International Journal of Scientific Research in Computer Science, Engineering and Information Technology
© 2017 IJSRCSEIT | Volume 2 | Issue 5 | ISSN : 2456-330

Intensify Login Security by Using Extra Authentication level with OTP

Gagan Madaan
Assistant Professor, Department of Computer Science & Applications, S.U.S. Panjab University Constituent College Guru Harsahai, Punjab, India

ABSTRACT

In Online based applications most of them used static passwords. In that they follow multiple technics to secure their credentials. For examples: Multi level password authentications, hard codes, Session Passwords, bio- matric technics, and One Time Password. Every method has some advantages and disadvantages. Our proposed idea is to enhance the security level of One Time Password by Using Extra Authentication level with the OTP also called Two-factor authentication. It increases the security level of the system.

Keywords : Authentication, Security, One-Time Password;

I. INTRODUCTION

In the present digital day with remarkable development in Computer sector, Securing the system and remote access using passwords is not easy in the World Wide Web. Simple, obvious and easy-to-guess passwords, such as names and age, are effortlessly found via computerized secret key gathering programs and expanded access to information increases weakness to hacking, cracking of passwords and online frauds. Security is a major concern today in all sectors such as banks, governmental applications, military organization, educational institutions, etc. The rapid growth in the number of online services leads to an increasing number of different digital identities each user needs to manage. Users tend to use easy-to-guess passwords, use the same password in multiple accounts or store them on their machines, etc. Furthermore, hackers have the option of using many techniques to steal passwords such as shoulder surfing, snooping, sniffing, guessing, etc. Moreover passwords can be written down, forgotten and stolen, guessed deliberately being told to other people.

Thus conventional login/password authentication is not secured for several security-critical applications such as login to Mailing Accounts, Social Networks, Gadgets, Financial accounts, official secured networks, commercial websites online etc. Obliging more than one independent security level increases the difficulty of providing false credentials.

Several proper strategies for using passwords have been proposed. Some of which are very difficult to use and others might not meet the company's security concerns. Some solutions have been developed to eliminate the need for users to create and manage passwords. Our

Solution is typical based on that we will ask another Authentication factor (like he will be asked to enter the full mobile number that is linked with account, enter date of birth or any other security questions that are answered while creating a account) before sending an OTP to client. As only Authenticating the user only based on the OTP is not secured, as the mobile on which the OTP is sent can be lost.

OTP with Extra Authentication level proposal guarantee a higher protection level by extending authentication factor. This paper focuses on the implementation of OTP with Extra Authentication level and thus affording an additional password adds an extra layer of security. The paper is organized in such a way that section 2 briefs about existing authentication methods, section 3, explains about proposed method, system design and system implementation, section 4 explains about proposed method advantages & disadvantages.

II. EXISTING AND PROPOSED AUTHENTICATION METHOD

The impact of the Internet over the last few years has meant fundamental changes in the way we access business systems. The network security perimeter has crumbled at all levels while the number of users wanting network access has grown. The geographical location of users has also widened to a situation where they can be, not just in a different department or company branch office, but anywhere in the world. While there are enormous productivity benefits available from increased access, the security risks have greatly increased. The traditional method of securing system access was by authentication through the use of passwords. Unfortunately, traditional password authentication is totally unsuitable for securing the access requirements of today's distributed users. According to the DTI Information Security Breaches Survey 2006, businesses are still overwhelmingly dependent on user IDs and passwords to check the identity of users attempting to access their systems. Weak single factor authentication is the use of single static passwords and still employed by most companies. The benefit is that static passwords are easy to remember. However, when you have different passwords for different systems, they start to become very difficult to remember and have to be written down, making them vulnerable. The many disadvantages of single static passwords include how easy it is to crack them. They are short and based on topics close to the user, such as birthdays, partner names, children's names etc; and they are typically letters only. They are also vulnerable to social engineering i.e. people asking for your password or guessing it. They can also be picked up by spyware. The alternative method of password management is to change passwords regularly. Operated correctly, this has the benefit of being more inherently secure than static passwords. A disadvantage of frequently changing passwords is that they can be easily forgotten, leading to very high support costs and significantly increased administration costs. This is particularly relevant for larger organizations with hundreds of applications.

The goal of computer security to maintain the integrity, availability, and privacy of the information entrusted to the system can be obtained by adapting this authentication technique .As per defenders, Using Extra Authentication level with the OTP also called Two-factor authentication could definitely lessen the occurrence of online fraud, and other online extortion. This type of authentication is not a new concept for an example considering the banking industry without replacing the existing authentication system, instead serves as an added layer of security that protects and enriches the existing authentication system. The proposed system is an information security process in which two means of identification are combined to increase the probability that an entity, commonly a computer user, is the valid holder of that identity.

III. SYSTEM DESIGN AND IMPLEMENTATION

In this paper, we propose a computer-based software token along with the security questions that are asked before generating the OTP. In the System firstly the user are asked the Questions, he has to answer the question in the same way as he is answered while creating a account. After validating the security questions ,the System process involves generation of Secured OTP using Cryptographic algorithm and delivering it to user's mobile in the form of SMS or user can able to create his own OTP using smartphone and validating the OTP using same Cryptographic algorithm. The proposed system is secured and consists of two parts: (1) the server software, (2) the client software: Client application on PC for transaction & android application on smartphone for creating OTP.

