International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Impact Factor (2012): 3.358

OPASS Authentication Schemes Using Android Mobile Application in Providing Web Security

P. Shailaja

M.Tech, School of Information Technology, JNTUH, Hyderabad, Telangana, India

Abstract: ***Popular form of authentication for user is through text password because of its effortlessness and convenience .On the other hand these passwords can be hacked by using malicious software and threads. Firstly, as users maintain several accounts on different websites they choose weak passwords which are easier to remember and they use same passwords for different websites. Reusing the same password for different websites may cause user to lose his information, if one account of user is hacked then hacker can gain access to all other accounts of user. Entering the passwords into public computers may not be safe if the attacker uses malicious software like keystroke logger to get user's password. In this paper we design opass (one time password) authentication scheme for providing security to websites using an android mobile application. In this scheme we are using an android mobile and SMS (short message service) to prevent attacks while reusing passwords and stealing of passwords and to provide web security.***

Keywords: authentication protocol, Opass Browser, web security.

1. Introduction

User authentication for websites has been through text passwords for past few years. A user registers himself or herself with the website by entering details like username, date of birth etc and creates a text password for that account so that it is used for authentication of user for next login. User authentication through text passwords may have drawbacks like user may forget the passwords. Generally users tend to use weak passwords so that they are easy to remember even if they know that these passwords are not secure. Another crucial problem is that users reuse passwords across various websites [1]. For online accounts, users access different accounts from the same machine [2]. A user has an average of 6.5 passwords among which he or she shares it with 3.9 different websites. Each user has nearly 25 accounts that require passwords, and uses an average of 8 passwords per day. For easily remembering those passwords user choose weak passwords. Users forget passwords a lot, we estimate that for each month at least 1.5% users of Yahoo forget their passwords [3].Graphical passwords were an alternative to text passwords, in which a user is asked to remember an image (or parts of an image) instead of a text word. Its complex for Humans to remember difficult or meaningless passwords [4][5]. Pass Points involves a user have to create a five-point click sequence on a background image. Scalable attacks require that the attacker collect enough "human-computed" data for the target image, for systems with multiple images it costs more. This leads to ask whether more scalable attacks exist mainly, effective fully automated attacks. [6] An attacker may install a malicious program such as a keystroke logger that results in password stealing attack. [7][8].

2. Related Work

2.1 Large scale Study of Web Password Habits

We report the results of an outsized scale study of password use and password re-use habits. The study concerned a million users over a three month amount. A shopper element on user's machines recorded a range of parole strength usage and frequency metrics. this enables US to live or estimate such quantities because the average variety of passwords and average variety of accounts every user has, what number passwords she sorts per day however usually passwords square measure shared among sites, and the way usually they're forgotten. We have a tendency to get extraordinarily elaborate knowledge on password strength, the categories and lengths of passwords chosen, and the way they vary by web site. The info is that the massive scale study of its kind, and yields varied alternative insights into the role the passwords play in user's online expertise.

2.2 Password Management Strategies For Online Accounts

Given the widespread use of password authentication in on-line correspondence, subscription services, and looking, there's growing concern regarding fraud. Once people apply their passwords across multiple accounts, they in- crease their vulnerability; compromising one password will facilitate an offender take over many accounts. They often did not notice that customized passwords like phone numbers will be cracked given an oversized enough wordbook and enough tries. We have a tendency to discuss however current systems support poor watchword practices. We have a tendency to conjointly gift potential changes in web site authentication systems and watchword managers.

3. Proposed System

The Objective of opass authentication schemes using android mobile in providing web security is to free users from entering the passwords into un-trusted public computers and to securely access their web accounts .user authentication protocol involves an android mobile , Short message service and opass browser(data verification browser), where user only need to remember a long-term password . One time password is generated for each login through this we can prevent password stealing and password reuse attacks.

