International Journal of Latest Trends in Engineering and Technology
IJLTET Special Issue- ICRACSC-2016 , pp.056-062
e-ISSN:2278-621X

OPASS: AN IMPROVED USER AUTHENTICATION METHOD FOR ONLINE TRANSACTIONS

B. Saritha[1] and N.Sabitha[2]

Abstract - Most systems today rely on user name and password as main credentials for all web applications. And many users are using password in the web applications as static passwords to verify the user's identity. However, such passwords come with major management security concerns. Usually users have tendency of selecting weak passwords and reuse the same for more websites . This reusing of password creates chain reaction when an opponent learns one password ,it will be used by her to gain access to rest of all concerned websites. Secondarily, entering password in suspicious systems results in threats of password stealing. A hacker can use various password stealing methods such as surfing, spooling , sniffing , guessing, malware, keyloggers etc. thus there is the clear need of maintenance of security in all web applications in mobiles. Traditionally text password is in practice and nowadays we are experiencing graphical passwords which is not implemented fully, biometric which are expensive . In this paper we have designed an improved user authentication method using Opass technique to avoid the problem of security in Andriod based mobile phones. This app controls the user's mobile phoneand SMS's to obstruct the intruders from stealing the passwords and also avoids reuse attacks. As we know Opass requires each mobile phone user is assigned an unique phone number registered with a specific Telecommunication services provider , is used for recovery. Here user need to install the application in their android based mobile phone for registration process. through this updated Opass ,users only need to remember is a long term password for loging into all websites. After the transaction of authentication phase is completed with out any clutches ,we believe that the improved Opass is efficient.

I. INTRODUCTION

In the ever changing world of global data communications, inexpensive Internet connections, and fast-paced software development, security is becoming more and more of an issue. Security is now a basic requirement because global computing is inherently insecure. Network security technologies protect your network against the theft and misuse of confidential business information and guards against malicious attacks from Internet borne viruses and worms. Without network security in place your company risks unauthorized intrusions, network downtime, service disruption, regulatory noncompliance and even legal action[3].Network security has become a requirement for businesses, especially those that rely on the Internet. Your customers, vendors and business partners probably expect you to protect any information they share with you. While network security has almost become a prerequisite to running a business, it also pays off in multiple ways[4]. There is a huge transformation in user authentication over the decades from Text Based passwords to graphical and bio-metric passwords, depending on the level of security required[5]. The advancement in technology has helped in both directions to protect users data by strong encryption techniques, while on the other side finding methods to access users data from the perspective of attackers or intruders .Text based password have been implemented as the primary mean of user authentication for websites. User selects username and text passwords when registering accounts on a website. User can log into the website successfully only up on providing the correct passwords [6]. Generally, password based user authentication can resist brute force and dictionary attacks if users select strong passwords to provide sufficient information. However, it has a major problem of memorizing text strings. As a solution user chooses easy-to-remember passwords (i.e., weak passwords) or reuse passwords across various websites [6- 8]. Many graphical password schemes were designed to address user's password recall problem [9]. Although graphical password is a great idea, it is not yet mature enough to be widely implemented in practice [10-11] and is still vulnerable to several attacks [12-13]. Adversaries steal or compromise passwords and impersonate users' identities to launch malicious attacks, collect sensitive

[1] *Department of Computer Science and Engineering, MVSR Engineering College, Nadergul, Hyderabad,Telengana,India*
[2] *Department of Computer Science and Engineering, MVSR Engineering College, Nadergul, Hyderabad,Telengana,India*

information, perform unauthorized payment actions, or leak financial secrets. Phishing is the most common and efficient password stealing attack. 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 SecureID [15]), and scan her biometric features (e.g., fingerprint or pupil). Three factor authentications 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. And recently most of the premium/local banks are offering online solutions to their customers which are making it easier to make online transactions from any place. To access such solutions, the user follows a process: customer has to register, customer needs to opt for the respective service from the bank, register for the same through the online portal of the respective bank [15-16]. The drawback of such a system is once if the credentials (username/passwords) were stolen, anyone can make use of the details to get execute the online transactions. To avoid these problems some premium banks came up with two way authentication solutions, which involves regular username/password authentication followed by the approach of One Time Password(OTP). One Time Password is the method which involves second level of authentication by sending a OTP as a message to the registered customers mobile number. User uses this One Time Password to complete the second level of authentication to make this transaction more secure. 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. In this paper, we propose a user authentication approach named OPass which leverages a user's mobile phone and short message service (SMS) to prevent password stealing and password reuse attacks .Unlike generic user authentication, OPass involves a new component, the mobile phone, which is used to generate one-time passwords and a new communication channel, SMS, which is used to transmit authentication messages.

