Improved Password Authentication System against Password attacks for web Applications

Vaishnavi Yalamanchili,
Department of Computer Science & Engineering,
Gudlavalleru Engineering College,
Gudlavalleru , Andhra Pradesh, India.

Dr.P.Pandarinath, M.Tech, Ph.D
Professor, Department of CSE,
Gudlavalleru Engineering College,
Gudlavalleru , Andhra Pradesh, India.

***Abstract* – Password security is important for user authentication on small networking system as well as large networking system. Till today many researchers introduced various practices to protect passwords on network. Passwords prone to various types of attacks like brute force attack, password stealing attack, password reuse attack, password cracking attack, etc. To scale back the harm of phishing and spyware attacks, banks, governments, as well as other security-sensitive industries are deploying one-time password systems, where users have numerous passwords and utilize each password only once in the existing approach using opass. Unfortunately, the password entropy that users can comfortably memorize seems insufficient to build up unique, secure passwords for all those these accounts, and it will be likely to remain constant as the range of passwords. In existing work a user authentication protocol named oPass which leverages a user's cellphone and short message service to secure password stealing and password reuse attacks is designed[2]. oPass only requires each participating website possesses a unique telephone number, and involves a telecommunication service specialist in registration and recovery phases. But existing system entirely depends on telecommunication service provision and users contact number . Existing oPass approach is a bit more cost effective . Within this proposed system , we propose a method that utilizes a strengthened cryptographic hash function to compute secure passwords for arbitrarily many accounts while requiring the user to memorize merely a single short password. This mechanism functions entirely on the client; no server-side changes are needed. In our proposed system we implemented email service in order to recover the users password after registration.**
Proposed System framework generates strong passwords by enhancing the hash function utilizing a large random salt. Using the support of a salt repository, it gains a significantly stronger security guarantee than existing mechanisms. Proposed approach is less vulnerable to offline attacks, and this provides stronger protection against password theft. Our system is less cost effective and better defense mechanism against attacks.

***Keywords* – Password Protection, Authentication, Hashing, TSP,Telecommunications,SMS.**

I. INTRODUCTION

Within the last few decades, text password has been adopted as the main secure mechanism to user authentication for websites. People select their username and text- passwords when registering accounts on a website. So that you can once you have logged into the web page successfully, users must recall these passwords. Generally, password based user authentication can resist brute-force and dictionary attacks if users select strong passwords. However, password-based user authentication has a significant problem that humans typically are not experts in memorizing text strings. Thus, high percentage of consumers would choose easy to-remember passwords (i.e., weak passwords) even if they are able to know those passwords could be unsafe. Another crucial problem is users are inclined to reuse passwords across various websites. Password reuse causes users to lose sensitive information held in different websites any time a hacker compromises one of their passwords. This attack is known as the password reuse attack. All the above issues are as a result of the bad part influence of human factors. Therefore, it is essential to take human factors into note when designing an individual authentication protocol. Despite their prevalence and importance in online authentication, passwords do have two well-known and long-standing problems: weak passwords are extremely easy to crack, and passwords are sensitive to theft. Password security is determined by creating strong passwords and protecting them being stolen. A strong password should be sufficiently long, random, and difficult to uncover by crackers. In comparison, a weak password is normally short, common, and easier to guess. Examples of strong passwords include "t3wahSetyeT4" and "Tpftcits4Utg!"; and instances of weak passwords include "susan123" and "password"[4-8]

Password security is most important on network system. Various types of passwords like text password, graphical password can be used. Also different number of factors can be used for user authentication like- 1) Single password can be used to login into website. 2) Two factor authentication depends on what you know (e. g. password) and what you have (e. g. token). 3) Three factor authentication depends on what you know (e. g. password), what you have (e. g. token) and who you are (e. g. Biometric). Among all text password is most commonly used for user authentication on different websites. By selecting username and password one can

register their account on website. Later on, to successfully login on a website user must recall that password. If selected password is strong, different attacks that reveal password can be avoided. But if selected password is weak, it can be vulnerable to various types of attacks. If same password is used across different websites and once that password is revealed adversary may get access into different websites. So, different researchers studied various types of passwords, their benefits and drawbacks, how they are vulnerable to different types of attacks.

II. LITERATURE SURVEY

Shirley Gaw and Edward W. Felten studied online accounts and password management strategies for those accounts. Their technology did not help for recalling password of an online account but their tips to strengthen passwords but failed to explain the nature of dictionary attacks [2].

