Volume 6, Issue 2, April 2019 ISSN: 2348-8565 (Online)
International Journal of Modern Engineering and Research Technology
Website: http://www.ijmert.org Email: editor.ijmert@gmail.com

Secure Method for Alphanumeric One Time Password Generation

Abhilasha Chaurasia
M.Tech. Research Scholar
Shriram Group of Institutions
Jaballpur, (M. P.) [INDIA]
Email: abhilashasrist@gmail.com

Sapna Choudhary
Associate Professor & Head of the Department
Department of Computer Science & Engineering
Shriram Group of Institutions
Jaballpur, (M. P.) [INDIA]
Email: *choudharysapna@gmail.com*

ABSTRACT

Most people now access all the important areas of their life—banking, shopping, insurance, medical records, and so on—simply by sitting at their computer and typing a username and password into a website. Getting access to something this way is called one-factor authentication, because you need to know only one thing to get into the system: the combination of user name and password. In theory, this kind of protection should be reasonably secure; in practice, it's less and less trustworthy. This paper presents an approach to further increase security using a two-factor authentication scheme. The One Time Password will be used for authentication any time the user wishes to access a restricted resource. The one time password as the name implies will expire after a single use and after a period of 60 seconds. The system uses random image and text based OTP generation with SHA-512 algorithm and again the concept of actual and fake OTP is introduced in the work.

Keywords:— *One Time Password (OTP), Image Based OTP, SHA based One Time Password, Time-based One Time Password (TOPT), Cryptography, Email, Authentication.*

I. INTRODUCTION

Despite the growing number of innovative ways to authenticate users, password-based authentication is still one of the most popular methods of all [1]. Passwords can easily be memorized and users at no cost are able to use them in their daily life [1]. On the other side, passwords can be forgotten because of mixture of different passwords of various accounts [2]. As time passes, different methods of authentication have gradually been introduced in the forms of biological and graphical passwords. The new emerging trends of authentication systems are a combination of two or more methods. These systems employ the combination to distinguish true users from so-called users. There are three main schemes into which authentication systems fall [3], namely what you know, what you have, and what you are. Figure 1 below shows the three main schemes.

Figure 1: Authentication System

One time passwords (OTPs), which can authenticate users by agreeing on the possession of a pre-shared value, are one of the most popular possession factors in two factor authentication (TFA or 2FA). TFA is a widely used subcategory of multi-factor

authentication (MFA). Knowledge factor, in practice, is the well-known username password pair. As this is the most widely deployed method of authentication, almost all TFA implementations include this factor and add one of the others.

Inherence factors are related to who the user is and what the user does. Authentication is fulfilled by using static biometric methods (e.g., fingerprint, palm, and retina scanning) and dynamic biometric methods (e.g., hand-waving, gait, touch-screen, keystroke, and voice analysis). Authentication by inherence helps to overcome the difficulties of carrying tokens, memorizing passwords, and identifying users. On the other hand, there are some challenges when designing biometric authentication.

Four major issues can be listed as follows: storing sensitive personal information is difficult, revocation and cancellation options must be available in case of a theft or a loss, biometric reader devices are costly and cannot be always available, and privacy concerns occur when organizations share their databases. Altogether, biometric authentication is difficult to adopt and manage in daily practice for regular users.

Due to the different means of authentication systems, it is clear that most of the authentication factors are not independently reliable and vulnerable to different attacks or their fault tolerance affect the output. Most of the authentication factors independently are vulnerable and that is why password based factor is still popular in most proposed systems.

In fact, multi-factor authentication is a chain of different steps to harden the process of user login to the system while other aspects like usability and performance will be affected by making the system more complex.