A. GSM MODEM BACKGROUND

OPass adopt the one time password strategy, here also described GSM modem which is acting as a web server. Here client interact with GSM modem.

GSM MODEM:

GSM modem is a specialized type of modem which accepts a SIM card, and operates over a subscription to a mobile operator, just like a mobile phone. From the mobile operator perspective, a GSM modem looks just like a mobile phone. Importing the comm Driver and connecting the Modem to the PC with serial port.

B. OTP GENERATION:

After entering the correct details from browser and correct long term password from mobile, one time pass word is generated now. OTP is the string of characters consisting of small and capital alphabets, numeric values from 0 to 9 and finally special symbols. From the above all group of characters server will generate OTP with any six characters. With this OTP string MD5 algorithm will generate digital signature. From that digital signature, sub string of 8 characters are considered to avoid complexity.

C. PROBLEM DEFININATION AND ASSUMPTION

Most systems today rely on user name and password as main credentials for all web applications. And many users are using password in the web applications as static passwords to verify the user's identity. However, such passwords come with major management security concerns. If the user have chance to select or create password and user name , user may select weak password and reuse the same password in multiple accounts, write the passwords or store them on their machines, etc. Thus intruders can steal passwords by using several techniques such as shoulder surfing, snooping, sniffing, guessing, etc. Text password is simple to implement ,practically it is not a strong secure as it has lot of problems while creating and using for the above all attacks. Compared to the above mentioned method, biometric is good but it is expensive, therefore it not opted in every places. Today new technique is graphical passwords, but it is not implemented fully. User clearly needs more security to use the web applications. In this application to avoid all above problems we are describing one Android application which is " An improved user authentication method for online transactions " to handle man in middle attack, phishing attacks etc.. In this applications user don't need to use unsafe browsers to register a particular site, instead user can install one android app in his/her mobile set. And then users mobile will receive a long term password to proceed with next step : login process. During this process of login , user have to enter two details through browser like user name and URL, and then it will ask for long term password from mobile. After entering the long term password from mobile it will receive one OTP. That OTP has to be entered into the browser, this is verified in the server , if the entered OTP is correct it will process user request otherwise it will be rejected .

D. Assumptions

Fig.1 describes the architecture of the an improved OPass system. For users to perform secure login on untrusted computer, this method contains a trusted mobile phone, a browser on the computer, and a web sever that users wish to access. The user operates user mobile 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 done through the SMS channel. The web browser interacts with the web server via internet. In our application, we required the cell phone interacting directly with the browser.

The assumptions in an improved Opass system are as follows

1. Here we are considering GSM modem as web server.

2. Each GSM modem possesses a unique phone number (SIM). Via this phone number user can interact website through SMS channel.