4. System Module

4.1 Registration phase

The aim of this phase is to allow the user to register for particular web server, so that user is authenticated for succeeding logins. This phase begins with installation of registration application on to the user's cell phone, user types user details like server number i.e. phone number of SIM present in GSM modem and username, user ID ,URL i.e. URL of website to be opened in to the registration application. The mobile program sends user details to GSM modem through SMS once the GSM modem receives the user details it traces the user's phone number based on user's SIM card. GSM modem plays the role of third party to distribute information between user and the server, GMS modem forwards these user details to server through RS232 .Server will create user account and stores this information in the database, it generates long-term password and sends it to GMS modem then forwards the long-term password to the user's cell phone.

Table 1: Notations

Name	Description
IDu	identity of user
LTP	long term password
OTP	one time password
Req	Request
Res	Response

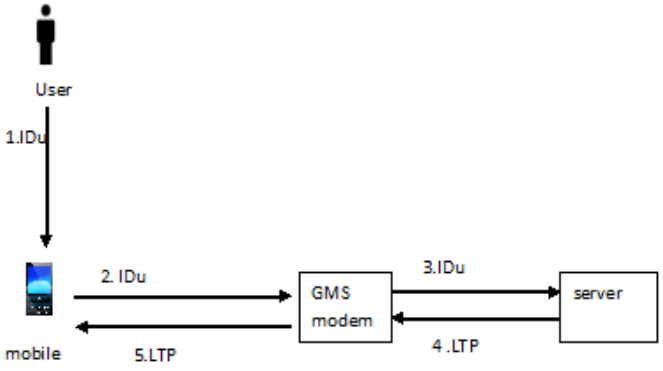

Figure 1: Procedure for Registration phase

4.2 Login Phase

Login phase begins when the user wishes to log into his or her favorite website (already registered) .user opens opass browser and enters username and URL of the website .server checks whether the user is already registered user or not, if the user is not registered before, it promotes a dialog that user is unauthorized user or else it will promotes a dialog to enter long term password into android mobile. user installs login application in the android mobile and enters server number and long-term password into it .these details are forwarded to GMS modem, GSM modem sends them to web server .Based on pre shared secret credentials, server verifies and authenticates user if long-term password is correct, server generates one time password and sends it to user mobile phone or else server will not send OPT to user. User enters this OTP (one time password) into opass browser. The request is send to server, the onetime password for current login is recomputed if the received equals the previously generated, the user is legitimate, otherwise sever will reject this login request upon successful verification.

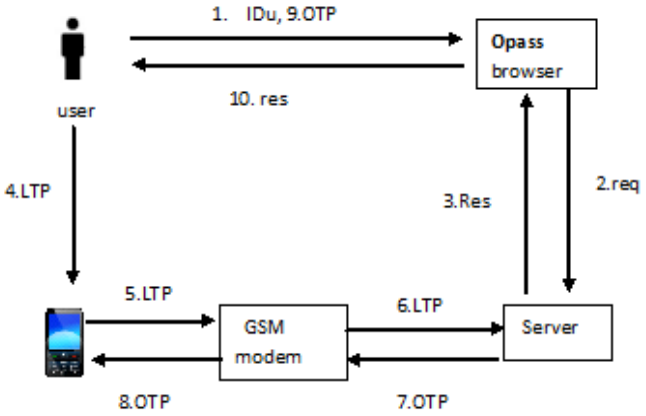

Figure 2: Procedure for Login phase

4.3 Recovery phase

Recovery phase is designated for some specific conditions. For example, a user may lose his or her cell phone. The protocol is able to recover opass setting on her new cell phone assuming he or she still uses the same phone number (apply a new SIM card with old phone number). Once user installs the opass recovery program on his or her new cell phone, he or she can launch the program to send a recovery request with his or her account ID. Similar to registration, GMS modem can trace her phone number based on her SIM card and forward her account ID to the server through an RS232.

4.4 GSM Modem Implementation

GSM modem is a specific type of modem, it is just like a cell phone which accepts a SIM (Subscriber Identity Module) card, and operates over a subscription to a mobile network operator. From the mobile network operator perspective, a GSM modem looks like a mobile phone. It imports the comm Driver and connects the Modem to the PC.

