce. To prepare a secure login SMS, the cellphone encrypts and with and generates the corresponding HMAC. The next action on the cellphone is sending the SMS message to server. After receiving the login SMS, the server recompute 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.

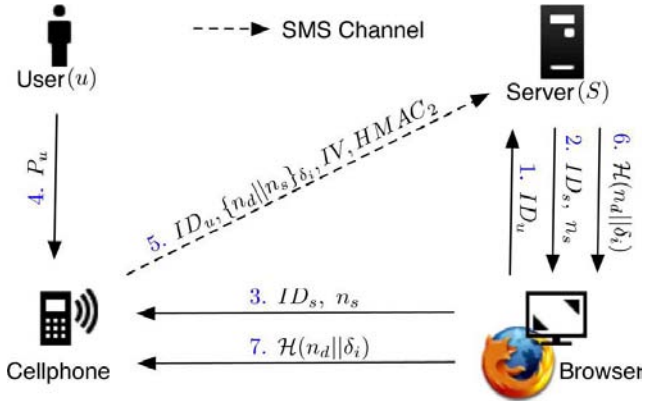


Figure 3: Procedure of login phase

5.4 Recovery Phase

Recovery phase is designated for some specific conditions; For example, a user may lose her cellphone. The protocol is able to recover oPass setting on her new cellphone assuming he 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, he can launch the program to send a recovery request with her account ID and requested server ID to predefined TSP through a 3G connection. As we mentioned before, ID can be the domain name or URL link of server. Similar to registration, TSP can trace her phone number based on her SIM card and forward her account ID and to server through an SSL tunnel. Once server receives the request, probes the account information in its database to confirm if account is registered or not. If account ID exists, the information used to compute the secret credential will be fetched and be sent back to the user. The server generates a fresh nonce and replies a message. This message includes all necessary elements for generating the next one-time passwords to the user .When the mobile program receives the message, like registration, it forces the user to enter her long-term password to reproduce the correct one-time password (assuming the last successful login before lost her cellphone). During the last step, the user's cellphone encrypts the secret credential and server nonce to a cipher text. The recovery SMS message is delivered back to the server for checking. Similarly, the server computes and decrypts this message to ensure that user is already recovered. At this point, her new cellphone is recovered and ready to perform further logins. For the next login, one-time password will be used for user authentication. Fig 4. Shows the detail flows of recovery phase.

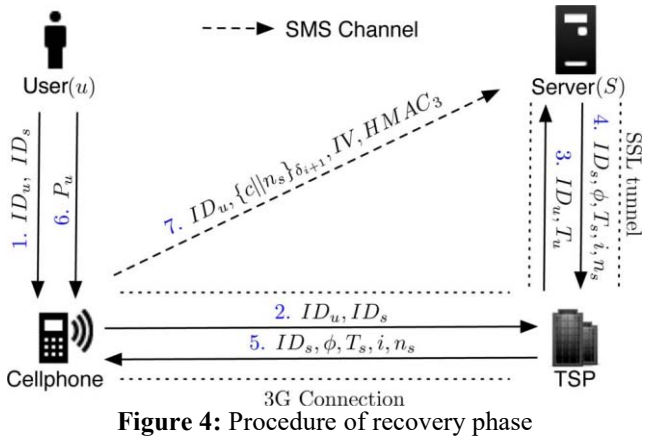


Figure 4: Procedure of recovery phase

6. Security Analysis

An attacker can target user or server side. At user side, he can install malwares or use phishing sites to fetch the passwords. But in oPass, passwords are not entered into browsers. So, oPass resists phishing & malware attacks. At server side, attacker can intercept & manipulate messages to launch SMS spoofing attacks. But as cipher text cannot be decrypted without corresponding secret key & hash function is irreversible, this attack will fail. Also the attacker doesn't know the session key of 3G connection & SSL tunnel. So he cannot derive the secret credential c .If someone steals the cell phone, he can't login as he doesn't know the long-term password setup by user.

6.1 Threat Model

Attackers can intercept, eavesdrop, and manipulate any message transmitted over the Internet and other wireless networks. The attacker can also spoof an SMS to cheat websites. The computer which a user uses to log into websites is considered untrusted. Attackers can install malwares and setup a backdoor to collect a user's sensitive information (e.g., passwords).The attacker's goal is to masquerade itself as a legitimate user and to gain access to websites without being detected.

6.2. Attacks on Registration

The main task of the registration phase is to generate a shared credential for computing one-time passwords between users and websites. The shared credential should be kept secret to guard oPass from attacks. To prove the guaranteed secrecy of credential in the registration phase.

