IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 5, Issue 6, June 2016

Two Factor Authentication for Secured Login

Nagaashwini Nayak V J[1], Nagaveni B Biradar [2]

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.

Keywords: authentication, password, alphanumeric password, graphical password, secured login, network security, data protection.

1. INTRODUCTION

Today security concerns are on the ascent in all areas. Most systems today rely on static passwords to verify the user's identity. Users have a propensity to use obvious passwords, simple password, easily guessable password and same password for multiple accounts, and even write their passwords, store them on their system or asking the websites for remembering their password etc. Utilization of static passwords in this expanded dependence on access to IT systems progressively presents themselves to Hackers, ID Thieves and Fraudsters. In addition, hackers have the preference of using numerous techniques / attacks such as guessing attack, shoulder surfing attack, dictionary attack, brute force attack, snooping attack, social engineering attack etc to steal passwords so as to gain access to their login accounts. Quite a few techniques, strategies for using passwords have been proposed but some of which are especially not easy to use and practice. To solve the password problem in banking sectors and also for online transaction two factor authentications using OTP and ATM pin / cards have been implemented.

A validation component is a bit of data and methodology used to verify or check the character of an individual or other element asking for access under security imperatives. Multifactor verification is a security framework in which more than one password of confirmation is executed to confirm the authenticity of an exchange. In two-factor authentication, the user provides dual means of identification, one of which is typically a physical token, such as a card, and the other of which is typically something memorized, such as a security code. The goal of MFA is to create a layered defense and make it more difficult for an unauthorized person to access a target such as a physical location, computing device, network or database. If one factor is compromised or broken, the attacker still has at least one more barrier to breach before successfully breaking into the target. Multifactor authentication is a system where in two or more different factors are used in conjunction to authenticate. Using more than one factor is sometimes called "strong authentication". The process that solicits multiple answers to challenge questions as well as retrieves 'something you have' or 'something you are' is considered multifactor.

Multifactor confirmation is a security structure in which more than one appearance of affirmation is executed to affirm the valid ness of a trade. In two-factor confirmation, the customer gives twofold technique for conspicuous verification, one of which is normally a physical token, for instance, a card, and the other of which is ordinarily something held, for instance, a security code. The goal of MFA is to make a layered hindrance and make it more troublesome for an unapproved individual to get to a focus, for instance, a physical zone, figuring contraption, framework or database. In case one part is exchanged off or broken, the attacker still has no short of what one more impediment to break before viably breaking into the target. Multifactor approval is a system where in two or more unique parts are used as a piece of conjunction to approve. Using more than one segment is every so often called "strong affirmation". In general the multifactor method demands various reactions to test request and recoups 'such as something you have' or 'something you are' .

Two-components or multi-component verification is precisely what it seems like. As opposed to utilizing one and only kind of confirmation element, for example, just things a client KNOWS (Login Ids, passwords, mystery pictures, imparted privileged insights, requested faculty data, and so forth), two-factor verification requires the expansion of a second component, the expansion of something the user HAS or something the user IS . Two

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 5, Issue 6, June 2016

factor confirmations have limitations which incorporate the expense of buying, issuing, and dealing with the tokens or cards. Keeping this a new scheme has been proposed, Authentication
using two well known factors such as Alphanumeric and graphical password . The paper is organized in such a way that section 2 briefs about existing authentication methods, section 3, 4 and 5 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. 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 . 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 . 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.

• Something you know

• Something you have

• Something you are

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 . 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. Two-factor 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. 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:

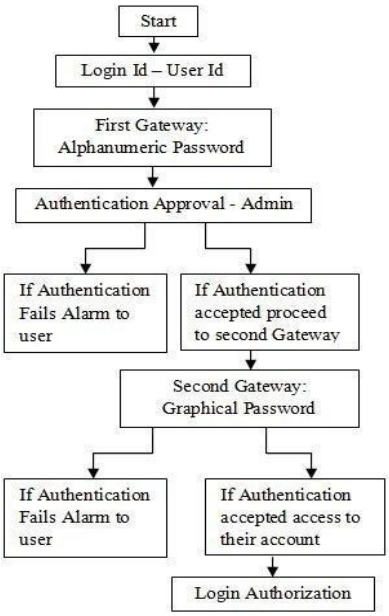
(i) Something the user knows, e.g. a alphanumeric password

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

DOI 10.17148/IJARCCE.2016.56189

3. SYSTEM DESIGN

The System design of the proposed two factor authentication method is as follows:



4. DESIGN IMPLEMENTATION

Two mode of operation are accessible for the users focused around their inclination and imperatives. The first approach is a stand-alone approach that is not difficult to utilize, secure, and cheap which is the traditional mode of authentication known as Alphanumeric Password. The second approach is an approach that is also easy to use and secure which is a Graphical Password such as Pass faces, click points, image and picture based.

After the user provides his/her username to login into their account, first gateway will be the Alphanumeric Password which the user has chosen at the time of registration for that particular site. Once it's get authenticated by the admin the user has to provide the password for the second gate way which will be an image / pass faces. If the authentication fails at either gateway alarm will be given to the user stating false authentication. Features of the proposed authentication system are it is easier to use, secure and cheap. Both the password are user chosen not provided by any other password management system and also maintained by service provider not by password management system.

5. 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.

6. CONCLUSIONS

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/multi fa ctor-authentication-MFA.
[2] McAfee Case Study "Securing the Cloud with Strong Two-Factor Authentication through McAfee One Time Password" http://www.mcafee.com/in/case-studies/cs-cloudalize.aspx.
[3] http://www.oneid.com/wp-content/uploads/2014/05/OneID_WhitePaper_Ad v-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] Jeff Yan, Alan Blackwell, Ross Anderson, Alasdair Grant "Password Memorability and Security: Empirical Results" IEEE security and privacy Vol. 2, Issue: 5, pp. 25 - 31, 2004.
[6] Dinei Florencio, Cormac Herley " A Large-Scale Study of Web Password Habits" Proceedings of the 16th international conference on the World Wide Web, ACM Digital Library, pp 657-666, 2007.
[7] Andrew Kemshall, Phil Undewood "White paper - Options for Two Factor Authentication" SecurEnvoy July 2007.
[8] Alireza Pirayesh Sabzevar, Angelos Stavrou "Universal Multi-Factor Authentication Using Graphical Passwords", Proceedings of the 2008 IEEE International Conference on Signal Image Technology and Internet Based Systems. pp. 625-632, 2008.
[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.

DOI 10.17148/IJARCCE.2016.56189