IJCSE International Journal of Computer Sciences and Engineering Open Access
Research Paper Vol.-7, Special Issue-10, May 2019 E-ISSN: 2347-2693

Authentication Using Improved Image Based OTP

Shweta Gupta[1*], Prateek Gupta[2], Amit Ranjan [3]

[1,2,3] Department of Computer Science & Engineering, SRIST, Jabalpur, MP, India

[*]*Corresponding Author: shwetag63@gmail.com, Tel.: +91-7999874162*

DOI: https://doi.org/10.26438/ijcse/v7si10.6467 | Available online at: www.ijcseonline.org

Abstract**—** Everything in our digital life requires an authentication mechanism to establish the identity of the user and protect his/her privacy. Since passwords are the most common form of authentication, our aim is to provide an alternative form that is not susceptible to the security risks and problems associated with passwords. However, the password may be foreseeable because it should be easy for users to memorize. Thus, an rival could get the passwords of users by brute-force attack in a short period of time. Two-Factor Authentication (TFA) can be used as a antidote to this weakness. One Time Password is mostly used authentication method now days. Our proposed idea is to enhance the security level of One Time Password by using improved and more secure image based OTP. In this method text fields are encrypted with image as key string to produce OTP. Proposed method keep resistance against token theft, man in the middle attack, reply attacks etc.

Keywords**—**Authentication, TFA, MFA, OTP, Image OTP

I. INTRODUCTION

Banking and financial industry, during the last few decade, have shown exceptional growth in volume and complexity [1].The growth of both the industries has developed the traditional banking system to the digital banking system. In the Online banking system an important development has been under great consideration from the security perspective. The security for online banking has changed considerably during the relative short period of its existence. With the instigate of android phones in 2007, the rise of the Android platform has been meteoric. As Mobile equipment play an important role in today's world and have become an integral part of our daily life as one of the predominant means of communication [2], more and more people pay attention to the security of the Android applications. According to 2014 Juniper Networks report, and follow up press release, they found "a 372% increase in Android malware samples since July 2015" [3].

User authentication is a process to manifest that whether a user is permitted to use a target service or system. There are assorted user authentication methods such as knowledge-based authentication, ownership-based authentication and attribute-based authentication. Among them, knowledge-based authentication is broadly used these days, such as ID/PASSWORD in most websites or services [5]. However, the password may be foreseeable because it should be easy for users to memorize. Thus, an rival could get the passwords of users by brute-force attack in a short period of time. Two-Factor Authentication (TFA) can be used as a antidote to this weakness [4]. OTP (One Time Password) are very much popular for two factor and strong authentication. A One-time password (OTP) is a password that is valid for only one login session or transaction, on a computer system or other digital device [10]. OTPs circumvent a number of shortcomings that are associated with traditional (static) password-based authentication [5]. Image based OTP (IBO) depicts how One time password is generated by using the features of images which is used for authentication process. IBO shows generation of numerous OTP's from a single image and is highly secure compared to the conventional methods. Proposed work consists of development of more secure OTP generation method.

II. RELATED WORK

Existing techniques which are used for OTP Generation are mentioned below. These user authentication techniques take different criteria to authenticate the users using OTP.

SMS End-to-End Encryption

The first scheme uses end-to-end encryption to protect OTP messages when the SMS message gets obstruct or eavesdropped on. The OTP generated is encrypted using the powerful AES algorithm. The generated OTP value is encrypted using powerful AES algorithm and sends it to users.AES is an iterative and asymmetric key block cipher that uses key strengths of 128, and 256 bits. The AES uses 128 bits as a block for encryption and decryption. It is one of the perfect cryptography algorithms to protect personal data. The encrypt AES tool converts the input plain text to cipher text in a number of repetitions based on the encryption key. The AES decrypt method uses the same process to transform the cipher text back to the original plain text using the same encryption key. It is very difficult to break even using brute force attack. The encrypted OPT password is send to mobile through Bluetooth technology or modem [6]. The drawback of this method is that it has large system load for encryption and decryption.

