International Journal of Applied Engineering Research ISSN 0973-4562 Volume 13, Number 10 (2018) pp. 7576-7579

Three-Factor Authentication for Fortified Login to Ensure Privacy Preservation and Improved Security

C. Lakshmi Devasena

Faculty of Operations & IT, IBS Hyderabad, ICFAI Foundation for Higher Education, IFHE University, Hyderabad, India.

Abstract

In today's digital era with incredible development in the information technology sector, single-factor authentication using passwords and two-factor authentication is not adequate to provide better security. Hacking programs, simple computerized secret key gathering programs and password generators made it difficult to provide security even when single-factor or two- factor authentication used in securing the remote access and the system. The security threats using malwares like entered key trackers are always there to increase the security threats. Expanded access to information upsurges weakness to cracking of Passwords, hacking and online scams. In this regard, conventional login/password authentication is inadequate to provide security for several security-critical applications such as login to Banking Accounts, Mailing Accounts, Gadgets, Social Networks, Sensitive Financial accounts, commercial websites, official secured networks, and online payment, etc. Considering multi-level independent factor increases the complexity of providing correct credentials by the attacker. Multi-factor authentication proposal assures a higher protection level by extending the single authentication factor or two factors. This paper concentrates on the implementation of three-factor authentication by using users friendly traditional Alphanumeric Password and graphical Password and a security question as gateway for authentication. An effort has been made by using three-factor authentication, and in this paper the proposed three-factor Authentication model and implementation is described. Thus extending an additional password increases an extra level of security.

Keywords: authentication, alphanumeric password, data protection, graphical password, fortified login, network security, three-factor authentication.

INTRODUCTION

Today security concerns are growing more in all areas, since every business area is digitized and globalized. Today, most systems depend on static passwords [3] to authenticate the user's identity. Users have tendency to use apparent passwords, easily guessable password, very simple password, and more often same password for multiple accounts, and even note their passwords, store them on their system or asking the websites for remembering their password [1, 2] etc. Utilization of static passwords and storing them in IT systems gradually presents themselves to ID Thieves, Hackers and Impostors. In addition, system hackers have the inclination of using numerous attacks / techniques like guessing attack, dictionary attack, shoulder surfing attack, brute force attack, social engineering attack, snooping attack, etc to steal passwords to gain entrée to their login accounts.

Multifactor verification [4, 6] is a security context in which at least two or more authentication/secret key of confirmation is executed to approve the authenticity of an exchange. In two-factor authentication, the user offers dual means of proof of identity, one of which is classically a token or user id or identity card, and other of which is usually something remembered, such as a security code/image. The objective of multi-factor authentication (MFA) is to create a layered protection and make it tougher for an unauthorized person to enter a target such as a computing device, physical location, network or database. Even if one factor is negotiated or broken, the invader still has at least one or more barrier to breach before magnificently breaking into the target. In Multi-factor authentication is a system, two or more diverse factors are used in aggregation to authenticate the user [6, 14]. Using more than one factor in authentication sometimes called as "strong authentication". The objective of MFA is to make a layered interference and make it more complex for an unapproved individual to get to a focus, for instance, a physical zone, gadget, virtual zone, framework or database. In general the multifactor method demands numerous reactions to test entreaty and regains the user authenticity [6]. Multi-factor verification requires the expansion of a second, third component, the expansion of something the user HAS or something the user IS [7]. Two factor validations have limitations which integrate the expense of buying, issuing, and dealing with the tokens or cards [8, 9]. Keeping this in mind, a new scheme has been proposed, Authentication using three factors such as Alphanumeric, graphical password and a security question. The paper is organized in the following manner: section 2 explains briefly about existing authentication methods, section 3 presents the proposed three-factor authentication framework, and section 4 &5 explains the implementation of proposed method and its advantages.

EXISTING AUTHENTICATION METHOD

Authentication to access a user account, reading online newspapers, accessing social engineering accounts, online ticketing using user accounts are carried out by Alpha-Numeric Password or Graphical password [11]. Alternative authentication came in the form of Biometric Authentication using finger print, facial detection, iris recognition, palm print and heat beat. Human tendency in creating easily memorable password leans to password snares [1, 2, and 3]. Substitute to common mode of alphanumeric password authentication and easily memorable graphical password are developed by different researchers [15, 16, 17, 18, and 19]. By definition, Authentication is the use of one or more factors/mechanisms to endorse that you are the authenticated user declare to be. Once the uniqueness of the machine or human is confirmed, access is granted. Unanimously, existing acknowledged authentication factors of today are (i) what you know such as Alphanumeric passwords, Graphical Password (ii) what you have like tokens or ATM card and (iii) what you own uniquely like Finger print, Iris recognition, Thumb Impression, heart beat called biometrics authentication [10].

Two-factor authentication solution provides customer with a cost effective flexible and strong authentication. However, since fraud is still being conveyed with Two-Factor authentication, it is understood that it is not totally secured but the fraud rate is reduced as associated to that of One-Factor authentication. The goal of computer security to uphold the availability, integrity and privacy of the information entrusted to the system can be attained by using two-factor authentication technique [5, 7, 8, 9, 12 and 13]. As per protectors, two-factor Authentication could undeniably decrease the existence of online fraud, and other online extortion.

