Web Based Security using Online Password Authentication in Mobile Application

A. T. Bhole[1], Sheetal Chaudhari[2]

[1]Associate Professor, SSBT's College of Engineering & Technology, North Maharashtra University, Bambhori, Jalgaon, India
PG Student, SSBT's College of Engineering & Technology, North Maharashtra University, Bambhori, Jalgaon, India

Abstract: ***The internet has one of the most convenient and widely used media for people for exchanging information and to do business over the internet. E.g. Accessing web based emails, online auction or banking sites. But now a day's accessing the internet is faced with many challenges. One of the most popular challenges is to ensure security with vital role to provide security in websites. Text password is a convenient and simplest form for a user authentication on websites, and it is level to security attacks. User mostly used weak password and it is often used across several websites and reuse password by typing into untrusted websites causes password threats. Hackers launch password stealing methods to grab password such as phishing, malware, and key loggers. The proposed system is a user authentication protocol named LOPass which creates long term password and one time password for authenticating the user. It uses three phases as registration, login and recovery phase. Here random password is generated for each login. Registration is used to register the user. Recovery phase is used, if the user's mobile phone gets lost. The user needs remember only his long term password which has been stored in database very secretly and securely.***

Keywords: Network security, User authentication, Long Term Password, One Time Password, LOPass.

1. Introduction

As a few days earlier, text passwords have been used for the authentication process. Users choose their passwords which can be easily remembered. Generally, password based user authentication can oppose brute force and dictionary attacks if the user choose the strong passwords. But, users have problem in memorizing the text passwords. Users select the weak passwords even if they know the password might be not safe. The important 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. The problems are caused due to negative influence of human factors. When designing a user authentication, the important consideration is human factors. Since humans are adept in remembering graphical passwords than text password [4]. 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 passwords reuse and recall problems. Users only have to remember a master password for accessing the tool. 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 [5] users have trouble using these tools due to the lack of security knowledge.

Here user authentication protocol as LOPass is designed to solve these problems that occur at the time of user authentication. In this protocol requires the user mobile phone for accessing the application. It generates the long term password and one time password. By using the long term password, mobile phone is secured by the theft. And one time password is used to perform a secure login. Due to this methods used for stealing accounts by using phishing, malware, and eavesdroppers are protected.

2. Problem Description

2.1 Weak Password

Regarding the weak password problem, user selects the password by them. So user creates the weak passwords because of easy to remember. Also user uses these same passwords across the various website. That means it reuses the same password across the website. Password reuse is also the various serious problems. Hackers can easily steal the password because the user use same password through various websites and also used weak password. By using phishing attacks [5] hackers steals very sensitive information of user.

2.2 Recall problems

Users are not good in memorizing the complex text passwords. In some websites the random generated passwords are available for authentication but the users have recall problem. Even though, the users change their passwords periodically has a crucial problem. People use their username and password to access websites for login purpose. User must recall their passwords. Usually password based authentication resist brute force and dictionary attacks if users select strong password. But, the major problem is that humans are not expert in memorizing text passwords. User selects their password which can be easily remembered even though the password is unsafe. Then password reuses across several website causes lose of sensitive information. This is to be password reuse attack [6].

Humans are expert in memorizing graphical password than text password. But still has recall problem. Even though it provides strong password, still it is vulnerable to several attacks. Graphical password and management tool is easy to remember. It has a disadvantage that poor knowledge about security. In two factor authentication, user must remember pin code to work with a token. It doesn't work if user forgets

to bring their tokens like smart card, credit card etc. Graphical passwords can be easily remembered by user than text password. Although, it is great idea but not mature enough to implement in practice. Password management tool works well but have trouble due to lack of knowledge about it.

3. System Architecture

User authentication protocol LOPass, designed to generate different random passwords for each login to avoid recall problems and password reuse problems for the users. The figure1 shows the architecture of LOPass.