6.3. Attacks on Recovery

Potential threat in the recovery protocol is whether an attacker who stole a user's cellphone can succeed in guessing the correct long-term password. This attack is referred to as the password guessing attack. The attacker may try to guess the user's to compute the one-time password for login. He only has to masquerade as a normal user and execute the recovery procedure. After receiving the message from the TSP, the attacker enters a guessed and computes a candidate one-time password. The attacker then transmits a login SMS to the server. However, the attacker has no information to confirm whether or not the candidate is correct. Therefore, the protocol prevents a password guessing attack.

7. Conclusion

oPass protocol has a very high level of security. In this paper, we proposed a user authentication protocol named oPass which leverages cellphones 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 her cellphone. Users are free from typing any passwords into untrusted computers for login on all websites.

To make oPass fully functional, password recovery is also considered and supported when users lose their cellphones. They can recover our oPass system with reissued SIM cards and long-term passwords.

A prototype of oPass is also implemented to measure its performance. The average time spent on registration and login is 21.8 and 21.6 s, respectively. According to the result, SMS delay occupies more than 40% of total execution time. The delay could be shorter by using advanced devices. Besides, the performance of login of oPass is better than graphical password schemes, for example, Passfaces. The login time of Passfaces is from 14 to 88 s, which is longer than oPass. Therefore, we believe oPass is acceptable and reliable for users. To analyze oPass's usability, we invited 24 participants to conduct the user study. Most participants could easily operate all procedures of the oPass system. 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. Certainly, some of the participants prefer oPass to the original system.

8. Scope

oPass consists of registration, login, and recovery phases. Unlike generic web logins, oPass utilizes a user's cellphone as an authentication token and SMS as a secure channel. In the registration phase, a user starts the oPass program to register his new account on the website se 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.

References

[1] Hung-Min Sun, Yao-Hsin Chen, and Yue-Hsun Lin —Opass: A user authentication protocol resistant to Password stealing and reusing attacks." IEEE TRANSACTIONS ON INFORMATION FORENSICS

AND SECURITY, —Passwordmanagement strategies for online accounts," in OL. 7, NO. 2, APRIL 2012
[2] B. Ives, K. R. Walsh, and H. Schneider, —Thedomino effect of password reuse," Commun. ACM, vol. 47, no. 4, pp. 75–78, 2004.
[3] S. Gawand E. W. Felten, SOUPS '06: Proc.2nd Symp. Usable Privacy. Security, New York, 2006, pp. 44–55, ACM.
[4] 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.
[5] S. Chiasson, A. Forget, E. Stobert, P. C. van Oorschot, and R. Biddle, —Multiplepassword 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, —Thedesign and analysis of graphical passwords," in SSYM'99: Proc. 8th Conf. USENIX Security Symp., Berkeley, CA, 1999, pp. 1–1,USENIX Association.
[7] B. Pinkas and T. Sander, —Securingpasswords against dictionary attacks," in CCS '02: Proc. 9th ACM Conf. Computer Communications Security, New York, 2002, pp. 161–170, ACM.
[8] J. A. Halderman, B. Waters, and E. W. Felten, —A convenient method for securely managing passwords," in WWW '05: Proc. 14th Int. Conf.World Wide Web, New York, 2005, pp. 471–479, ACM.
[9] P. van Oorschot, A. Salehi-Abari, and J. Thorpe, —Purely automated attacks on passpoints-style graphical passwords," IEEE Trans. Information Forensics Security, vol. 5, no. 3, pp. 393–405, Sep. 2010.
[10] L. O'Gorman, —Comparing passwords, tokens, and biometrics for user authentication," Proc. IEEE, vol. 91, no. 12, pp. 2021–2040, Dec. 2003.
[11] L. Lamport, —Password authentication with insecure communication," Commun. ACM, vol. 24, pp. 770–772, Nov. 1981.
[12] H. Gilbert and H. Handschuh, —Securityanalysis of SHA-256 and sisters," in Selected Areas Cryptography, 2003, pp. 175–193, Springer.[30] TS 23.040: Technical Realization Short Message Service (SMS) 3GPP
[13] M. Bellare and C. Namprempre, —Authenticated encryption: Relations among notions and analysis of the generic composition paradigm," Advances Cryptology—ASIACRYPT 2000, pp. 531–545, 2000.
[14] 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.
[15] M. Mannan and P. van Oorschot, —Usinga personal device to strengthen password authentication from an untrusted computer," Financial Cryptography Data Security, pp. 88–103, 2007.
[16] R. Biddle, S. Chiasson, and P. van Oorschot, —Graphical passwords: Learning from the first twelve years," in ACM Computing Surveys,Carleton Univ., 2010