Because of such different drawbacks of text passwords graphical passwords were introduced years before. Ian Jermyn, Alain Mayer, Fabian Manrose, Michael K. Reiter and Aviel D. Rubin evaluated new graphical password schemes to achieve better security than text passwords. When Graphical password users were creating passwords they were able to quickly and easily create a valid password, but to learn those passwords they had more difficulty than alphanumeric password users. However, the graphical users took longer time and made more invalid password as compared to alphanumeric users while practicing their passwords [3,9].

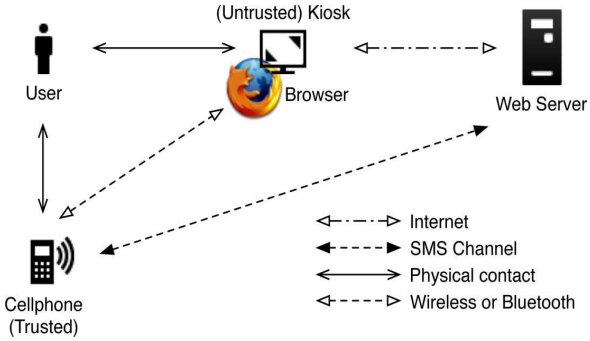
In 2005 researcher's Susan Wiedenbeck, Jim Waters, Jean-Camille Birget, Alex Brodskiy and Nasir Memon introduced the concept of graphical password system called PassPoints which was based on two areas i.e. security and usability [5]. They concluded that PassPoints are more efficient for security. Based on intricate, natural images with hundreds of potential click points, one can be easily obtain large passwords spaces. Another thing is that, they developed a robust discretization which enables that system to cryptographically hash PassPoints passwords. This robust discretization makes the system safe storage and protected during file back-up. Also it appears from the small sample in their experiment that users did not too often chose points that were within a grid square chosen by another individual[9].

First, users create their passwords by themselves. For easy memorization, users tend to choose relatively weak passwords for all websites. This behavior causes a risk of a domino effect due to password reuse. To steal sensitive information on websites for a specific victim (user), an adversary can extract her password through compromising a weak website because she probably reused this password for other websites as well. Second, humans have difficulty remembering complex or meaningless passwords. Some websites generate user passwords as random strings to maintain high entropy, even though users still change their passwords to simple strings to help them recall it. Phishing attacks and malware are threats against password protection. Protecting a user's password on a kiosk is infeasible when keyloggers or backdoors are already installed on it. Considering the current mechanisms, authenticating users via passwords is not a best solution.

oPass adopts the one-time password strategy; therefore, the strategy is given later. Finally, the security of 3G connection used in the registration and recovery phases of oPass is used.

One-Time Password:

The one-time passwords in oPass are generated by a secure one-way hash function. With a given input , the set of onetime passwords is established by a hash chain through multiple hashing[1-2].



Existing OPASS Framework

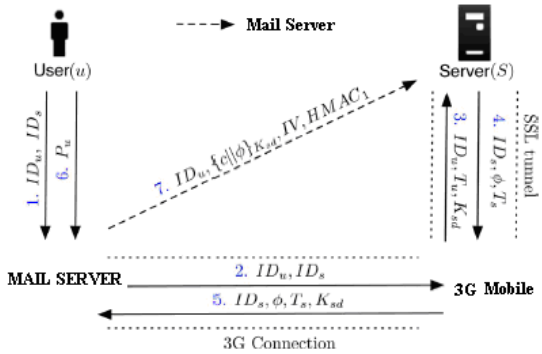
Fig. describes the architecture (and environment) of the oPass system. For users to perform secure login on an untrusted computer , oPass consists of a trusted cellphone, a browser on the kiosk, and a web server that users wish to access. The user operates her cellphone and the untrusted computer directly to accomplish secure logins to the web server. The communication between the cellphone and the web server is through the SMS channel. The web browser interacts with the web server via the Internet.

