Open access Journal International journal of Emerging Trends in Science and Technology

Web Based Security using oPass System: A Survey

Authors
Ms.Bhosale Akshaya A.[1], Mr.Singh R.B[2]

[1]Sinhgad Institute of Technology, Pune Univeristy
Lonavala,India
Email: *akshaya.bhosale@gmail.com*

[2]Sinhgad Institute of Technology,Pune University
Lonavala,India
Email:*Rase69@gmail.com*

Abstract:
Password authentication is an essential form of user authentication both on the Internet and for internal organizational computing systems. Password protection schemes are used to protect relatively low-sensitivity systems such as access to online archives as well as highly sensitive corporate intranets or personal bank accounts. 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. 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.
Keywords: about four key words separated by commas.

1. Introduction

The text password is the most popular form of user authentication on websites due to its simplicity. User's passwords are liable to be stolen under different threats and vulnerabilities. A variety of technologies are introduced to reduce the negative effect of human factors in the user authentication procedure [1]. To do so many graphical password schemes are designed. Password management tools are designed as an alternative for graphical password scheme [1] [6]. These tools automatically generate strong passwords for each website which solves the problem of password reuse and password recall [4] [9]. Three–factor authentication is introduced to provide more reliable user authentication. It depends on what you know (password), what you have (token), and who you are (biometric) [3]. In this scheme user must input a password and provide a pass code generated by the token, and scan his/her biometric features [8]. This scheme prevents users from password stealing attacks, but it requires high cost. Therefore two-factor authentication is introduced which also suffer from negative effect of human factors. In this scheme user have to memorize another four-digit PIN code to work together with token. Here a user authentication protocol called oPass is proposed which uses user cell phone and short message service (SMS) to prevent password stealing and password reuse attacks [5]. The oPass protocol uses user cell phone and short message service (SMS) to prevent password sealing and password reuse attacks [7]. The main concept of oPass is free user from having to remember or type password into untrusted public computers. 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.

2. oPass Architecture

The oPass system consists of a trusted cell phone, a browser on the kiosk, and a web server that users wish to access. The communication between web server and cell phone is through the SMS channel.

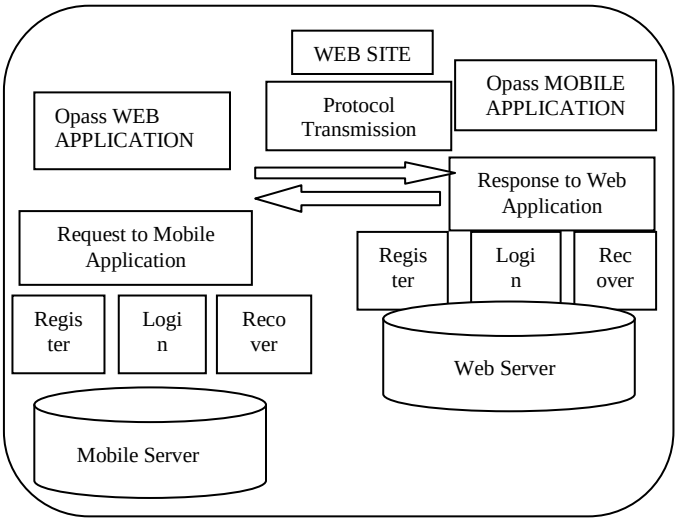

Figure 1.oPass Architecture

Here the web browser interacts with web server via internet.
Following assumptions are made in oPass system:-

1. Each web server must have unique phone number with help of which user can interact with website through SMS.
2. User's cell phone is virus free so that user can insert his/her LTP safely.
3. For registration and recovery telecommunication service provider will play important role. The TSP works as bridge between subscriber and web servers.
4. User connects to the TSP via 3G connection for transmission protection.
5. The TSP and web server establish a secure sockets layer protocol through which the TSP can verify the server by its certificate to prevent phishing attack.
6. If a user loses her/his cell phone, he/she can notify TSP to disable his/her lost SIM and apply for new car with same phone number.

3. Flow of Process

The oPass protocol consists of three phases, registration phase, login phase and recovery phase. In registration phase user starts the oPass program to register on new website. The server request user to set his/her long term password which is used to generate one time password. Recovery phase fixes some problems like losing one's cell phone.