Virtual Dedicated channel on the Handset

The mobile Trojans are major threats to the SMS OTP. A virtual dedicated channel is created to protect against Trojan attacks that requires little support from operating system manufacturers and minimal-to-no support from the service provider and cellular network operators. This dedicated channel inside the mobile phone *OS* by removing *certain* SMS messages from the general delivery process on the phone and redirecting them to a special OTP application. The endpoint of the virtual dedicated channel is an application with similar functionality to the default SMS application. It receives and stores SMS messages. The only difference is that it will only receive OTP messages, and that its message store cannot be read by other applications. [7].The server should distinguish the confidential messages from the normal ones. The drawback of this method is that the message is not encrypted while storing and it also required virtual network which increases the implementation cost.

OTP Generation using SHA-1

In generation of OTP there are many factors that can make OTP unique every time it is generated. In proposed system [8] OTP generation using SHA-1 is done by merging more than one unique factor that makes OTP unique in every generation. All data about user who is accessing the application will be fetched by server, i.e. Mobile number of the user, current time of application access, account number of user etc.

When all required information is yield, system will convert data into a string form using system code. Now that string will be considered as message in SHA-1 algorithm.SHA-1 algorithm will calculate hash string of 160 bits long. After calculation of SHA-1 hash value proposed method will be applied. And it will send 5 digit long numerical OTP to the registered mobile number of the user.

The drawback of this method is that it is only limited to Bank Application. The size of OTP is only 5 digits that are easy to crack.

Every year cyber onslaught advances to widen in frequency, resolution and impact. In the year 2015, the detected information security incidents were marked to 38% [11]. Most companies today seize advanced authentication as OTP service. This is clear from the fact that 95% of top organizations use highly secured authentication mechanisms such as OTP to ensure safety. Let us take a close look to expanding use of OTP. In the following survey we have the data for various years and present day adaptability scenario for OTP [12].

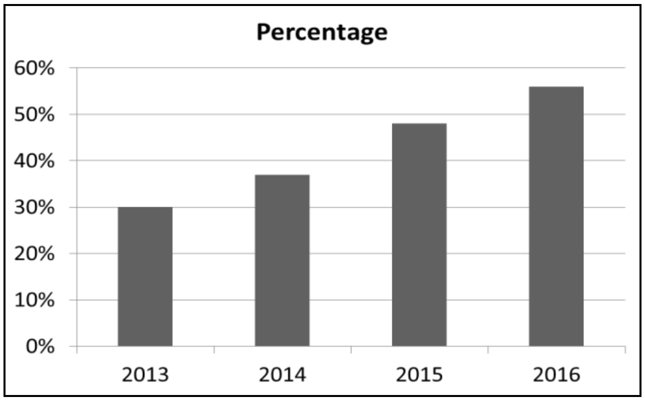

Figure 1: Yearly Adaptability of OTP Authentication in organizations

The comparison of different attack methods [14] is shown in table.

Table 1. Attacks

Attack Method	Attack Location	Examples
MITM (Man-in-the-Middle) [5]	Access path, channel	Attacking network segment
MITB (Man-in-the-Browser) [8]	Web browser	IE, JavaScript
MITPC/PHONE (Man-in-the-PC/PHONE)[13]	PC or Mobile Device	API monitoring , screen capturing etc

Now we will take a look on different OTP Generation ideas implemented based on previous research articles

Table 2. Related Work

Method	Advantages	Limitations
Text Based SMS [5]	Fast To Generate	Easy to Crack
Variable size Text SMS With Feistal Network [7]	Due to variable size hard to crack, More Secure With More number of rounds in the network.	Number of Rounds in the Network Increases the OTP Generation Time, hence Increases the Time complexity
OTP Generation Using SHA-1 [8]	Security is High Due To hashed function. Hard to crack	Text SMS is generated using mobile number and account number which is easy to guess
OTP Generation using RSA [9]	Due to Large prime number ,OTP generated is hard to crack. More secure.	OTP is stored on user machine without encryption .For same security level RSA uses Big Size key as compared to ECC.