III. PROPOSED SYSTEM

Registration Phase:

Registration Phase depicts the registration phase. This is to allow a user and a server to negotiate a shared secret to authenticate succeeding logins for this user. The user begins by opening the ProcurePass program installed on her cellphone. She enters IDu (account id she prefers) and IDs (usually the website url or domain name) to the program.The Email program sends IDu and IDsto the server through a 3G connection to make a request of

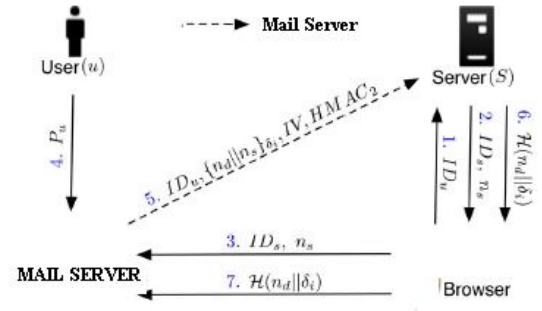
registration. Once the Server received the IDu and IDs, it can trace the user's mail id Tu. The shared key Ksd is used to encrypt the registration id with AES-CBC. Server S will establish an SSL tunnel to protect the communication. Then the Mail forwards IDu, Tu, and Ksd to the assigned server S.Server will generate the corresponding information for this account and reply a response, including server's identity IDs, a random seed , and server's Mail id[1-2].



Procedure of registration phase.

Login Phase:

The login phase begins when the user sends a request to the server S through an untrusted browser. The user uses her mail id to produce a one-time password, e.g., di, and deliver necessary information encrypted with dito server S via an Mail Server. Based on preshared secret credential c, server S can verify and authenticate user based on di.



Procedure of login phase.

The protocol starts when user u wishes to log into her favorite web server (already registered). However, u begins the login procedure by accessing the desired website via a browser on an untrusted browser. The browser sends a request to S with u's account IDu. Next, server S supplies the IDsand a fresh nonce nsto the browser[1,2].

Recovery Phase:

Recovery phase is designated for some specific conditions; for example, a user u may forgot his/her password. The protocol is able to recover Password setting on her new mail id.

IV.EXPERIMENTAL RESULTS

All experiments were performed with the configurations Intel(R) Core(TM)2 CPU 2.13GHz, 2 GB RAM, and the operating system platform is Microsoft Windows XP Professional (SP2).

Fig1: User registration phase

Fig2: User registration credentials calculated values

Fig3: Server phase for user and mail id validation

Fig4: Server authorization sending process

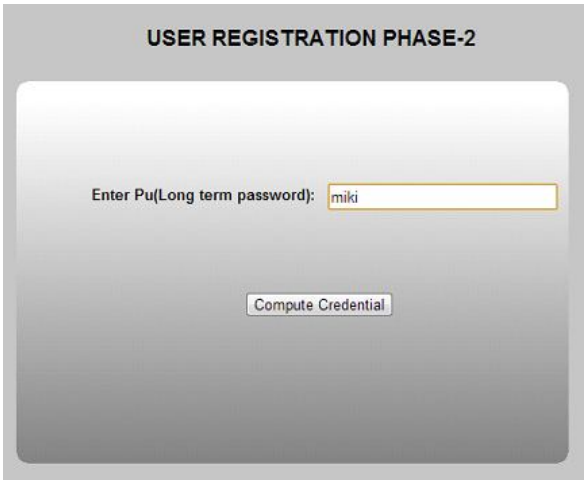


Fig5: User registration phase -2 for long term password

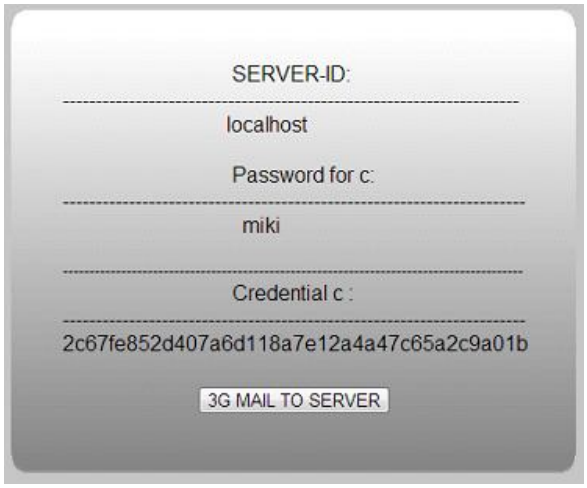


Fig6: Server id and credential c calculations

Fig7: User login phase

Fig8: User login credentials calculations generating nonce value.

Fig9 : User Password is entered for computing credential validations.

Fig10: User one time password hash value.

