Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X
IMPACT FACTOR: 6.017

IJCSMC, Vol. 6, Issue. 7, July 2017, pg.5 – 8

TWO FACTOR AUTHENTICATION

Asif Amin[1], Israr ul Haq[2], Monisa Nazir[3]

[1]Student, Computer Science Engineering, SSM College of Engineering & Technology, Kashmir, India
asifamin.am@gmail.com

[2]Student, Computer Science Engineering, SSM College of Engineering & Technology, Kashmir, India
haqisrar999@gmail.com

[3]Assistant Professor, Computer Science Engineering, SSM College of Engineering & Technology, Kashmir, India
monisanazir.ssm@gmail.com

……..***…….

Abstract: In the present digital day with remarkable development in Computer sector, Single factor authentication, e.g. passwords, is no more examined as secure in the World Wide Web. It has never been less difficult in Securing the system and remote access. Simple, obvious and easy-to-guess passwords, such as names and age, are effortlessly found via computerized secret key gathering programs. The security and privacy threats through malware are always constantly growing both in quantity as well as quality. Expanded access to information increases weakness to hacking, cracking of passwords and online frauds. In this association the conventional login/password authentication is taken into account inadequately secure 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 factor increases the difficulty of providing false credentials. Two-factor authentication proposal guarantee a higher protection level by extending the single authentication factor. This paper focuses on the implementation of two-factor authentication methods by using both users friendly traditional Alphanumeric Password and graphical Password as gateway for authentication. An attempt has been made by using two factor Authentication, and in this paper we describe the two factor Authentication system design and design implementation. Thus affording an additional password adds an extra layer of security.

1. INTRODUCTION

Security is a major concern today in all sectors such as banks, governmental applications, military organization, educational institutions, etc. Government organizations are setting standards, passing laws and forcing organizations and agencies to comply with these standards with non-compliance being met with wide-ranging consequences. There are several issues when it comes to security concerns in these numerous and varying industries with one common weak link being passwords. The rapid growth in the number of online services leads to an increasing number of different digital identities each user needs to manage. But passwords are perhaps the most common type of credential used today [1]. To avoid the tedious task of remembering difficult passwords, users often behave less securely by using low entropy and weak passwords. Most systems today rely on static passwords to verify the user's identity. However, such passwords come with major management security concerns. 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.

Several proper strategies for using passwords have been proposed [2]. 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. A typical solution is based on giving the user a hardware token that generates one-time-passwords, i.e. passwords for single session or transaction usage.

Moreover token also have disadvantages which include the cost of purchasing, issuing, and managing the tokens or cards. From the customer's point of view, using more than one two-factor authentication system requires carrying multiple tokens/cards which are likely to get lost or stolen. So we have a provision of OTP in Mobile, but there are major hurdles in that, we have to install OTP generation software in all clients mobile, the time in both mobile and server has to be always synchronized, if client purchase a new mobile, the mobile have to be registered and installed with the OTP generation software, updated software have to re-installed in all client mobile.

The paper is organized in such a way that section 2 briefs about existing authentication methods, section 3, and 4 explains about proposed method, system design and system implementation.

2. EXISTING AND PROPOSED AUTHENTICATION METHOD

Authentication to access a login account, accessing social engineering accounts, reading online news papers, online ticketing are carried out by Alpha- Numeric Password or Graphical password. Alternative authentication came in the form of Biometric Authentication using finger print, iris recognition and heat beat. Human tendency in creating easily rememberable password leans to password pitfalls [4, 5, 6].

Limitations in graphical and biometric password leads to development of validation of authentication process. Alternative to common mode of authentication alphanumeric password and easily rememberable graphical password are developing [18, 19, 20, 21]. This paper focuses on implementing these both methods as two factor authentication to enhance the security. By definition, Authentication is the use of one or more mechanisms to confirm that you are the authenticated user aver to be. Once the identity of the human or machine is validated, access is granted. Universally today existing acknowledged three authentication factors are (i) what you know like Alphanumeric passwords, Graphical Password (ii) what you have like ATM card or tokens and (iii) what you are like Finger print, Thumb Impression, Iris recognition, heart beat called biometrics authentication [13]. While the biometric-based authentication is relatively expensive and raises privacy concerns, One Time Passwords (OTP) offers a promising alternative for two factor authentication systems.

Drawbacks with OTP generation are it is an additional expense for the user and in particular whenever the user needs he/she has to carry to the device in which the user gets the OTP. Two-factor authentication solution equips customers with a cost effective means of providing flexible and strong authentication to very large scale. However, since fraud is still being reported with Two-Factor authentication, it shows that it is not totally secured, only that the fraud rate is reduced as compared to that of One-Factor authentication. Two factor authentication systems is user friendly approach and require memorability of both authentication passwords. 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 [7]. As per defenders, two-factor Authentication could definitely lessen the occurrence of online fraud, and other online extortion. Two-factor authentication (2FA) has been around for quite a while [12]. Two-factor authentication is not a new concept for an example considering the banking industry [11, 14]. Without replacing the existing authentication system, instead serves as an added layer of security that protects and enriches the existing authentication system. Two-factor authentication 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. 2FA requires the use of two reliable authentication factors:

(i) Something the user knows, e.g. a alphanumeric password

(ii) Something the user knows and which he clicks, e.g. a graphical password

3. SYSTEM DESIGN AND IMPLEMENTATION

In this paper, we propose a computer-based software token. This is supposed to replace existing hardware token devices. The System 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.

3.1 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 [5] 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.

4. ADVANTAGE AND DISADVANTAGE

Requiring more than one independent factor 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 both the passwords (ii) Space Complexity (iii) System Configuration so as to assist the second gateway which is a picture based and (iv) also take additional time.

5. 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. Two-factor confirmation 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.

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] The mobile phone as multi otp device using trusted computing http://eprints.qut.edu.au/37711/
[8] H. Wang, "Research and Design on Identity Authentication System in Mobile-Commerce", In: Beijing Jiaotong University, 2007, pp. 18-50.
[9] 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.
[10] 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.
[11] 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.
[12] Goode intelligence "Two Factor Authentication Goes Mobile" www.goodeintelligence.com, September 2012.

BIOGRAPHIES

Asif Amin is pursuing B.E Degree from SSM College of Engineering & Technology in Computer Science Engineering from University of Kashmir, J&K, India. His field of interest is ASP.Net & SQL**.**

Israr ul Haq is pursuing B.E Degree from SSM College of Engineering & Technology in Computer Science Engineering from University of Kashmir, J&K, India. His field of interest is ASP.Net Networking & SQL.

Monisa Nazir is the Assistant Professor at SSM College of Engineering & Technology in The Department of Computer Science Engineering. Her area of interest is Signal Analyst, Microprocessor and Software Engineering.