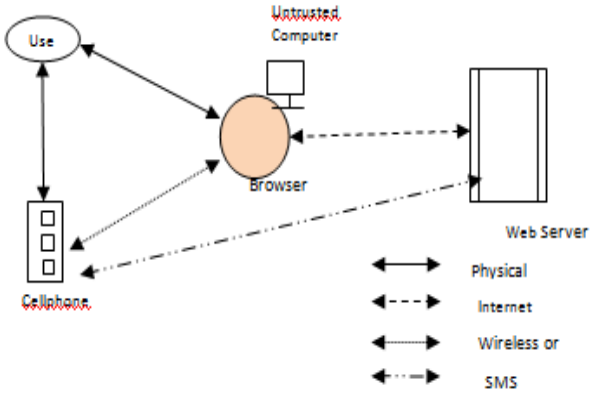

Figure 1 Architecture of LOPass

A protocol LOPass requires the only user's unique mobile number. LOPass generates random one time passwords for each login. There three phases are involved in the authentication protocol such as Registration, login and Recovery phase with the help telecommunication service provider(TSP).In the registration phase , user must provide their personal information with unique phone number. This personal information is stored into the database with the encrypted format and that used for further process. Providing user information user can be register for the application. Also user must register himself by starting LOPass program on their mobile. After this user will get the one long term password which is also stored in the database in the encrypted format. In login phase, user need t o provide the only the username as input to the system. User get random one time password generated by the web server after providing the long term password in mobile application. This one time password are created by using hash algorithm and stored in encrypted format. In the recovery phase, if user lost his mobile then the protocol is able to recover the user setting for the new phone. Setting can be recovered by using two things such as mobile number and long term password.

3.1 Registration phase

1. User enters user id and server id.
2. Cellphone transmit this info to TSP.
3. TSP transmit user id, user phone no and shared key to server.
4. Server generates secure info and send to TSP.
5. TSP sends server information with shared key to Cellphone.
6. User enter long term password.
7. Cell phone compute secret key and generate secured registration message and sent it to server for verify the authenticity.

3.2 Login Phase

1. Browser sends user request to server
2. Server checks information with database and generate fresh nonce.
3. Then this message pass to Cellphone
4. User enter long term password.
5. One time password is generate for current login and Cellphone generate nonce and secure login SMS.
6. Server check and verify the authenticity of login SMS.
7. Server send successful login message to Cellphone through Internet.

3.3 Recovery Phase

1. User enters user id and server id.
2. Cellphone transmit this info to TSP.
3. TSP transmit user id, user phone no and shared key to server.
4. Server checks for existence and generates fresh nonce and replies this message to TSP.
5. TSP sends server information to Cellphone.
6. User enter long term password.
7. Cellphone compute secret key and generate one time password and prepared secured recovery message and sent it to server for verify the authenticity.

4. Implementation

The prototype contains three processes 1) a program running on mobile phones for receiving SMS 2) the link between client and server through GSM modem and 3) the interface between the browser and the client using TCP/IP connection.

The LOPass generated password is encrypted for data confidentiality. After installing program, a user creates their accounts in websites during registration. Once the registration is successful a user can log into website securely through the LOPass. During registration, the details about the users need to be filled with secret long term password that is stored in the database. For login, SMS will be received by the user with encrypted random password. If it matches with the data stored in the database it allows the user to authenticate.

4.1 Client Program

An android program is developed and installed on the mobile phone to generate the long term password and one time password. Client program developed by using Visual .Net with Xamarin studio, which is used as for developing android and IOS, based application.

The program has been established on a Micromax A110 phone. The program can run on any android based mobile phone. For safety operation, fundamental information of LOPass is keep the safe in an encrypted in Microsoft SQL database with encrypted key. After installing the program, a user creates an account to a website via the registration phase. Upon the successful registration, the user can log into

the website. To make program smooth, the user only has to key in his long term password and select a website. Then the remaining operation would perform by the program through clicking a button.

4.2 Server Program

In the web server implementation, we developed a server program which consists of main server codes (VS.net with C#) and scripts for database (Microsoft SQL). Server program can be installed and performed on an UltiDev server.

4.3 Database Design

A database is needed on the server side to store the client's identification information such as the username, customer id, customer name, pin, password, IMSI number, unique symmetric key, and the mobile telephone number for each user. The password field will store the hash of the 10 minute password It will not store the password itself. Microsoft SQL is used as a back-end database

5. Discussion

Number of authors has developed system to protect user information from the phishing attacks in user authentication. These previous developed schemes use variable technologies, e.g. mobile devices, trusted platform module or public key infrastructure. However these solutions are not good for the negative influence of human factors, such as password reuse and weak password problems. Our user authentication protocol is compared with these previous schemes or protocol. The result is shows that LOPass user authentication is more reliable and more easily operable solution for the problem. Also it works in fewer requirements but provide the better security. Table 1 and Table 2 show the comparisons of LOPass with the some previous schemes. In table 1, 'yes' means attacks solved and 'no' means not provide to attacks. In Table 2, 'yes' means that schemes needs to be external requirements.