II. Literature Review

Two Factor Authentication via OTP /PIN: Google 2 step [4] verification is a two-factor authentication scheme which uses OTP as a second factor. The server sends OTP to the user's registered mobile number after receiving the user credentials. OTP, if entered correctly by the user, allows him to login onto the website. SAASPASS [5] is another two-factor authentication scheme which uses App generated PINs in place of SMS based OTPs. This reduces the cost of sending OTPs at every login. The user installs the SAASPASS App on his/her smartphone and links it with his/her personal web account. SAASPASS generates and displays a 6-character PIN to the user which is synchronized with the server and changes every 30 seconds. The user enters the PIN as the second factor for login verification. RSA Soft token, DUO also generate similar authentication code/ PIN through Apps for login. These schemes are vulnerable to MITM phishing attacks as the OTP/PIN can be acquired by a phishing website or through a malicious browser extension [Appendix].

Authentication using QR Codes: In Xie et al.'s [6] approach, a user submits the username and password to the website using a browser extension. The server generates and sends a barcode to the user. This barcode is displayed on the user's browser. The user scans the barcode using his smartphone App and after verification generates a vouch request in the form of a barcode which is scanned by the PC camera. The browser extension sends the vouch request to the server for final authentication. The approach claims to solve the problem of MITM phishing attacks and utilizes Diffie-Hellman to secure the communication channel between the user's browser and the server. Kim et al. [7] proposed an approach to provide security against MITM phishing attacks.

Their approach uses QR codes to exchange user credentials. It additionally uses the IP address of the Smartphone to verify the proximity of the user and the PC used for login. However, IP addresses can be spoofed which can cause the compromise of the scheme. The scheme proposed by Mukhopadhyay et al. [8] uses a third-party verifier. Both the third party and the user's Smartphone share a secret key. The third party checks the user credentials (submitted over the website) and after verification sends a challenge in an encrypted (using the shared secret key) QR code to the user. The user scans the QR code using his Smartphone App, verifies it, and sends back the encrypted response to third-party verifier. After verifying the response, third-party gives the user access to the server. In Dodson et al.'s [9] scheme, both the user and the server share a secret key which is used for authentication. The server sends a challenge to the user in the form of a QR code. The user's smartphone App encrypts the server challenge using the shared secret key and sends it back to the server. The server verifies the response and allows the user to log in. During our experiments, we found that none of these schemes are secure against the attacks described in the previous section.

Authentication using graphical password and CAPTCHA: Leung et al [10] proposed the concept of flash-based OTP CAPTCHA to avoid sophisticated attacks such as MITM and MEP attacks where attackers can capture the user's screen to steal credentials. The OTP CAPTCHA has moving digits. The user's mouse click coordinates and the time of click are sent to the server. Based on this information the server identifies the digits of the OTP, selected by the user. The scheme is not user -friendly and also fails in case of CR MITM attack. The scheme proposed by Zhu et al. [11] uses CAPTCHA as a graphical password. The user clicks his password characters displayed in the CAPTCHA and the coordinates of the mouse click are used by the server to verify the password. The scheme fails to handle MITM and screen logging attacks.

Authentication using push notification: In push notification based authentication, the user enters a user identification token (username) on the website while initiating a login session. Once the server receives the username from the user it generates a push notification message and sends it to the registered App running on the user's Smartphone. After the user approves the push notification message received on his App, the server allows the user to log in. Such push notification based login is provided by popular organizations such as Yahoo, Google etc. These schemes can be compromised using MITM attacks.

Authentication using separate hardware tokens: Schemes that require users to buy an additional dedicated hardware (Such as USB security keys, Smart cards etc.) for user authentication are considered as separate hardware token based schemes. Separate hardware tokens either store some cryptographic keys, passwords etc. which are communicated during the authentication process or the hardware tokens generate OTPs/PINs to be entered as the second factor during the authentication. The double armored Tricipher scheme [12] uses multipart credentials. One part of the credentials remains with the user whereas the other part is stored in a secure appliance kept in the enterprise data center. Moreover, a secret key is stored on the user's machine and is also known to the server. This key is used to encrypt the username and password entered by the user. The secure appliance signs (encrypts) the user credentials using the part of the credentials stored on it and sends them back to the user. The user sends these encrypted credentials directly to the