III. METHODOLOGY

When the user registers for the first time on the website, they are required to select a set of four images randomly from predefined large set of images such as natural scenery, automobiles etc. Every time a user login into the website or service, they are provided a user id and password. After first authentication, our system generates OTP using one of image selected at the time of registration with sha-512 encryption along with randomly selected text fields given at the time of registration. Than system select first 8 characters of cipher text and encrypt it with ECC . Than produced OTP will be stored and 8 character cipher text will be sent to user by email. When user enters OTP for validation again it will be decrypted using ECC and matched for authentication.
Work flow of proposed system is shown below:

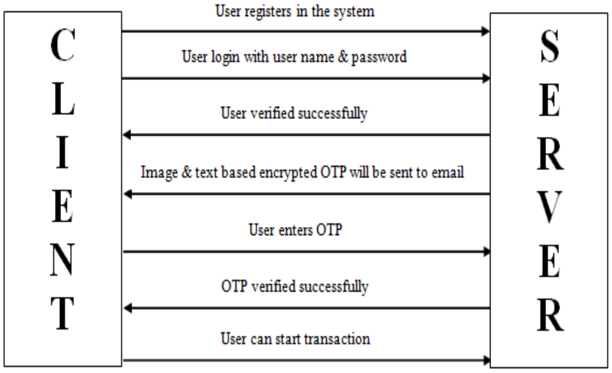
C L I E N T
User registers in the system
User login with user name & password
User verified successfully
Image & text based encrypted OTP will be sent to email
User enters OTP
OTP verified successfully
User can start transaction
S E R V E R

Figure 2: proposed work

User enters his/her details like user name, password, address, email address, date of birth etc. Users also selects four images among many images and submit the detail. That information will be stored in database for further uses.

User should login with registered user id and password, if login is successful than this module generates OTP based on a synchronous stream cipher that uses images, 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. The system 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 key stream 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 key stream 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 in the case of encryption.

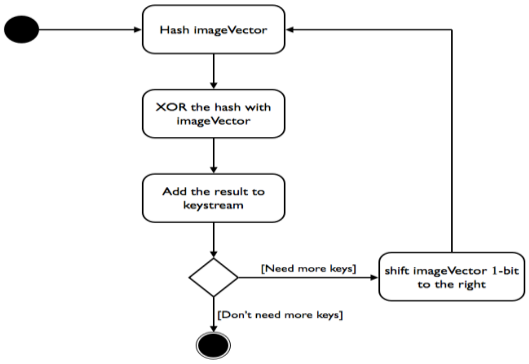
Hash imageVector
XOR the hash with imageVector
Add the result to keystream
[Need more keys]
shift imageVector 1-bit to the right
[Don't need more keys]

Figure 3: Key stream generation

A bit-wise circular right-shift simply means moving the bits in the array one step to the right, and the right-most bit becomes the left-most bit in the array. This is done to ensure that each key is different from the other keys in the key stream .Getting a hash value in Java is achieved using the Message Digest class in the java.security package. This class has a static method getInstance(String, String) that takes the name of the algorithm required and an optional argument for the name of the provider of the algorithm (e.g. Sun, Bouncy Castle, etc.) and returns a Message Digest instance that can be used to get hash values.

User entered OTP will be checked according to session and time. If it is within time than entered OTP will be decrypted by ECC & matched with stored encrypted OTP . If they matched than OTP is authorized so user can perform transaction otherwise message will be communicated to user. The process of generating the full key stream is illustrated in figure.

IV. RESULTS AND DISCUSSION

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

1. **Token theft**: Since we have two security tokens as OTP and Auth_code, it is difficult to ransack the tokens and is possible only if one's phone is stripped away.
2. **Token Duplication**: If an assaulter cannot steal the password he would try to duplicate it, hence it should not be written down. Along with it we have encrypted it with ECC algorithm.
3. **Replay Attack**: Since the OTP and Auth_code value changes every time a user logs in. Replay attack would not be possible in this solution.

4. **Eavesdropping**: Storage of passwords in encrypted form makes eavesdropping almost impossible for attackers.
5. **Man-in-the-middle attack**: As the credentials are unrevealed to any third person and also the client and server use their public private keys for authentication, this attack is not possible.