3. Here user's phone is malware free, so users safely can type long term password into cell phone.

4. GSM modem will participate in registration, login and recovery password scenarios.

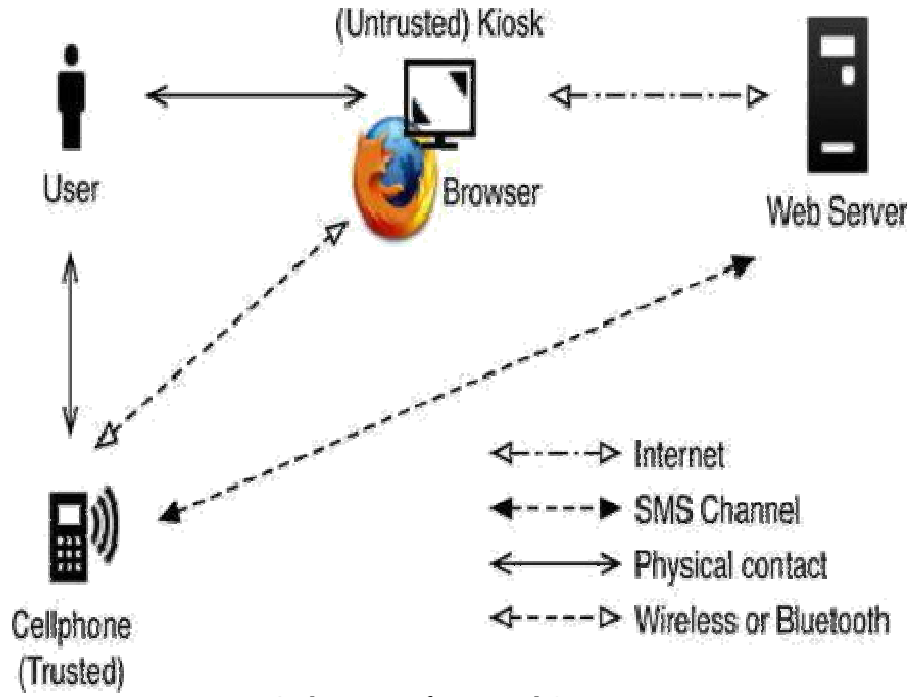

Fig:1.Architecture of improved OPass system.

II. OPASS

A. Overview:

The OPASS system looks like a client server model. Here, at client side, the user is the android mobile and browser, while at the server side, main server and GSM modem.This will work on the based on user's request where server needs to provide services on the demand. Here the user initially sends one registration request to the server as shown in Fig: 2, and server will process that request and send one long term password to client through GSM modem as shown in Fig:2. Here GSM modem is a part of sever, when request comes to server it will read that message by using GSM modem and generate one long term password. This long term password will be sent to mobile. User must use this long term password to login to that URL, for this to happen, the user has to go through browser as shown in Fig 2. In the browser , user will enter all details and then long term pass word is asked from mobile. After entering the long term password from mobile, server will process and generate one OTP. That OTP will be sent to mobile as shown in Fig: 2, user has to enter that OTP from the browser. If the OTP correct, our process will complete otherwise it will give error message.

B. Registration Phase:

The aim of this phase is to allow a user and a server to shared the secret key to process the authentication successfully to login . The user begins by opening the OPass program installed on user cell phone and user enter user Name(Uname), use IDu (prefered user identification) and URL (usually the website url or domain name) to the program. The mobile program sends account id and url to the telecommunication service provider (TSP) through a SMS to make a request of registration. Once the TSP received the account id and the url, it can trace the user's phone number based on user's SIM card. The TSP also plays the role of third-party to forward the message it has received to that specific server number what we are providing in the registration. The TSP and

the server will establish an SSL tunnel to protect the communication. Then the TSP forwards account id to the assigned server.

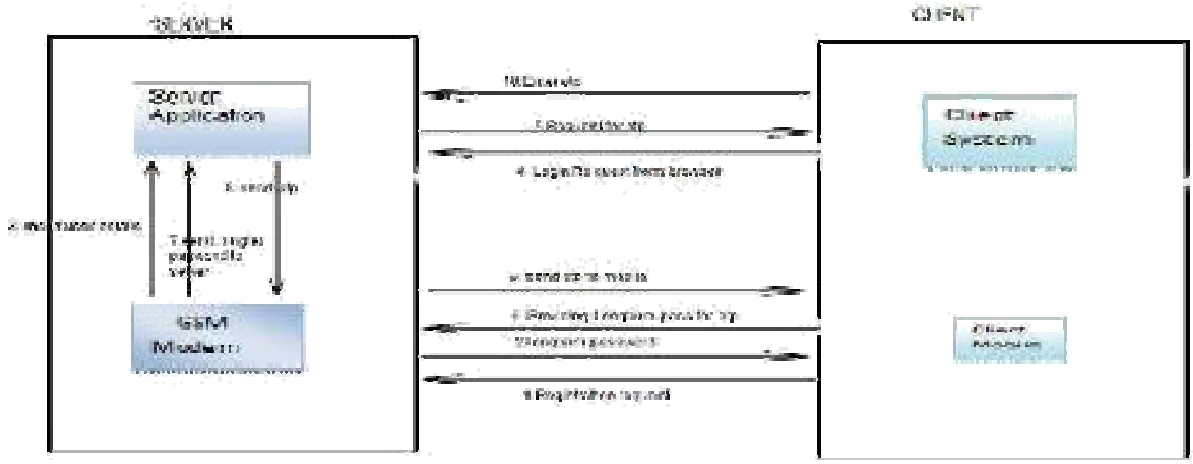

Fig: 2 Client Server Architecture model of Opass

Server will generate the corresponding information for this account and reply a response, including server's identity ID, a random seed, and server's phone number. The TSP then forwards id, and a shared key to the user's cell phone.

