Secure and Efficient Authentication Scheme against Password Attacks

S.Venkatesan
M.Tech Assistant professor
Department of Information Technology
Skp engineering college, Thiruvannamalai, Tamilnadu, India.

S.Savitha
Department of Information Technology
Skp engineering college, Thiruvannamalai, Tamilnadu, India.

S.P.Nisha
Department of Information Technology
Skp engineering college, Thiruvannamalai, Tamilnadu, India.

E.Navaneetham
Department of Information Technology
Skp engineering college, Thiruvannamalai, Tamilnadu, India.

S.Mahalakshmi
Department of Information Technology
Skp engineering college, Thiruvannamalai, Tamilnadu, India.

Abstract- Commonly text passwords are used for registering accounts in websites. People often reuse passwords for their easy remember. These reuse of password causes domino effect. If hacker had compromised any one password it made easy to access all website accounts. To avoid this type of hacking we go for user authentication protocol Opass. Opass avoids hackings like phishing, malware and key loggers. Opass which leverages users cell phone and short message service to thwart password reuse and stealing attacks. Opass only requires each participating websites and unique phone number. Through Opass user have to remember only the long term password.

I-INTRODUCTION

People nowadays rely heavily on internet widely deployed web services facilitate and enrich several applications. The authentication of user is handled by text passwords for different websites. This creates disadvantages for users. Users create passwords by themselves for their convenience; these passwords are weak so causes domino effect due to password reuse. When user reuse same password to different websites, hackers can easily compromises password through weak websites. Humans have difficulty remembering complex passwords. Some websites generate user passwords as random strings to maintain high entropy, even though users still change their passwords to help them recall it. These approaches could mitigate problems, but also make system more complicated. Phishing attacks and malware are threats against password protection. Current mechanisms are not the best solutions. Therefore a user authentication protocol called opass is proposed for password attacks. The goal of opass is to prevent typing passwords in un trusted computers. Through one-time passwords users' login to the un trusted computers. One-time password is expired when the user completes the current session. Opass leverages sms and users cell phones to avoid attacks. Based on sms, a user identity is authenticated without inputting passwords to un trusted computers. In opass, users need to remember only long-term password. Long-term password is used to protect the information.

II-OBJECTIVE

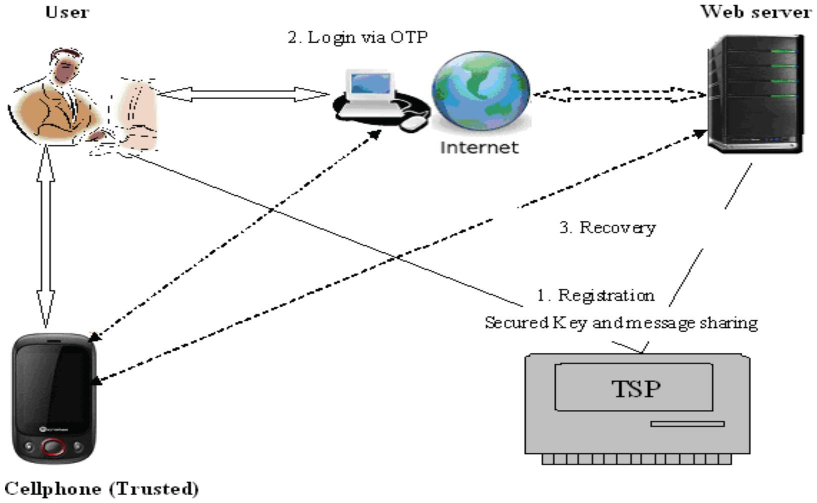
- To provide a user authentication protocol named oPass which leverages a user's cell phone and short message service to thwart password stealing and password reuse attacks.
- To provide Phishing protection and Anti malware to gather and protect the sensitive information from users.
- To ensure Password Reuse Prevention and Weak Password Avoidance.
- To use Secured Shared Key Sharing Mechanism to protect shared key.

III-PROPOSED ALGORITHM

Asymmetric key generation algorithm-

TSP delivers the shared key to both server and user. The shared key can be hacked by the attacker which affects the security of the authentication system. In order to provide more security, shared key must be sent securely. User and server generate the public and private key pair using the asymmetric key generation algorithm. Shared key is encrypted by the TSP using the public key of the user while sending it to the user. User decrypts it using the private key available with it. Shared key is encrypted by the TSP using the public key of the server while sending it to the server. Server decrypts it using the private key available with it. Hence the attack over the entire system is controlled through the addition of Secured Shared Key Sharing Mechanism.

IV-ARCHITECTURE DIAGRAM



V-MODULES

A. Registration phase-

This phase allow a user and server to negotiate a shared secret to authentication succeeding logins for users. The user begins by opening the opass installed in cell phone. User needs to enter the account id and preferred url to the program. Mobile program sends account id and url to telecommunication service provider (TSP) through a 3G connection to register. TSP receives id and url, it trace users phone number based on sim card. TSP also shares shared key between user and server. This shared key is used to encrypted sms. TSP forwards account id, url, and users phone number to server. Server receives details and generate response including severs id and servers phone number then forward to TSP. Then TSP forwards servers phone number, url, shared key to users cell phone. Once cell phones gets response, the user continues to setup long-term password in cell phone. The cell phone computes a secret credential.

$$c = \mathcal{H}(P_u \| \mathrm{ID}_s \| \phi)$$

Secure registration sms is prepared by encrypting secret credential with shared key. The cell phone sends an encrypted registration sms to server by phone number.

$$\text{Cellphone} \overset{SMS}{\rightarrow} S : \text{ID}_u, \{c\|\phi\}_{K_{sd}}, IV,$$
$$\text{HMAC}_1.$$

A server decrypt and verifies the registration sms and obtain the shared key. Server also compares the received sms with user phone number to prevent spoofing attacks. Finally cell phone stores all information except long-term password and secret credential. One-time password initially set to 0, the server authenticates during each login. The server stores all information and then completes registration.