3.1 Registration Phase

The aim of this phase is to allow a user and a server to negotiate a shared secret to authenticate logins for this user. The user begin by opening oPass program on his/her cell phone after that he/she will enter account id and website url. After receiving account id and website url TSP trace user's phone number. The TSP also distributes a shared key Ksd between user and server.
In this phase the cell phone computes a secret credential c by following formula:-

$$C=H(Pu \| IDs \| \phi) \ldots\ldots\ldots\ldots\ldots\ldots (1)$$

For secure registration SMS, the cell phone encrypt the computed credential c with the key Ksd and generates the MAC. The cell phone sends an encrypted registration SMS to the server by phone number.

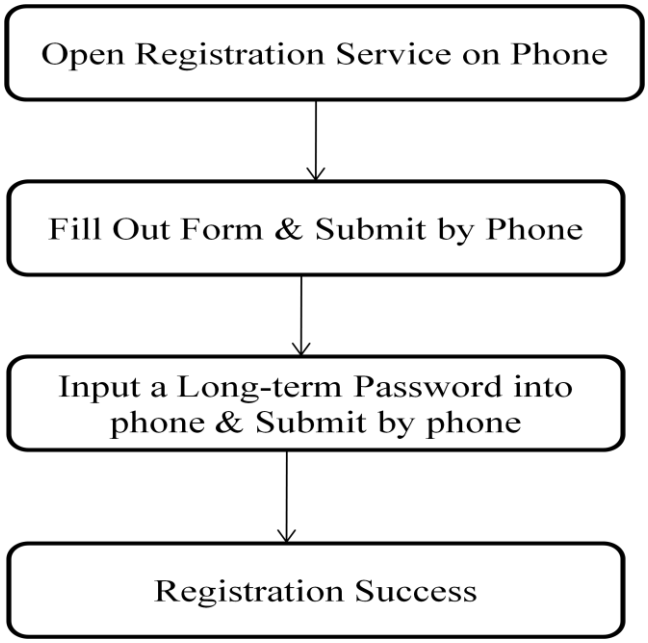

Figure 2.Registration Phase [2]

3.2 Login Phase

In this phase user send request to the server for accessing his/her account on web site. In this phase user uses his/her cell phone for one time password (OTP) generation.
When user start performing login on their favorite web site the browser send that request to the web server along with user identity (IDu). After that server send its own identity (IDs) and nonce (ns) to the cell phone along with Ts, Φ, i. At the same time user have to insert his/her LTP on cell phone which will generate credential c which is used for producing OTP for current login.

$$\delta i=H^{N-i}(C) \ldots\ldots\ldots\ldots\ldots\ldots (2)$$

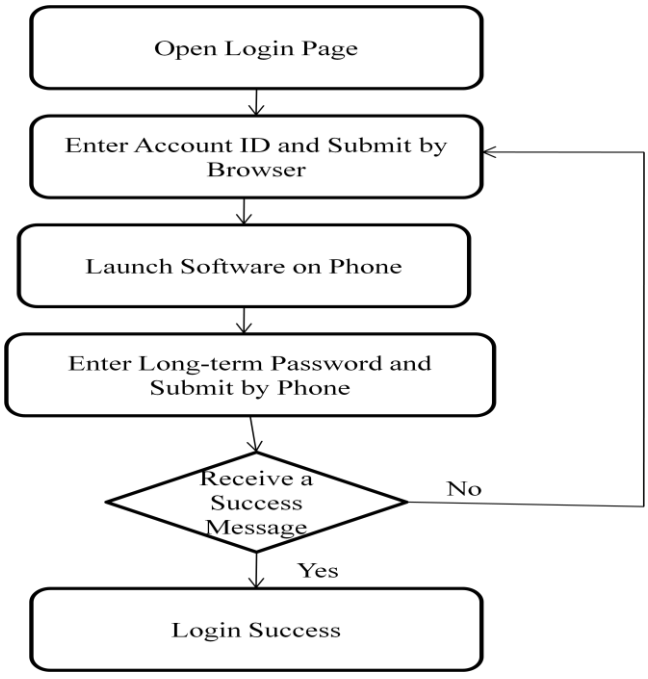

Figure 3: Login Phase [2]

3.3 Recovery Phase

This phase is designed for the condition in which if user loss his/her cell phone.