Without supplanting the existing authentication system, to serves as an extra layer of security that protects and enhances the existing authentication system, the proposed three-factor authentication (3FA) is described. 3FA is an information security process in which three means of credentials are combined to escalate the probability that an entity, generally a computer user, is the legal holder of that identity. This paper focuses on implementing the proposed methods as three-factor authentication to enhance the security. 3FA requires the use of three reliable authentication factors:

(i) Something user knows, e.g. an alphanumeric, general textual password

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

(iii) The security questions answered by the user at the registration time.

PROPOSED THREE-FACTOR AUTHENTICATION FRAMEWORK

The framework of the proposed three factor authentication method is as follows:

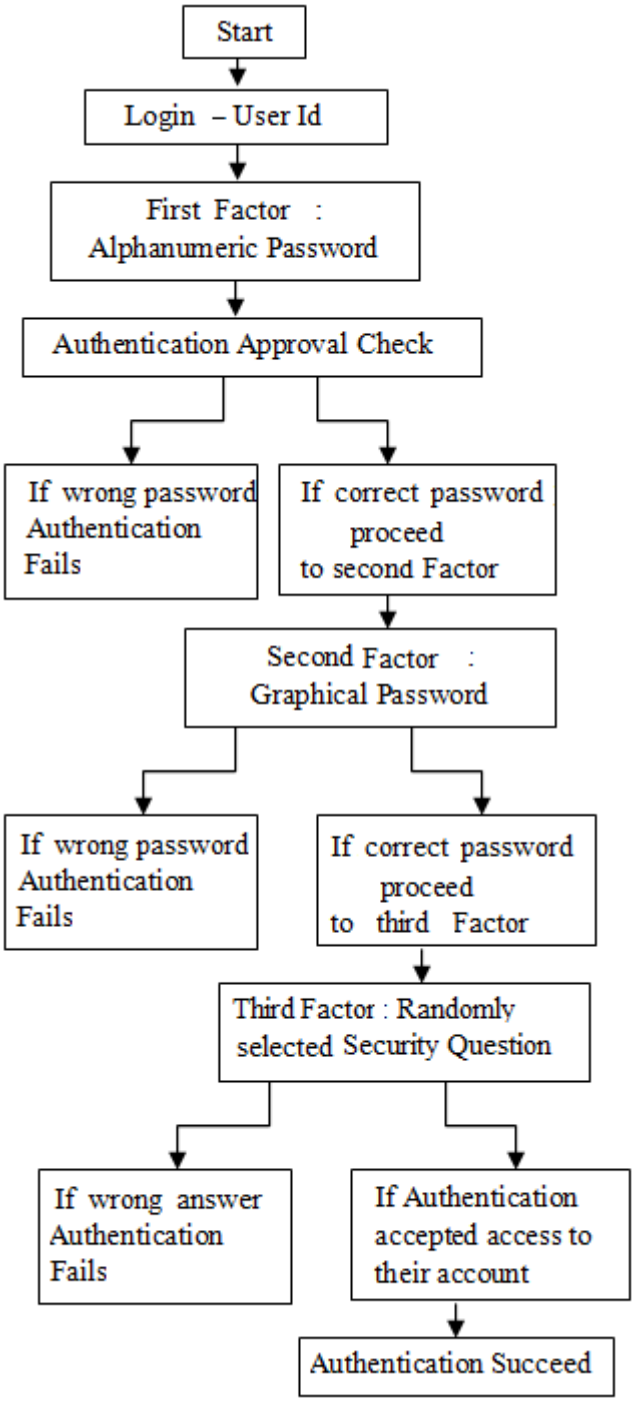

Figure 1. Framework of Proposed three-factor authentication method

PROPOSED MODEL IMPLEMENTATION

The proposed method uses three factors to authenticate the user into the target application/website. The first factor is a

usual approach, which is not very difficult to utilize, cheap and secure, which is the traditional mode of validation known as Alphanumeric Password. The second factor is the approach that is also easy to use and secure which is a Graphical Password such as click points, Pass faces, image and picture based data. After the user provides his/her username to login into their account, first authentication check will be the Alphanumeric Password which is chosen at the time of registration for that particular site/account. Once it's get validated by the admin, the user has to provide the graphic password to pass the second security check, which will be an image, click point / pass faces. If the verification failed at either gateway, alarm message will be sent to the user stating false authentication. If the verification succeeded, as a third factor, one of the security questions stored at the time of registration will randomly displayed and the user has to provide the correct answer. If wrong answer is given then authentication fails otherwise the user will be authenticated to enter into the website/account. Features of the proposed validation system are, it is easier to use, secure and cheap. Both the passwords and answers are user chosen not given by other password management system. And those passwords and answers maintained by service provider of the website/user account and not by password management system. This increases the success of the proposed system to the maximum extent.