A. Start opass and enter long-term password-

Login procedure does not require user to type passwords in un trusted computers. The user name is the only information input to browser. The user opens opass program in cell phone and enters long-term password. The program generates one-time password and send login sms to server. Login sms is encrypted by one time password.

B. Generate one time password-

The one-time password in opass is generated by secure one-way hash function. One-time password is established by hash chain through multiple hashing. To prepare one-time passwords, the first of these passwords is produced by performing hashes on input.

$$\delta_0 = \mathcal{H}^N(c).$$

C. Login phase-

The login phase begins when the user sends a request to server through an un trusted browser. The user uses cell phone to produce a one-time password and send it to server through sms message. Based on secret credential, the server verifies authenticated users. Protocol starts when user logins to websites on un trusted computers. Browser sends request to server with account id. Server supplies url and fresh nonce to browser. Messages are forwarded to cell phone through wireless interfaces. Cell phone inquires related information includes servers phone number. Next step is to set long-term password. Secret shared credential is generated by inputting long-term password. One-time password is generated and that is used for login.

$$c = \mathcal{H}(P_u\|\text{ID}_s\|\phi)$$
$$\delta_i = \mathcal{H}^{N-i}(c).$$

The cell phone generates fresh nonce. To secure login, the cell phone encrypts fresh nonce and one-time password. Then cell phone sends following sms message to server.

$$\text{Cellphone} \overset{\text{SMS}}{\rightarrow} S : \text{ID}_u, \{n_d\|n_s\}_{\delta_i}, IV,$$
$$\text{HMAC}_2.$$

After receiving login sms, server decrypts and verifies login sms. If the received are equal then user is legitimate otherwise the server rejects login request. The server sends back success message to user through internet. The cell phones receives message and ensures the verification completion. The last verification is to prevent phishing attacks. If verification failed, the user knows failure of login and device would not increase index value. If verification is success, the index value is increased automatically. To refresh one-time password recovery phase is used.

D. Recovery phase-

Recovery phase is designated for some specific conditions like when user lost their cell phone. The protocol is able to recover opass settings through the use of same phone number. The user has to install opass in new cell phone and click recovery. The program sends recovery request with account id and server id to predefined TSP through 3G connection. The url is the domain name. Similar to registration process, TSP trace user phone number based on sim and forwards account id and users phone number to server through an SSl tunnel. Once server receives request, server probes the account information in its database to conform if account user is registered or not. If account exists, the information used to compute the secret credential will be fetched and sent back to user. Again server generates fresh nonce and reply with corresponding information. These include all necessary elements for generating one-time password to user. When mobile receives message, it forces the user to enter long-term password to reproduce correct one-time password. Thus the information's are recovered. Finally the user's cell phone encrypts the secret credential and server nonce. The recovery sms message is delivered back to server. The server decrypts this message to ensure the user is already recovered. The new cell phone is recovered and ready for further logins. For the further logins the one-time password is used for user authentication. Thus the recovery phase finishes here.

VI-CONCLUSION

User authentication protocol named oPass is proposed in this paper which leverages cell phones and SMS to thwart password stealing and password reuse attacks. In this paper each website possesses a unique phone number. Also assume that a telecommunication service provider participates in the registration and recovery phases. The design principle of oPass is to eliminate the negative influence of human factors as much as possible. Through oPass, each user only needs to remember a long-term password which has been used to protect her cell phone. Users are free from typing any passwords into un trusted computers for login on all websites. Compared with previous schemes, oPass is the first user authentication protocol to prevent password stealing (i.e., phishing, keylogger, and malware) and password reuse attacks simultaneously. The reason is that oPass adopts the one-time password approach to ensure independence between each login. To make oPass fully functional, password recovery is also considered and supported when users lose their cell phones. They can recover our oPass system with reissued SIM cards and long-term passwords. Secured Shared Key Sharing Mechanism has been used to protect the shared key from attackers

REFERENCES

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

[2] 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.

[3] 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.

[4] 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.

[5] 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.

[6] A. Perrig and D. Song, "Hash visualization: A new technique to improve real-world security," in Proc. Int.Workshop Cryptographic Techniques E-Commerce, Citeseer, 1999, pp. 131–138.

[7] J. Thorpe and P. van Oorschot, "Towards secure design choices for implementing graphical passwords," presented at the 20th. Annu. Computer Security Applicat. Conf., 2004.

[8] 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.

[9] S. Wiedenbeck, J. Waters, L. Sobrado, and J.-C. Birget, "Design and evaluation of a shoulder-surfing resistant graphical password scheme," in AVI '06: Proc. Working Conf. Advanced Visual Interfaces, New York, 2006, pp. 177–184, ACM.

[10] B. Pinkas and T. Sander, "Securing passwords against dictionary attacks," in CCS '02: Proc. 9th ACM Conf. Computer Communications Security, New York, 2002, pp. 161–170, ACM.