A sample result for OTP generation time is shown in figure below:

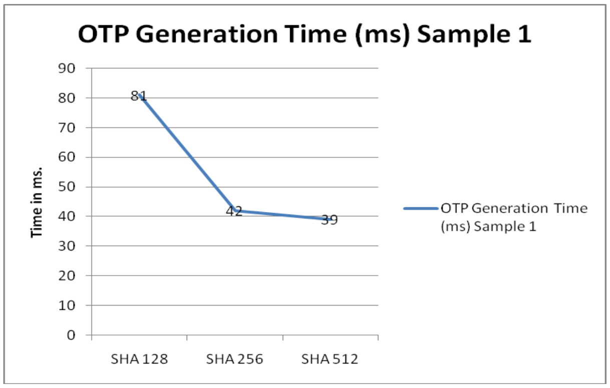

Figure 3: Comparison of OTP generation time

V. CONCLUSION AND FUTURE SCOPE

Our proposed system Image Based OTP Generation surpasses all the problems of OTP based Authentication mechanism. It has been tested under various test cases. In this research paper we have proposed Image Based OTP-Generation method for enhancing the security to the next level. This is a simple but an effective measure to combat the different online account thefts and frauds to secure our m-commerce transactions. In the future, this OTP generation can use with more cryptographic hash functions. As newer algorithms getting advised (like HMACSHA-3),this system can generate more unique OTPs to secure the system.

REFERENCES

[1] Leeladhar, V. “*Taking Banking services to the common man-financial inclusion”*. Reserve Bank of India Bulletin, (2006).

[2] Davi, L., A. Dmitrienko, et al.,“*Privilege Escalation Attacks on Android Information Security*,” M. Burmester, G. Tsudik, S. Magliveras and I.Ilic, Springer Berlin /Heidelberg. 6531: 346-360, 2011.

[3] “*Juniper Networks.Mobile Malware Development Continues To Rise,Android leads The Way”*. Available at http://globalthreatcenter.com/?p=2492, 2011.

[4] Ausitn, Charles Frederick, Xingsheng Wan, and Andrew Wright. ”*Two factor authentication”*, U.S. Patent Application 13/748, 153

[5] K. Rieck, P. Stewin, and J.-P. Seifert ,“*SMS-Based One-Time Passwords: Attacks and Defence*” DIMVA 2013, LNCS 7967, Springer-Verlag Berlin Heidelberg 2013,pp. 150–159, 2013.

[6] *“Man in the Middle”* Available on http://securityblog.s21sec.com/2010/09/zeus-mitmo-man-in-mobile-i.html 2010

[7] Dr. Ananthi Shesashaayee, D. Sumathy*” OTP Encryption Techniques in Mobiles for Authentication and Transaction Security*” IJIRCCE Vol 2, Issue 10, Oct 2014.

[8] Mohammed Hamid Khan “*OTP Generation using SHA-1*” IJRITCC Vol 3, Issue 4, Apr 2015.

[9] Safa Hamdare, Varsha Nagpurkar, Jayashri Mittal “*Securing SMS Based One Time Password Technique from Man in the Middle Attack”*, (IJETT)-Volume 11 Issue 3- May 2014.

[10] Himika Parmar1, Nancy Nainan2 and Sumaiya Thaseen, “*Generation 0f Secure One-Time Password Based On Image Authentication*”, CS & IT-CSCP 2012.

[11] Pwc, “*pwc cybersecurity*,” Pricewaterhouse Coopers, 2016. [Online]. Available: http://www.pwc.com/gsiss. [Accessed 30 May 2016].

[12] TechTarget .(2015,March).Retrieved May 20, 2016,

[13] Hoyul Choi, Hyunsoo Kwon “*A Secure OTP Algorithm Using a Smartphone Application*”, IEEE-2015.

[14] Changsok Yoo, Byung-Tak Kang, Huy Kang Kim, ”*Case study of the vulnerability of OTP implemented in internet banking systems of South Korea*”, An International Journal Springer Science+Business Media New York 2014, 10.1007/s11042-014-1888-3, 2014.

Authors Profile

Ms. Shweta Gupta pursed Bachelor of Engineering from CSE, SRIST, Jabalpur. Currently pursuing MTech in CSE from SRIST, Jabalpur.

Prof. Prateek Gupta pursed Bachelor of Engineering from CSE, GRKIST, Jabalpur and Master of Technology in Comp. Sc. & Engg. From SSSIST, Sehore. He is currently pursuing Ph.D. from MITS Gwalior and working as an assistant profesor in SRIST, Jabalpur. He is having more than ten years of teaching experience. He has published more tha ten research papers.

Prof. Amit Ranjan pursed Bachelor of Engineering from CSE, GRKIST, Jabalpur and Master of Technology in Comp. Sc. & Engg. From RGPV, Bhopal. He is currently working as an assistant profesor in SRIST, Jabalpur. He is having more than five years of teaching experience.