C. Login phase:

The login phase begins when the user sends a request to the server through an un trusted browser (on a kiosk). The user uses her cell phone to produce a one-time password, e.g., and deliver necessary information in encrypted form to server via SMS message. Based on pre shared secret credential, server can verify and authenticate the user. The protocol starts when user wishes to log into her favorite web server (already registered). However, begins the login procedure is started by accessing the desired website via a browser on an un trusted kiosk. The browser sends a request to with account IDs. Next, server supplies the ID and a fresh nonce to the browser. Meanwhile, this message is forwarded to the cell phone through GSM Modem. After reception of the message, the cell phone inquiries related information from its database via IDs, which includes server's phone number and other parameters .The next step is promoting a dialog for her long term password. Secretly shared credentials can be regenerate by typing the correct data on the cell phone. The one-time password for current login is recomputed to check if the received is equal to the previously generated , this declares the user is legitimate or not ; otherwise, the server will reject this login request. Upon successful verification, the server sends back a success message through the Internet, if the user is successfully log into the server.

D. Long term Password Encryption:

When user entered login details from browser like user name and URL , it will prompt like "please enter long term password from your mobile". At that time user have to open android app in his/her mobile and have to enter long term password which he/she received at the time of registration. After user entered the long term password, then long term password will be encrypted by using AES algorithm with a private key and then sent to server. Server will receive that message and decrypt that message by using AES along with same key. If the decrypted message is as same as user entered data then verification is done with respect to the database. If this long term password generated for that URL and user name then it will generate one OTP.

E. Recovery Phase:

Recovery phase is designated for some specific conditions; for example, a user may lose his/her cell phone. The protocol is able to recover OPass setting on user new cell phone assuming user 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, user 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. When server receive 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. 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. During the last step, the user's cell phone encrypts the secret credential and server nonce to a cipher text. The recovered SMS message is delivered back to the server for checking. Similarly, the server computers 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 will be used for user authentication.

III. RESULT ANALYSIS

A. Scalability

Scalability is ability of a system, network, or process to handle a growing amount of work

in a capable manner or its ability to be enlarged to accommodate that growth.

B. Registration phase:

Like traditional server, GSM modem can receive multiple request where each request is processed one after the other handling concurrency problem. To handle the second request it will take some time.

1. If thread sleep is given as 60 units of time after receiving the request, it will overlap the request and it may not give correct results.

2. If thread sleep is given as 1000 after receiving the request , it will process the first request and may struck in the reading mode.

3. If thread sleep is given as 2000 it will give better results by taking the gap between each request maximum of 15sec.

4. If thread sleep is given as 3000 it will work fine but it will take extra time to delete the message and to process next request.

5. If thread sleep is given as 4000 it will also work fine but same problem repeat as above. And the time of long term password generation here i used random function.

There are two options to consider long term password like from user details or from phone number. If you use like this it will confuse to user to remember characters and number for long time.

C. Login Phase:

For generating OTP, MD5 algorithm is used by considering all alphabets, symbols, and numbers if OTP generate from user details, the probability of describing strong OTP will decrease. SO it becomes easy for an intruder to hack.

Ex: user details

userName : kotamraju ; Uid : reddycherla ; phoneNo : 8977520780

Instead the following is considered:

option1: A to Z
option2: a to z

option3: 1 to 9

option4: all symbols

In user details less number of characters are available, So the probability to hack OTP will increase so as to avoid this the above mentioned options are considered compare to user details.

D. Recovery phase:

In case of loss of mobile phone, user may use this app to reset his long-term password. But if user didn't get his old number which is used at the time of registration he can't use this application. When user enters all details, the server will check phone number along with user details and gives the confirmation.

E. Anti-malware:

Malware (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.