5. Conclusion

A user authentication protocol which involves user's android mobile and short message service to prevent attacks on stealing of password and password re-usage. Users need to remember a long term password for login on to different web accounts. Opass authentication schemes using android mobile application in providing web security is reliable and acceptable for users. In computer security, access to a computer system is controlled by authenticating and identifying the user referring to credentials presented by the user. This protocol applied in different security areas such as Government sectors, online business, Crime Investigation Department, Military sectors. Recovery of password is also considered and supported when cell phone is lost.

References

[1] B. Ives, K. R. Walsh, and H. Schneider, "The domino effect of password reuse" .
[2] S. Gawand E. W. Felten, "Password management strategies for online accounts" .
[3] D. Florencio and C. Herley, "A large-scale study of web password habits".
[4] S. Chiasson, A. Forget, E. Stober, P. C. van Oorschot, and R. Biddle, "Multiple password interference in text passwords and click-based graphical passwords".
[5] I. Jermyn, A. Mayer, F. Monrose, M. K. Reiter, and A. D. Rubin, "The design and analysis of graphical passwords".
[6] P. van Oorschot, A. Salehi-Abari, and .I. Thorpe, "Purely automated attacks on passpoints-style graphical passwords".
[7] N. Provos, D. Mcnamee, P. Mavrommatis, K. Wang, and N. Modadugu, "The ghost in the browser: Analysis of web-based malware"
[8] B. Pinkas and T. Sander, "Securing passwords against dictionary attacks,"in CCS '02: Proc. 9th ACM Conf. Computer CommunicationsSecurity, New York, 2002, pp. 161–170, ACM.
[9] J. A. Halderman, B. Waters, and E. W. Felten, "A convenient methodfor securely managing passwords," in WWW '05: Proc. 14th Int. Conf.World Wide Web, New York, 2005, pp. 471–479, ACM.
[10] K.-P. Yee and K. Sitaker, "Passpet: Convenient password managementand phishing protection," in SOUPS '06: Proc. 2nd Symp. Usable PrivacySecurity, New York, 2006, pp. 32–43, ACM.
[11] S. Chiasson, R. Biddle, and P. C. van Oorschot, "A second look at theusability of click-based graphical passwords," in SOUPS '07: Proc. 3rdSymp. Usable Privacy Security, New York, 2007, pp. 1–12, ACM.
[12] K. M. Everitt, T. Bragin, J. Fogarty, and T. Kohno, "A comprehensivestudy of frequency, interference, and training of multiple graphicalpasswords," in CHI '09: Proc. 27th Int. Conf. Human Factors ComputingSystems, New York, 2009, pp. 889–898, ACM.
[13] J. Thorpe and P. C. van Oorschot, "Graphical dictionaries and thememorable space of graphical passwords," inSSYM'04: Proc. 13th Conf.USENIX Security Symp., Berkeley, CA, 2004, pp. 10–10, USENIX Association.
[14] R. Dhamija, J. D. Tygar, andM. Hearst, "Why phishing works," in CHI'06: Proc. SIGCHI Conf. Human Factors Computing Systems, NewYork, 2006, pp. 581–590, ACM.
[15] C.Karlof,U. Shankar, J. D.Tygar, andD.Wagner, "Dynamic pharmingattacks and locked same-origin policies for web browsers," in CCS '07:Proc. 14th ACMConf. Computer Communications Security, NewYork 2007, pp. 58–71, ACM.
[16] T. Holz, M. Engelberth, and F. Freiling, "Learning more about the undergroundeconomy:Acase-study of keyloggers and dropzones," Proc.Computer Security ESORICS 2009, pp. 1–18, 2010.

Author Profile

P. Shailaja received Bachelor of Technology in Computer Science and Engineering from Jawaharlal Nehru Technological University in 2012. She is pursuing Master of Technology in Computer Science in School of Information Technology, Jawaharlal Nehru Technological University Hyderabad. Her research interests are Information Security, Web Technology, Parallel Computing, Human Computer Interaction and Data Mining.