server. This completes the authentication process. The triple armored Tricipher scheme requires an additional hardware security key during the authentication process. Other hardware token based authentication schemes include RSA SecurID hardware tokens, U2F security keys such as Yubikey etc. RSA SecurID generates authentication code usually every 60 seconds using a clock and a random seed. The seed is provided to the token via the RSA server when the device is purchased. The server verifies the authentication code during the login by computing the authentication code which is valid at that moment using the seed stored in its records for the token and the value of the clock. If the code matches the user gets authenticated. Yubikey follows the U2F protocol for user verification during web authentication. Password managers: Password managers also provide an ease to user authentication. They store user credentials for individual websites and automatically enter them when the websites get visited by the user. Most of the password managers store the user credentials in an encrypted form in the browser storage and auto-fill them whenever the respective websites are opened in the browser. Password manager based schemes are vulnerable to MEP attacks. Other similar schemes include Ross et al. [13] where the authors used a browser extension to modify the password entered by the user, using the SALT stored at the client machine and the domain information of the website.

III. Proposed Work

Strong authentication systems address the limitations of static passwords by incorporating an additional security credential, for example, a temporary one-time password (OTP), to protect network access and end-users' digital identities. This adds an extra level of protection and makes it extremely difficult to access unauthorized information, networks or online accounts.

One-time passwords can be generated in several ways and each one has trade-offs in term of security, convenience, cost and accuracy. Simple methods such as transaction numbers lists and grid cards can provide a set of one-time passwords. These methods offer low investment costs but are slow, difficult to maintain, easy to replicate and share, and require the users to keep track of where they are in the list of passwords.

Our proposed system will generate secure One Time Password using text encryption with image. It uses SHA512 for this purpose. For providing extra layer of security proposed system will generate two OTPs – one is fake OTP (send to user) and another is actual OTP (used at the time of authentication). Genuine user uses an application which converts received fake OTP into actual than user enters actual OTP for authentication. This extra layer protects the system in various intrusions like email hack, device theft etc.

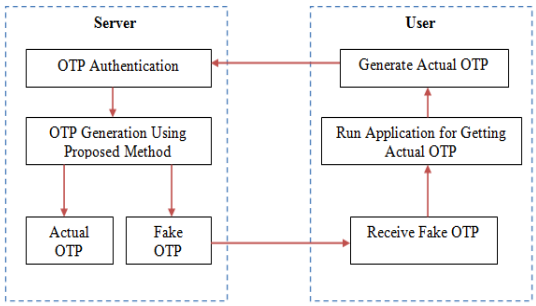

Figure 2: Proposed System

3.1 Proposed OTP Generation Method

The system is based on a synchronous stream cipher that uses images, instead of passwords, as the secret key. A synchronous stream cipher is a type of symmetric key algorithm that generates a pseudo-random sequence of bits, called the key stream, independent of the plaintext and cipher text. These bits are then combined with the

plaintext bits (usually using exclusive-or) to produce the cipher text, and then system will generate two OTP from cipher text. One is Actual OTP and another is Fake OTP. This Fake OTP will be sent to user's email or mobile. If user enters same OTP for authentication it will not work. Authorized user should use an application for converting this fake OTP to generate actual OTP. Than this actual OTP will be entered for authentication, it increases more security in the system.

Figure below represents process for OTP generation.