Table 1: Attacks prevent by Schemes

	Attacks Prevention			
Scheme	*Phishing*	*Keylogger*	*Password reuse*	*Sniffing*
LOPass	Yes	Yes	Yes	Yes
Wt. Token[10]	Yes	Yes	No	
Full proof [11]	Yes	Yes	No	
Bite		Yes	No	
MP-Auth [12]	Yes	Yes	No	Yes
Session Magnifier		Yes	No	Yes

Table 2: External Requirements for Schemes

	Requirements			
Scheme Name	*UICC*	*Physical Account Setup*	*Logical Account Setup*	*TPM*
	-1	*-2*	*-3*	*-4*
LOPass			Yes	
Wt. Token	--	Yes	--	--
Full proof	Yes	Yes	--	--
Bite	--	No	--	Yes
MP-Auth	Yes	Yes	No	--
Session Magnifier	--	No	--	--

	Requirement		
Scheme Name	*On-Device secret -5*	*Trusted Proxy -6*	*Malware free mobile -7*
LOPass		Yes	Yes
Wt. Token	Yes	Yes	Yes
Full proof	Yes	--	Yes
Bite	Yes	--	Yes
MP-Auth	--	--	Yes
Session Magnifier	Yes	--	Yes

6. Conclusions

In this paper, a user authentication protocol LOPass uses a user's mobile phone and SMS to prevent from password hacking and password stealing. In LOPass the users need only remember the long term password to secure to each login. Every time random one time password is created by the using the long term password. This one time password is used for each login. For every login it creates new one time password. The main thing is that the users are free from typing the passwords in untrusted computers. When compared with other schemes, LOPass is more secure because the generated password is valid for that particular session alone.

7. Acknowledgment

We would like to thank our Institution and faculty members, without whom this Paper would have been a distant reality. Last but not the least, we would also like to thank to our friends for listening to our ideas, asking questions and providing feedback and suggestions for improving our ideas.

References

[1] B.Ives, K.R,Walsh and H.Scheider, "The domino effect of password reuse", Communication ACM,vol47,no.4,pp.75-78,2004.

[2] S GAW and E W Felten, "Password management strategies for online accounts", SOUPS '06 proc.2nd Symp. Usable Privacy Security, New York, 2006, pp.44-55, ACM.

[3] D. Florencio and C. Herley, "large-scale study of web password habits", in *WWW: Proc. 16th Int. Conf. World Wide Web., ACM*, pp. 657–666, 2007.

[4] S.Chiasson, A.Forget, E.Stobert,P.C. van Oorschot, and R.Biddle, "Multiple password interferences in text passwords and click based graphical passwords," in CCS/09: proc.16th ACM Conf .Computer Communications Security,NewYork,2009,pp.500-511,ACM.
[5] K. P. Yee and K. Sitaker, "Passpet: Convenient password management and phishing protection", in *SOUPS: Proc. 2nd Symp. Usable Privacy Security*, *ACM*, pp. 32–43, 2006.
[6] 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 Information Forensics and Security*, vol. 7, no. 2, pp.651-663, April 2012.
[7] Do van Thanh, Tore Jønvik, Boning Feng, "Simple Strong Authentication for Internet Applications using Mobile Phones", in *IEEE*, 2008.
[8] Mohammed Alzomai Audun Josang, "The Mobile Phone as a Multi OTP Device Using Trusted Computing", *Proceedings of the Fourth International Conference on Network and System Security, IEEE Computer Society*, pp. 75-82, Oct. 2010.
[9] T. Venkat Narayana Rao, Vedavathi K, "Authentication Using Mobile Phone as a Security Token",*IJCSET*,Vol 1, Issue 9, pp. 569-574, Oct. 2011.
[10] M.Wu, S. Garfinkel, and R. Miller, "Secure web authentication with mobile phones", in *DIMACS Workshop Usable Privacy Security Software*, *Citeseer*, 2004.
[11] B. Parno, C. Kuo and A. Perrig, 2006, Phoolproof phishing prevention, Financial Cryptography Data Security, pp. 1–19.
[12] 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.

Author Profile

Sheetal Chaudhari was born in Jalgaon, She received the B.E degree in computer Engineering in SSBT's College of Engineering, Jalgaon in 2003 and currently pursuing M.E. degree in computer Science and Engineering in North Maharashtra University, Maharashtra. Her research interests are in Network Security.