Secure One Time Password Generation for Website Security using Mobile Phone with Biometrics

C. Josy Nambickai Rani[1], Linda Joseph[2], E.R.Naganathan[3]

[1]M. Tech, Computer Science and Engineering
School of Computing Sciences and Engineering
Hindustan University, Chennai, India
josy.rani89@gmail.com

[2]School of Computing Sciences and Engineering
Hindustan University, Chennai, India
lindaj@hindustanuniv.ac.in

Head of the Department
[3]School of Computing Sciences and Engineering
Hindustan University, Chennai, India

Abstract: ***Authentication is an essential part of network security. It is a process of confirming the identity to ensure security, with a vital role to provide security in websites. Even though text password is a convenient user authentication on websites, it is prone to security attacks. Weak passwords are often used across several websites and typing the password into un trusted websites causes password threats. An opponent, who compromises the password, uses password stealing methods such as phishing, malware, and key loggers. The same password is used to access across several websites, with the usage of the same password to access several websites by the authentic users. The proposed system is a user authentication protocol named SOTP which uses the user's mobile phone number and the short message service which is being provided by a service provider. Secure Hash Algorithm (SHA-I) is used to generate a secure one time password. Random password is generated for each login. To provide high security in the websites, a combination of biometric feature i.e., Fingerprint along with hash function is used for authentication. A Telecommunication Service provider (TSP) is used for the registration of the users and also used the recovery phase. The registration phase involves the user's mobile number, secret answer and fingerprint. Recovery phase is used, if the user's mobile phone gets lost. The SOTP requires only the unique mobile number of the user and a service provided by a service provider. The user needs to remember only his long term password which has to be kept secret.***

Keywords: Network security, User authentication, Secure One Time password.

1. Introduction

Previously, 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 [5]-[9]. Using password management tools is an alternative [10]-[12]. 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[13],[14] and is still vulnerable to several attacks[15].users have trouble using these tools due to the lack of security knowledge.

A user authentication protocol named SOTP is designed to overcome the existing problems faced by users during authentication. It requires user's mobile phone for accessing their accounts. It generates random password for each session using SHA. Through SOTP, the methods used for stealing accounts by using phishing, malware, eavesdroppers are protected. By using long term password, the mobile phone is protected from theft. In this, biometric feature extraction is used to provide high reliable security to authenticate user. Minutiae are extracted from fingerprint by using fuzzy extraction.

2. Problem Formulation

2.1 Weak passwords

Generally, users create their passwords by themselves. Users select weak passwords for all websites for easy remembrance. And also users reuse the same password for different websites. An opponent steals the user's password through compromising a weak websites because users use the same password across several websites. Through phishing, an opponent steal the user's sensitive information like username, password.

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 said to be password reuse attack.

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. Proposed System

User authentication protocol SOTP, designed to generate different random passwords for each login to avoid recall problems and password reuse problems for the users. In figure 1, shows the SOTP architecture of the process.

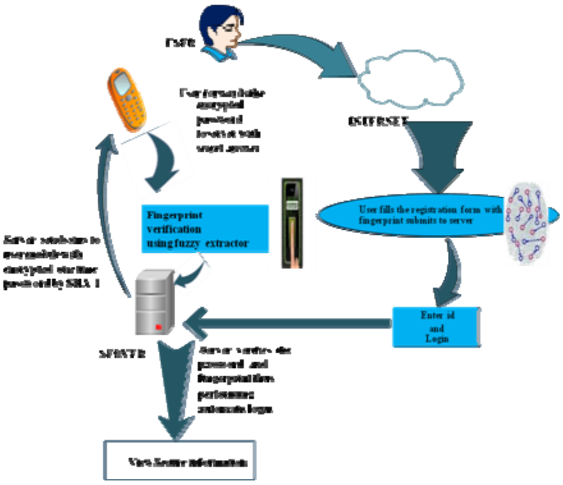
USER
User forwards the encrypted password located with secret answer
INTERNET
User fills the registration form with fingerprint submits to server
Fingerprint verification using fuzzy extractor
Server sends sms to user mobile with encrypted one time password by SHA 1
Enter id and Login
SERVER
Server verifies the password and fingerprint then performs automatic login
View Secure information

Figure 1: SOTP Architecture Diagram

A user authentication protocol SOTP, requires only users unique mobile number. SOTP generates random one time password for each login. There are two phases involved in the authentication such as registration and recovery phase with the help of Telecommunication Service provider (TSP). In registration phase, the user need to provide their personal information with the unique phone number, extraction of minutiae from the fingerprint through reader device by using fuzzy extractor. Information are stored in the database as template for further authentication process. From first login process, the users need to give only username as input to the system. The secure one time password is generated by server using secure hash algorithm (SHA)-1. The generated one time password is in encrypted format is to provide data confidentiality. The random password is send to the user's mobile phone as sms. The main advantage is after receiving the secure one time password with the secret question, instead of typing the received password in the system, the user forwards the password with long term password as sms to the server. To ensure the correct user, biometric feature i.e., finger print is extracted by using fuzzy extractor. It is used for authentication and verification purpose. It compares the extracted fingerprint with template stored. If the password, long term password and fingerprint match with the template that is stored in the database, then it allows the user to authenticate. Otherwise, it declares that the unauthorized user trying to access the accounts and blocks them.