5. DISCUSSION ABOUT BENEFIT AND WEAKNESS OF PROPOSED MODEL

Requiring more than one independent factor increases the chance of providing false credentials. This will protest the unauthenticated person to enter into the genuine system. The benefits of proposed system are (i) it improves privacy preservation (ii) there will be fortified Login mechanism to secure portals, websites, and web applications (iii) Since there are three level of protection, it provide in depth security. (iv) it is easy to implement. On the subject of the weakness (i) it require remembering ability of the passwords and answers to security questions (ii) it require more memory to store necessary information and (iii) also it take small amount of additional time to login. But these limitations are negligible and can be compromised with the level of security obtained and the protection mechanism achieved.

CONCLUSIONS

Progression in validation techniques has to check out tomorrow's authentication inevitabilities not today's. At the point, when everything is ok, one needs to spend more to get superior degree of security. Upholding security to a standard will be tougher and bothersome with time. Some challenges can be predicted and projected, such as improvements in computation that are making it increasingly easier to dictionary-attack a password database. Some challenges are harder to forecast, for example, the exposure of new "day-zero" vulnerabilities in the software being used. Subsequently, security preconditions are not altered, yet increment with time. Three-factor authorization can be habitually being utilized to work around the basic inadequacies in password administration. Integrated three-factor authentication gives the best expediency for better security. As the confirm mechanism for authentication, the proposed view can be suitably used in many secure-critical applications/areas especially in the web oriented applications. The ultimate thought is that the proposed three-factor authentication will provoke more vital security.

ACKNOWLEDGEMENT

The author expresses her deep gratitude to the Management of IBS, Hyderabad to the motivation and support provided.

REFERENCES

[1] 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.

[2] 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.

[3] 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.

[4] Ayu Tiwari, Sudip Sanyal, Ajith Abraham, Svein Johan Knapskog and Sugata Sanyal, "A Multi-Factor Security Protocol for Wireless Payment- Secure Web Authentication Using Mobile Devices," IADIS International Conference Applied Computing, ISBN: 978-972-8924-30-0, 2007.

[5] Andrew Kemshall, Phil Undewood "White paper - Options for Two Factor Authentication" SecurEnvoy July 2007.

[6] Alireza Pirayesh Sabzevar, Angelos Stavrou "Universal Multi-Factor Authentication Using Graphical Passwords", Proceedings of the 2008 IEEEInternational Conference on Signal Image Technology and Internet Based Systems. pp. 625-632, 2008.

[7] 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.

[8] Chun-Ta Li, Cheng-Chi Lee, Lian-Jun Wang and Chen-Ju Liu, "A Secure Billing Service with Two-Factor User Authentication in Wireless Sensor Networks," International Journal of Innovative Computing, Information and Control, Volume 7, Number 8, August 2011, pp. 4821-4831.

[9] 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.

[10] Sharifah Mumtazah Syed Ahmad, *et al* "Technical Issues and Challenges of Biometric Applications as access control tools of Information Security"International Journal of Innovative Computing, Information and Control Vol8, No. 11, pp 7983 – 7999 Nov 2012.

[11] Haichang Gao, Wei Jia, Fei Ye, Licheng Ma "A survey on the use of Graphical Passwords in Security", Journal of software, Vol. 8, No. 7, July 2013.

[12] Rahul Kale, Neha Gore, Kavita, Nilesh Jadhav, Swapnil Shinde " Review Paper on Two Factor Authentication Using Mobile Phone" International Journal of Innovative research and Studies, Vol. 2, Issue 5, pp. 164 - 170, May 2013.

[13] Alexandra Dmitrienko, Christopher Liebchen, Christian Rossow, and Ahmad-Reza Sadeghi "On the (In) Security of Mobile Two-Factor Authentication" Lecture Notes in Computer Science, pp. 365-383, Nov 2014.

[14] Sea Chong Seak, Ng Kang Siong, Wong Hon Loon, Galoh Rashidah Haron, "A Centralized Multimodal Unified Authentication Platform for Web-based Application", Proceedings of the World Congress on Engineering and Computer Science 2014 Vol I, 2014.

[15] Sanket Prabhu and Vaibhav shah, "Authentication using session based passwords," Procedia Computer Science,45 (Elsevier), pp. 460 – 464, 2015.

[16] Amish shah et el. "Shoulder surfing resistant graphical password system," Procedia Computer Science , 45 (Elsevier), pp. 477 – 484, 2015.

[17] Smita Chaturvedi and Rekha Sharma, "Securing text and image password using a combination of persuasive cued click points with improved advanced encryption standard ," Procedia Computer Science , 45 (Elsevier), pp. 418 – 427, 2015.

[18] S. Vaithyasubramanian, A. Christy, D. Lalitha "Two factor Authentication for Secured Login Using Array Password Engender by Petri net" Accepted for Procedia Computer Science, Elsevier 2015.

[19] C. Shoba Bindu, "Secure Usable Authentication Using Strong Pass text Passwords," I. J. Computer Network and Information Security, 3, pp. 57-64, 2015.