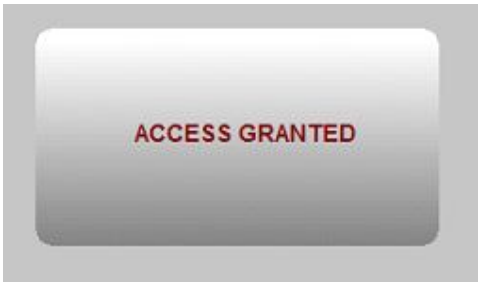
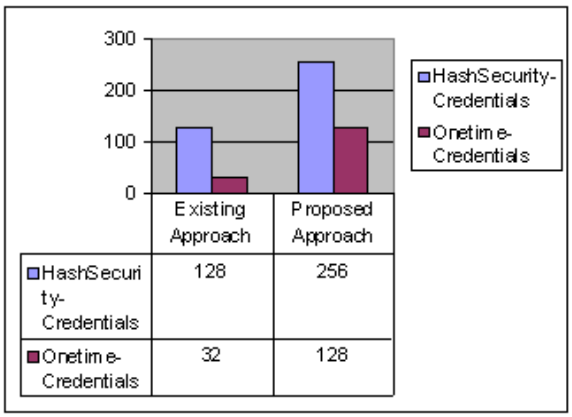
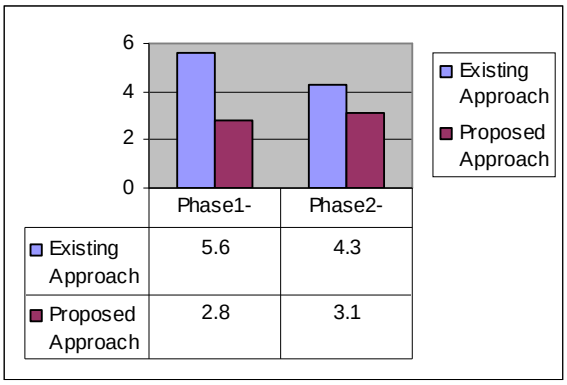


Fig11:If one time password is correct then access is granted.

Performance Results:



Comparison between Credential data bits generated in existing and proposed work for more security.



Phase-1 and Phase -2 time comparison

V. CONCLUSION AND FUTURE SCOPE

Proposed user authentication protocol which leverages cell phone and email system to thwart unusual stealing and password reuse attacks. This system assume that each person possesses a unique number as mail id. It successfully creates the registration and recovery phases. This proposed approach eliminates the existing opass negative influence of human factors whenever possible. Through Proposed Opass, each user only requires to remember a permanent password which has been made use to protect her cellphone. Users are protected from typing any passwords into untrusted computers for login on various websites. Compared with previous schemes, this approach would be the first user authentication protocol to minimize the risk of password stealing and password reuse attacks simultaneously. For the reason that Proposed opass adopts the one-time password strategy to ensure independence between each login.

REFERENCES

[1] ProcurePass: A User Authentication Protocol to Resist Password Stealing and Password reuse

Attacks Mariam M. Kassim, A. Sujitha B.Tech., M.E. International Journal of Scientific & Engineering Research, Volume 4, Issue 6, June-2013 57 ISSN 2229-5518

[2] oPass: A User Authentication Protocol Resistant to Password Stealing and Password Reuse Attacks Hung-Min Sun, Yao-Hsin Chen, and Yue-Hsun Lin IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY, VOL. 7, NO. 2, APRIL 2012.

[4] J. Thorpe and P. van Oorschot, ―Towards secure design choices for im-plementing graphical passwords, presented at the 20th. Annu. Com-puter Security Applicat. Conf, 2004.

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

[6] B. Pinkas and T. Sander, ―Securing passwords against dictionary at-tacks, inCCS '02: Proc. 9th ACM Conf. Computer Communications Security, New York, 2002, pp. 161–170, ACM.

[7] J. A. Halderman, B. Waters, and E. W. Felten, ―A convenient method for securely managing passwords, inWWW '05: Proc. 14th Int. Conf. World Wide Web, New York, 2005, pp. 471–479, ACM.

[8] K.-P. Yee and K. Sitaker, ―Passpet: Convenient password management and phishing protection, inSOUPS 06: Proc. 2nd Symp. Usable Pri-vacy Security,New York,2006,pp.32–43,ACM.

[9] L. Lamport,, ―Password authentication with insecure communication, Commun. ACM, vol. 24, pp. 770–772, Nov. 1981.

[10] H. Krawczyk, ―The order of encryption and authentication for pro-tecting communications (or: How secure is SSL?), inAdvances Cryp-tology—CRYPTO 2001, 2001, pp. 310–331.