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 SOTP 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 SOTP and the biometric feature. During registration, the details about the users need to be filled with the fingerprint and secret answer that is stored in the database. From first login, the user needs to produce their fingerprint for authentication. If it is successful the SMS will be received by the user with encrypted random password and secret answer. The user needs to forward the encrypted password with secret answer. If it matches with the data stored in the database it allows the user to authenticate.

A. SHA-1

This standard specifies a secure Hash Algorithm, SHA-1, for computing a condensed representation of a message or a data file. When a message of any length< 264 bits is input, the SHA -1 produces a 160-bit output called a message digest. The message digest can then be input to the Digital Signature Algorithm (DSA) which generates or verifies the signature for the message. Signing the message digest rather than the message often improves the efficiency of the process because the message digest is usually much smaller in size than the message. The same hash algorithm must be used by the verifier of a digital signature as was used by the creator of the digital signature.

The SHA-1 is called secure because it is computationally infeasible to find a message which corresponds to a given message digest, or to find two different messages which produce the same message digest. Any change to a message in transit will, with very high probability, result in a different message digest, and the signature will fail to verify. SHA-1 is a technical revision of SHA (FIPS 180). This revision improves the security provided by this standard. The SHA-1 is based on principles similar to those used by Professor Ronald L. Rivest of MIT when designing the MD4 message digest algorithm and is closely modeled after that algorithm.

B. Fuzzy Extractor

Biometric authentication device measures the physical characteristics of a user and matches them against a user profile. It is the most secure authentication tool, as it cannot be stolen or forgotten and also forging is impossible. For the verification, the system validates a user's identity by comparing the captured biometric data with her biometric template stored in the database. Identity verification is used for positive recognition. The main aim of the biometric is to avoid multiple users using the same identity. Through biometric, identity can be obtained with higher level of reliability.

Fingerprint is most successful biometric technique for personal identification and verification process. Every user has unique fingerprints. Fingerprint device is available easily than any other biometric devices. The fingerprint of identical twins also differs completely. For authentication purpose, instead of typing password, the user needs to touch the fingerprint device.

The user need to produce all their information including mobile number, secret answer as long term password and extracting fingerprint through device by using fuzzy extractor technique during registration phase is stored in the database as a template. Fuzzy extractor is used for extracting minutiae from fingerprint and used for verification purpose. The extracted input is to be compared with template. If it matches, the user allowed accessing the webpage. From first login process the user need to type only user name as input to browser.

5. Conclusion

In this paper, a user authentication protocol SOTP uses a users mobile phone , SMS and Biometric feature to prevent from password hacking. It eliminates the negative influence of the human factors. In SOTP the users need to remember only secret answer which only known by the user. The main thing is that the users are free from typing the passwords in un trusted computers. When compared with other schemes, SOTP is more secure because the generated password is valid for that particular session alone. To ensure high reliable security fingerprint is used. Through biometric feature the authorized user can only participate in the authentication process. The proposed system targets in coming up with techniques that can be implemented to ensure website security.

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, "A large –scale study of web password habits," in WWW '07:proc.16th Int.conf.World Wide Web., NewYork, 2007, pp.657-666, ACM

[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] L.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.vanOorschot,"Towards secure design choices for implementing graphical passwords," presented at the 20th.Annu.Computer Security Applicant.Conf., 2004.

[8] S.Wiedenbeck, J.Waters, L.Sobrado, and 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, 2004.

[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.

[11] J.A.Halderman, B.Waters, and E.W.Felton, "A convenient method for securely managing passwords," in WWW'05:proc. 14th Int. Conf World Wide Web, New York, 2005, pp471-479, ACM.

[12] Ka-Ping Yee, Kragen Sitaker, "PASSPET: Convenient Password Management and Phishing Protection", in SOUPS '07: Proc. 3rd Symp. Usable Privacy Security, New York, 2007. Pp.32-43, ACM

[13] S.Chaisson, R.Biddle and P.C.van Oorschot, "A Second look at the usability of click based- graphical passwords", in SOUPS 07:Proc. 3rd Symp. Usable Privacy Security, New York, 2007, pp 1-12 ACM

[14] K.M. Everut,T.Bragin,J.Fogerty and T.Kohno, "A comprehensive study of frequency, interference, and training of multiple graphical passwords", in CHI 09:Proc 27th Int.Conf Human Factors Computing Systems, New York, 2009,pp 889-898,ACM

[15] J. Thorpe and P. C. vanOorschot, "Graphical dictionaries and the memorable space of graphical passwords," in SSYM'04: Proc 13th Conf USENIX Security Symp, Berkeley, CA, 2004, pp10, USENIX association.

Author Profile

C. Josy Nambickai Rani was born in Villupuram. She received the B.E degree in Computer Science and Engineering in Mailam Engineering College, Mailam, in 2010, and currently pursuing M. Tech degree in Computer Science and Engineering in Hindustan University, Chennai. Her research interests are in Network Security with a focus on security on websites.