F. 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.

G. Password Reuse Prevention and Weak Password Avoidance:

OPass achieves one-time password approach. The mobile phone automatically derives different passwords for each login. They only keep a long-term password for accessing their cell phones, and leave the rest of the work to OPass.

H. Mobile phone Protection:

An adversary can steal users mobile phones and try to pass through user authentication. However, the mobile phones are protected by a long-term password. The adversary cannot impersonate a legal user to login without being detected.

IV. CONCLUSION

In this paper the application , an improved user authentication protocol named OPass is introduced. The app influences mobile phones and SMS to confuse password stealing and password reuse attacks. Here each website possesses a unique phone number and also assume that a telecommunication service provider involves in the two phases(registration and recovery phases) in form of GSM modem. The design principle of OPass, with the combination of Long Term Password eliminates the negative leverages of human factors as much as possible. 0nly thing the user need to remember is a long-term password which has been used to protect her mobile phone. Now using this protocol user can type any passwords into suspicious systems for logging into all websites. Compared with previous schemes, OPass is the first android based improved 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 secure sovereignty between each login. To produce OPass fully serviceable, password recovery is also weighed and supported when users lose their mobile phones. They can reclaim our OPass system with renewed SIM cards and long-term passwords. Future Work - Currently we can use oPass for the URL that user has given during registration. In future we would like to develop the application that can support for all website. And see that it works to handle multiple request at a time. Also we like to develop this application for banking purposes.

REFERENCES

[1]. Hung-Min Sun, Yao-Hsin Chen, and Yue-HsunLin "oPass: A user authentication Protocol Resistant to password Stealing and password Reuse attack" IEEE transactions on information forensics and security, April 2012.

[2]. Zhang Baoshi. Research on computer network security analysis model [J]. Electronic technology and software engineering, 2014.

[3]. B. Daya ,"Network Security: History, Importance, and Future ,"University of Florida Department of Electrical and Computer Engineering , 2013.

[4]. 4. Jain, M.K., 2011. Wireless sensor networks:Security issues and challenges. International Journal of Computer and Information Technology, 2(1):62-67.

[5]. A. R. F. Hamedani, "Network Security Issues, Tools for Testing," School of Information Science, Halmstad University, 2010.

[6]. 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.

[7]. D. Florencio and C. Herley, "A largescale study of web password habits," in WWW '07: Proc. 16th Int. Conf.World Wide Web., New York, 2007, pp. 657–666, ACM.

[8]. 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.

[9]. S. Wiedenbeck, J. Waters, J.-C. Birget, A. Brodskiy, and N. Memon, "Passpoints: Design and longitudinal evaluation of a graphical password system," Int. J. Human- Computer Studies, vol. 63, no. 1–2, pp. 102– 127, 2005.

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

[11]. D.Davis, F. Monrose, and M. K. Reiter, "On user choice in graphical password schemes," in Proceedings of the 13th Usenix Security Symposium, San Diego, CA, 2004.

[12]. D. Weinshall and S. Kirkpatrick, "Passwords You'll Never Forget, but Can't Recall," in Proceedings of Conference on Hman Factors in Computing Systems (CHI), Vienna, Austria: ACM, 2004.

[13]. S. Man, D. Hong, and M. Mathews, "A Shoulder-Surfing resistant graphical password scheme," in Proceedings of International Conference on security and management Las Vegas, NV, 2003.

[14]. W. Jnasen, S. Gavrila, V. Korolev, R. Ayers, and R. Swanstrom, "Picture Password:A Visual Login Technique for Mobile Devices," National Institute of Standards and Technology Interagency Report NISTIR 7030, 2003.

[15]. W. Jansen, "Authenticating Users on Handheld Devices," in Proceedings of Canadian Information Technology Security Symposium, 2003

[16]. A S. Patrick, A C. Long, and S. Flinn, "HCI and Security Systems", presented at Cm, Extended Abstracts (Workshops). Ft Lauderdale, Florida, USA., 2003

[17]. R. Dhamija and A Perrig, "Deja Vu: A User Study Using Images For Authentication", 9th USENIX Security Symposium, 2000.

[18]. A. Perrig and D. Song, "Hash Visualization: A New Technique To Improve Real-World Security," in Proceedings of the 1999 International Workshop on Cryptographic Techniques and E-Commerce, 1999.