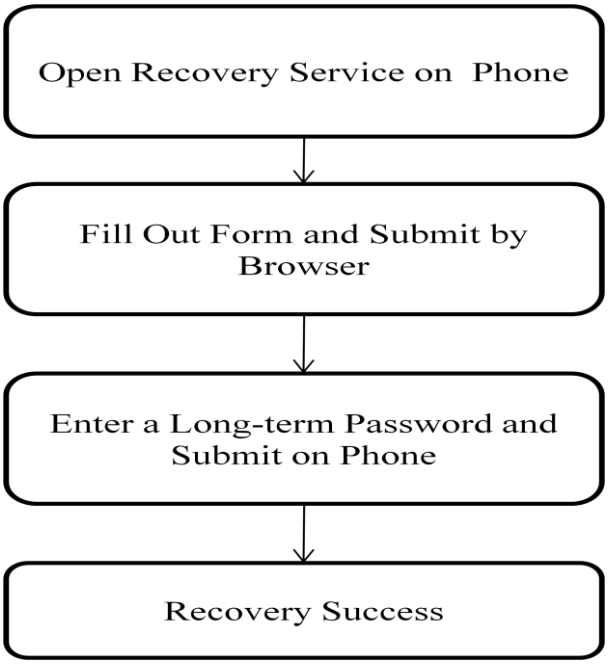

Figure 4: Recovery Phase[2]

In this phase we are going to assume that user loss his/her cell phone and he/she is going to use same number for new cell phone and after getting same mobile number there is no need for user to again do registration for same web site he/she just have to perform steps for recovery . After installation of oPass system on new cell phone user will send recovery request to the server.

4. Equations

In registration phase credential C is required which is generated using (Pu,IDs, ϕ) as input

$$C=H(Pu\| IDs\| \phi)$$

Then registration SMS is encrypted using (C,IDu,Ksd, ϕ,IV,HMAC1) as input

$$\text{Cellphone} \longrightarrow \text{S:IDu,}\{C\|\phi\}Ksd,IV,HMAC1 \ldots..(3)$$

In login phase OTP δi is generated using credential C as input

$$\delta i=H^{N-i}(C)$$

Then login SMS is encrypted using (Idu, ns, nd, δi, IV, HMAC2) as input

$$\text{Cellphone} \longrightarrow \text{S:IDu,}\{nd\|ns\}\delta i,IV,HMAC2 \ldots..(4)$$

References

[1] I. Jermyn, A. Mayer, F. Monrose, M. K. Reiter, and A. D. Rubin, "The design and analysis of graphical passwords," in *SSYM'99: Proc. 8th Conf. USENIX Security Symp.*, Berkeley, CA, 1999, pp. 1–1, USENIX Association.

[2] Hung-Min Sun,Yao-Hsin Chen and Yue-Hsun Lin, "oPass:A User Authentication Protocol Resistant to Password Stealing and Password Reuse Attacks", *IEEE Trans. InformationForensics Security*, vol. 7, no. 2, April. 2012.

[3] B. Blanchet, "An efficient cryptographic protocol verifier based onprolog rules," in *Proc. 14th IEEE Computer Security FoundationsWorkshop*, 2001, pp. 82–96.

[4] L. O'Gorman, "Comparing passwords, tokens, and biometrics for user authentication," *Proc. IEEE*, vol. 91, no. 12, pp. 2021–2040, Dec. 2003.

[5] B. Ives, K. R. Walsh, and H. Schneider, "The domino effect of password reuse," *Commun. ACM*, vol. 47, no. 4, pp. 75–78, 2004.

[6] S. Gaw and 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.

[7] 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.

[8] 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.

[9] P. van Oorschot, A. Salehi-Abari, and J. Thorpe, "Purely automated attacks on passpoints-style graphical passwords," *IEEE Trans. InformationForensics Security*, vol. 5, no. 3, pp. 393–405, Sep. 2010.

[10] K.-P. Yee and K. Sitaker, "Passpet: Convenient password managementand phishing protection," in *SOUPS '06: Proc. 2nd Symp. Usable Privacy Security*, New York, 2006, pp. 32–43, ACM

Author Profile

Ms. Akshaya A. Bhosale is graduated in Information Technology from Mumbai University,Maharashta, India in 2009 and is pursuing Master's Degree in ComputerEngineering from Sinhgad Institute of Technology.Her area of interest is Web Security and Database.She has published 2 International Journal Papers.

Mr. R.B. Singh is graduated in Computer Engineering from Amravati University (M.S.), India in 1992 and is post graduate in Computer Engineering from Dr.B.A.T.U.,Lonere,Maharashtra, India.His area of interest is Mobile Ad-hoc Network. He has published 2 International Journal Papers.