So the Proposed System can be Majorly Cauterized into two parts.
(1) Validating the **Security Questions**.
(2) Validating the **One Time Password (OTP)**.

3.1 Security Questions: Security question is one type Authentication method that helps us to verify client in manycases as in case of Login password is Forgotten or Before generating the OTP and sending it to user mobile ,the security question must be asked because only OTP is not Secured to Authenticate the Client as One Situation is that the client mobile can be lost or theft then in that case, the alpha-numeric password can be hacked as it may be stored in the User Mobile Browser ,then by easily generating the Only OTP method the client account can be accessed. So we propose a method to use the security question before generation the OTP. These question are asked to the user at the time of account-id creation and stored in the database.

What makes a good security question? A good security questions should possess the followings Properties:

Safe: cannot be guessed or researched
Stable: does not change over time
Memorable: can remember
Simple: is precise, simple, consistent
Many: has many possible answers

- **Childhood Related**

What was your childhood nickname?
What is the name of your favorite childhood friend?

- **Family Related**

In what city or town did your mother and father meet?
What is the middle name of your oldest child?

- **Favorites Related**

What is your favorite team?
What is your favorite movie?

- **Favorites Historical Related**

What was your favorite sport in high school?
What was your favorite food as a child?

- **Firsts Related**

What is the first name of the boy or girl that you first kissed?
What was the make and model of your first car?

- **Personal Characteristics**

What was the name of the hospital where you were born?

Who is your childhood sports hero?

- **Education**

What school did you attend for sixth grade?

What was the last name of your third grade teacher?

- **Work**

In what town was your first job?

What was the name of the company where you had your first job?

3.2 One Time Password (OTP):

A one-time password (OTP) is a password that is valid for only one login session or transaction. OTPs avoid a number of shortcomings that are associated with traditional (static) passwords. The most important shortcoming that is addressed by OTPs is that, in contrast to static passwords, they are not vulnerable to replay attacks. This means that a potential intruder who manages to record an OTP that was already used to log into a service or to conduct a transaction will not be able to abuse it, since it will be no longer valid. On the downside, OTPs are difficult for human beings to memorize. Therefore they require additional technology to work.

How to generate OTP and distribute?

OTP generation algorithms typically make use of pseudo randomness or randomness. This is necessary because otherwise it would be easy to predict future OTPs by observing previous ones. Concrete OTP algorithms vary greatly in their details. Various approaches for the generation of OTPs are listed below:

- Based on **time-synchronization** between the authentication server and the client providing the password (OTPs are valid only for a short period of time)

- Using a mathematical **algorithm** to generate a new password **based on the previous password** (OTPs are effectively a chain and must be used in a predefined order).
- Using a mathematical **algorithm** where the new password is **based on a challenge** (e.g., a random number chosen by the authentication server or transaction details) and/or a counter.

3.3 OTP Algorithm:

in order to secure the system, the generated OTP must be hard to guess, retrieve, or trace by hackers. Therefore, it is very important to develop a secure OTP generating algorithm. Several factors can be used by the OTP algorithm to generate a difficult-to-guess password. Users seem to be willing to use simple factors such as their mobile number and a PIN for services such as authorizing mobile micro payments, so we propose a Secured Cryptographic algorithm

The unique OTP is generated by the mobile application offline, without having to connect to the server. The mobile phone will use some unique information in order to generate the password. The server will use the same unique information and validate the OTP. In order for the system to be secure, the unique OTP must be hard to predict by hackers. The following factors will be used to generate the OTP:

IMSI number: The term stands for International Mobile Subscriber Identity which is a unique number associated with all GSM and Universal Mobile Telecommunications System (UMTS) network mobile phone users. It is stored in the (SIM) card in the mobile phone. This number will also be stored in the server's database for each client. **ATM PIN:** Needed for verifying the authenticity of the client. If the phone is stolen, a valid OTP can't be generated without knowing the user's PIN. The PIN isn't stored in the phone's memory. It is only being used only to generate the OTP and destroyed immediately after that.

Timestamp: Used to generate unique OTP, valid for a short amount of time. The timestamp on the phone must be synchronized with the one from the server.

DOB: Date of birth of user whose going to use the application.

Username: Username of customer provided by bank.

How OTP Generated: The Username, password, date of birth of user is taken from the user and then concatenated with the current date, time and the time stamp for which the one time password is valid. This concatenated string is then given as input to Secured Hash Algorithm (SHA1) Algorithm. SHA- 1 algorithm returns its message digest which is 20 bytes value. These 20 bytes are reduced to 5 bytes by XORing a group of 4 bytes , i.e byte no. 1, 4, 8, 12 are XORed ; 2, 5, 9, 13; 3, 6, 10, 14; 4, 7, 11, 15; 5, 8, 12, 16; 17, 18, 19, 20 are Xored. Then from this 5 byte value, every byte is right shifted with 4 digits and then is converted to hexadecimal. Finally by converting the ASCII values to a character string, it is displayed as a onetime password to the user.