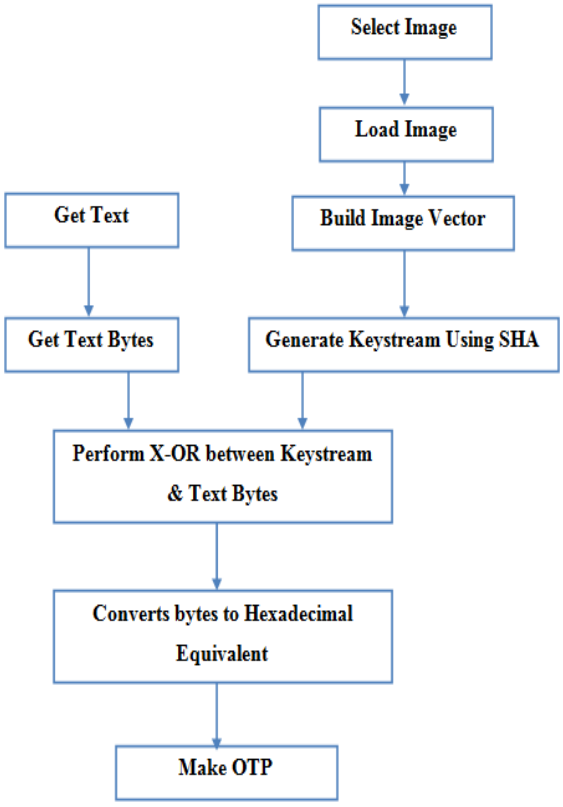

Figure 3: Proposed OTP Generation System

OTP generation starts by loading the image into memory and getting the input text bytes, and then building a vector by applying a transformation function to the image's pixels to be used later as the secret key. The system will then generate the keystream by combining multiple keys together. A single key is generated by a sequence of bit-shifting the image vector, then hashing it (using one of the Secure Hash Algorithms) and finally performing an exclusive-or between the image vector and the hash value. After generating all the keys required so that their combined bytes are equal to or greater than the input text bytes, the remaining process is simply performing an exclusive-or operation between each keystream byte with the input text bytes. The system will then represent the resulting bytes by a readable form, which may be the hexadecimal values of the encrypted bytes. Theses bytes will produce fake and actual OTP.

IV. RESULTS AND DISCUSSION

Information and data security are based on factors such as authenticity, accuracy, availability, data credibility, confidentiality and no repudiation. The proposed approach has the ability to contribute to the necessary data and information security. It uses authentication token as certificates to prove authenticity.

Proposed system generates One Time Password by manual selection of image, text, method and number of threads because parameters can be analyzed, but in actual system these will be automatically selected. Automatic selection of images and text from large corpus will increases randomness in the system, which will increase more security also. Image and text may also be selected in real time from web. So there is no way to guess selected image and text. Our proposed system will generate OTP in alphanumeric form which is also more secure than numeric OTP.

Proposed system will generate two OTP- one is actual and another is fake (generated from actual by own encoding method). Actual OTP is stored at the side of server while fake OTP will be sent to user. So

every user will get fake OTP whether user is authorized or not. If unauthorized user enters fake OTP for authentication, it will not match. Authorized user should use an application provided by system for converting fake OTP into actual OTP. Then user can be authorized. So it will provide more security against device theft or email hacking.

Proposed system uses SHA 512 method to encrypt text from image. Key stream will be generated from image which is more secure than other versions of SHA like 128, 256.

Our proposed system surpasses all the problems of password based mechanism. It keeps resistance against the following security hazards and susceptibility:

Token theft*:* Since we have two security tokens as OTP- actual and fake OTP. User should also require an application to decode fake OTP into actual OTP. There is no chance of token theft.

Token Duplication*:* Due to randomness of image and text there exist no chance of duplication of OTP.

Replay Attack*:* No chances of replay attack.

Eavesdropping*:* OTP received by user is fake. Fake OTP makes eavesdropping almost impossible for attackers.

Man-in-the-middle attack*:* System protects against Main In the Middle attack because of system generated fake OTP and use of own application for conversion of fake OTP into actual.