IV. ADVANTAGES AND DISADVANTAGES:

Requiring more than one independent factors like security questions along with the OTP increases the difficulty of providing false credentials. Still there will be limitations for implementing this method. If the proposed system is implemented then the advantages are (i) It improves Information Security (ii) there will be Secured Login - Secures websites, portals and web applications (iii) Since there is two level protections it will be Defense in depth. (iv) Ease to implement. On the subject of the weakness (i) Remembering ability of all security questions(ii) Space Complexity as all the security question & answers related to each user are stored in the database (iii) System Configuration so as to assist the second gateway which is OTP based and (iv) also take additional time.

V. CONCLUSION

Advancement in authentication techniques has to check out tomorrow's validation necessities not today's. At the point when all is said in done, one needs to spend more to get bigger measure of security. Maintaining and Keeping up security to a standard is going to be tougher and troublesome with time. Some of the challenges can be anticipated, such as advances in computation that are making it progressively easier to dictionary-attack a password database. Different difficulties are harder to foresee, for example, the revelation of new "day-zero" vulnerabilities in working programming. Consequently, security prerequisites are not altered, yet increment with time. One Time Password by Using Extra Authentication level also called two-factor verification is frequently being utilized to work around the basic shortcomings in password administration. While two-factor verification does enhance security also it builds client resistance. Integrated two factor authentication gives the best convenience to better security, so a two-factor confirmation innovation that can be moved up to coordinate the two elements all the more nearly has the best capacity to become as requirements change and also to amplify client uptake of discretionary two factor authentication. As the confirm mechanism for authentication our view can be suitably and securely used. The fundamental thought is that using our proposed two factor authentication will provoke more essential security. This, accordingly, should formulate universal security.

VI. REFERENCES

[1]. http://searchsecurity.techtarget.com/definition/multifactor-authentication-MFA.

[2]. McAfee Case Study "Securing the Cloud with Strong Two-Factor Authentication through McAfee One Time Password" http://www.mcafee.com/in/casestudies/cs-cloudalize.aspx.

[3]. http://www.oneid.com/wpcontent/uploads/2014/05/OneID_WhitePaper_Adv-of-Integrated-2FA-final.pdf.

[4]. Edward F. Gehringer "Choosing passwords: Security and Human factors" IEEE 2002 international symposium on Technology and Society, (ISTAS'02),\ ISBN 0-7803-7284-0, pp. 369 - 373, 2002.

[5]. Sagar Acharya, Apoorva Polawar, Priyashree Baldawa, Sourabh Junghare, P.Y. Pawar " Internet Banking Two Factor Authentication Using Smartphone" , IJSER, IJSER, Volume 4, Issue 3, March Edition, 2013, (ISSN 2229-5518)

[6]. Aladdin Secure SafeWord 2008. Available at http://www.securecomputing.com/index.cfm?skey=1713

[7]. Asif Amin, Israr ul Haq2, Monisa Nazir3, "Two Factor Authentication" International Journal of Computer Science and Mobile Computing, july 2017

[8]. Ms. E.Kalaikavitha,Mrs. Juliana gnanaselvi "Secure Login Using Encrypted One Time Password (Otp) and Mobile Based Login Methodolo " International Journal Of Engineering And Science ,Apr 2013

[9]. The mobile phone as multi otp device using trusted computing http://eprints.qut.edu.au/37711/

[10]. H. Wang, "Research and Design on Identity Authentication System in Mobile-Commerce", In: Beijing Jiaotong University, 2007, pp. 18-50.

[11]. Ziqing Mao, Dinei Florencio, and Cormac Herley "Painless Migration from Passwords to Two Factor Authentication" in 'WIFS' , IEEE, Brazil, pp. 1-6, Nov 29th-Dec 2nd, 2011.

[12]. Manav Singhal and Shashikala Tapaswi "Software Tokens Based Two Factor Authentication Scheme" International Journal of Information and Electronics Engineering, Vol. 2, No. 3, pp. 383 - 386, May 2012.

[13]. Olufemi Sunday Adeoye "Evaluating the Performance of two-factor authentication solution in the Banking Sector" IJCSI International Journal of Computer Science Issues, Vol. 9, Issue 4, No 2, July 2012.

[14]. Goode intelligence "Two Factor Authentication Goes Mobile" www.goodeintelligence.com, September 2012.

Author Profile:

Gagan Madaan received his B.C.A. degree from Panjab University Chandigarh and M.C.A. Panjab University Chandigarh in 2012 and 2015 respectively. He is currently an Assistant Professor in S.U.S. Panjab University Constituent College Guru Harsahai, Punjab, India with 2 years of experience. He was awarded with the Gold Medal in BCA at college level & in M.C.A. at University Level by the Governor of Punjab & Haryana for his academic Excellence. He has also Qualified UGC-NET in the subject of Computer Science.