Evaluation on the basis of OTP Generation Time

Chart below represents comparison of OTP generation time for all samples

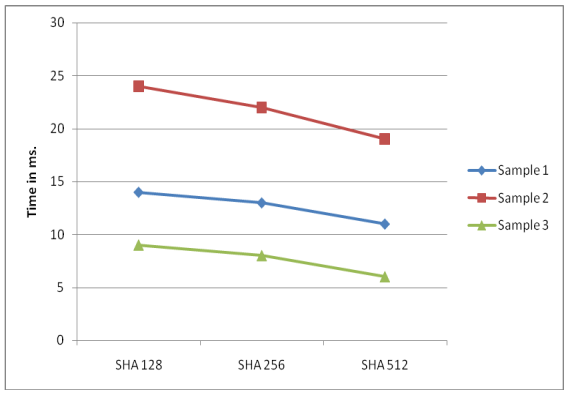

Figure 4: Chart for OTP Generation Time

V. CONCLUSION

To sum up, authentication systems can be simple at the first glance. But in fact, they are complex in security, usability and availability aspects. As poorly chosen passwords could not protect users properly, Multi-factor authentication systems presented in different ways to increase the reliability of authentication systems. In this thesis, we reviewed many of those factors in different systems such as SMS, time-based and hardware-based tokens. Despite the security advantages and deficiencies, each of the aforementioned factors affects the usability, cost-effectiveness, availability and implementation of an authentication system. Clearly, the user must come first in a multi-factor authentication system and since the influence of the technical issues is significant, it is an arduous task to achieve this trade-off in an authentication system. However, each of three authentication methods has some issues which make them not reliable separately.

Therefore, we suggest a new authentication and integration framework for cloud computing to secure data and information hacks. User authentication in proposed work is performed on the basis of secure OTP & user name and email password. It is verified on the basis of several security aspects and is verified to be available, accessible, feasible, secure, and user-friendly and provides strong authentication

system. The proposed framework shows the close agreement with the standard criteria for security.

In this thesis we propose a novel lightweight identity authentication based access control scheme for cloud. We propose offbeat classification system for existing authentication methods in cloud computing. We present an analogously analysis and recommends future research in improving the surveyed implicit authentication in Cloud Computing.

REFERENCES:

[1] Shen, C., Yu, T., Xu, H., Yang, G., & Guan, X. (2016). User practice in password security: An empirical study of real-life passwords in the wild. Computers and Security, 61, 130–141. https://doi.org/10.1016/j.cose.2016.05.00.

[2] Nicholson, J., Coventry, L., & Briggs, P. (2013). Faces and Pictures: Understanding age differences in two types of graphical authentications. International Journal of Human Computer Studies, 71(10), 958–966.

[3] Almuairfi, S., Veeraraghavan, P., & Chilamkurti, N. (2013). A novel image-based implicit password authentication system (IPAS) for mobile and non-mobile devices. Mathematical and Computer Modelling, 58(1–2), 108–116. https://doi.org/10.1016/j.mcm.2012.07.00.

[4] Google. Using security key for 2-step verification . Available: https://suppor.google.com/accounts/answer/6103523 .

[5] Barker I Saaspass makes two-factor authentication available to the masses . Available: https://betanews.com/2015/01/15 saaspass-makes- two- factor- authentication-available- to- the- masses.

[6] Xie M , Li Y , Yoshigoe K , Seker R , Bian J . CamAuth: Securing Web Authentication with Camera. In: High Assurance Systems Engineering (HASE), 2015 IEEE 16th International Symposium on; 2015. p. 232–9 .

[7] Kim S-H , Choi D , Jin S-H , Lee S-H . Geo-location based QR-Code authentication scheme to defeat active real-time phishing attack. In: Proceedings of the 2013 ACM workshop on Digital identity management; 2013. p. 51–62 .

[8] Mukhopadhyay S , Argles D . An Anti -Phishing mechanism for single sign-on based on QR-code. In: Information Society (i-Society), 2011 International Conference on; 2011. p. 505–8.

[9] Dodson B, Sengupta D , Boneh D , Lam MS . Secure, consumer-friendly web authentication and payments with a phone. In: International Conference on Mobile Computing, Applications, and Services , Santa Clara; 2010. p. 17 –38 .

[10] Leung C-M . Depress phishing by CAPTCHA with OTP. In: Anti-counterfeiting, Security, and Identification in Communication, 2009. ASID 2009. 3rd International Conference on; 2009. p. 187–92 .

[11] Zhu BB, Yan J, Bao G , Yang M , Xu N . Captcha as Graphical Passwords-A New Security Primitive Based on Hard AI Problems. IEEE Trans Inf Forensics Secur 2014;9:891–904 .

[12] TRICIPHER, “Preventing man in the middle phishing attacks with multi-factor authentication,” 2016.

[13] Ross B, Jackson C, Miyake N, Boneh D, Mitchell JC. Stronger Password Authentication Using Browser Extensions. In: Usenix security; 2005. p. 17–32.

* * * * *