International Journal of Engineering & Technology, 7 (4.10) (2018) 470-472

International Journal of Engineering & Technology

Website: www.sciencepubco.com/index.php/IJET

Research paper

Study and Development of Graphical Authentication System for Secure File Transmission

P.L.P.Ramyasri[1], D.Malathi[2], J. D. Dorathi Jayaseeli[3], K.Senthilkumar[4]

[1]M.Tech Student, SRM Institute of Science and Technology, Kattankulathur
email id : plpramyasree@gmail.com
[2]Professor, CSE Department, SRM Institute of Science and Technology, Kattankulathur
email id: malathi.d@ktr.srmuniv.ac.in
[3,4]Assistant Professor, CSE Department, SRM Institute of Science and Technology, Kattankulathur
**Corresponding author E-mail: plpramyasree@gmail.com*

Abstract

The text-based password has been the most common practice from ancient days till present. Text based pass-words are also known for various threats, and it is prone to attacks like guessing attacks, dictionary attacks, social engineering attacks, brute force attacks, etc. The next immediate concept following the text based password is the graphical password schemes to improve password security and usability. In present days graphical passwords are being implemented more commonly. This approach is different from the traditional alpha numeric as it deals with images. In this paper a survey study is done to analyse various techniques used for authentication and also some of the methods for graphical authentication techniques like Pass Matrix, Cued Clicked points(CPP), CAPTCHA, Image distortion with text association, Doodle scheme, Standard recognition-based scheme, Stegno pin authentication method. Based on the existing methods, the future research can be done in order to improve security for graphical authentication.

Keywords: *Graphical Password, Pass Matrix, CAPTCHA, Image distortion, Doodle scheme, Standard recognition- based scheme.*

1. Overview of Existing Authentication Methods

The various existing authentication techniques are grouped as Token - authentication, Biometric-authentication, Knowledge authentication. Some of the commonly used token-based techniques are smart cards, key cards and bank cards. These token based authentication systems also involve some concepts ofknowledge-based techniques as well to improve security. ATM cards are an example for this. Biometric based authentication techniques like our iris reader, fingerprints, facial recognition arenotcommonly used. These systems are expensive, slow and at times unreliable. In spite of all draw backs these techniques still has the strongest security level. Knowledge based authentication technique method includes both picture-based password method and text-based password method. The picture-based authentication technique is divided into: recall-based graphicaltechnique and recognition-based graphical technique. In case of the latter method the user must correctly identify the images that were already selected by the user during registration. In case of recall-based techniques, the user is requested to recreate the pattern that was already being created by the user in the registration step. The next immediate concept following for authentication is CAPTCHA. It is a newly evolved concept to enhance the security techniques further. CAPTCHA is known as "Completely Automated Public Turing test to tell Computers and Humans Apart". It is typically used to verify if the user is human or robot or any other software as such.

2. Drawbacks of Existing System

In the existing system for graphical authentication system pass-matrix is implemented, that chooses one square for sequences of n-images instead n-squares in one image. During the login phase, login-indicator is implemented as it generates the characters in the grid format. The login-indicator generates different characters each time. A Random-guess attack can happen when attackers try to randomly choose square for each image until successful login occurs. The existing graphical authentication is not user friendly and biggest drawback of current graphical password is the Shoulder Surfing problem since Attackers can observe directly or use external recording devices to collect user's credentials. The drawback of applying biometrics is its intrusiveness on a user's Personal characteristic and biometrics is an expensive security solution.

3. Related Work

Hung-Minet al in [1] proposes an authentication system that is based on the pass matrix and the pass images. Through the one time login indicator the user will be able to point out the location of pass-square. The pass matrix chooses one square per image, so for n-images it chooses n-squares. The major advantage of this

Copyright © 2018Authors. This is an open access article distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

method is that the user need not remember the password at all. But the ultimate drawback is that it is not user friendly and at times random guess attacks might occur and Users has to remember more information or they have to perform more computation during authentication.

S. Gurav et al in [2] describes on image authentication and the methodologies involved in this method to enhance graphical authentication. Based on the previous works in this subject he proposed an enhanced graphical authentication in cloud through token generation. A key is generated in order to calculate le verification and data integrity. Future works can be projected on securing data using efficient techniques.

L. Wang et al in [3] proposed a scheme that combines graphical passwords with text-based CAPTCHA. It defines on the innovative use of CAPCTHA as a better protection against spyware attacks. The password space size is estimated and is compared with text based passwords. The user limitation in this approach is that both pass images are to be remembered and also enter the characters of CAPTCHA on the password position correctly. Future works can focus on improving login time.

T. Takada et al in [4] described a unique authentication scheme named fake pointer for a solution to a peeping attack by video capturing. The fake pointer has two unique features one it provides double layered interface for the secrete input. This is difficult for a attacker to identify user authentication. Here fake pointers are added as background to the screen or keypad. The limitation is camera-based attacks may happen.

Ms GrinalTuscano et al in [5] focuses mainly on inventing a more powerful secure authentication mechanism. He discusses in detail on image distortion technique that is carried out with the help of letters. In this approach both the original and the distorted images are show cased to the user. There is a risk of guessed at-tacks where the images can be combined along with the text. Results demonstrated that further studies can happen on pass-faces to reduce the fear of random guess attacks.

A. Bianchi et al in [6] discusses on the performance and the implementation of the PIN entry system on the Audio and the Haptic cues. A haptic cue is a sensory cue that is extracted from sensory input. An ANOVA (Analysis of variance) is a statistical technique that is implemented to determine the speed of authentication. Results show that the interaction between the two variables i.e. Pin length is significant. Future works can be proposed on combining PIN length and stimuli set size.

Khamis, Mohamed, et al in [7] proposed a new prototype called the GTmoPass architecture to enable multi factor authentication that is based on possession factor and knowledge factor. Knowledge factor deals on what the user remembers and knows. The Gtmopass is a multi-model scheme that uses touch based PINs to compute the position of gaze input on passwords entry time and to also compute the error count. It also computes the time taken to enter a password from first input to last input and calculate the number of times the password is typed incorrectly. Simulation results show that Gtmopass is secure and usable to fight against shoulder surfing. Further research can understand touch-based PINs.

D. Tan, P. Keyani, et al in [8] designed a unique spy-resistant keyboard to allow users to enter private text without revealing it to the attackers. This keyboard contains 42 characters with 2-Interactor lines, a textbox for feedback, enter button, a space button. Results of implementing this keyboard indicates that though users take longer time to enter their passwords it has drastic increased their ability to protect the passwords from a watchful observer. Future works can be proposed to provide a better usability and user friendly device.

Ron Poet et al [9] construct an attack exploiting predictability system called as the Semantic Ordered Guessing Attack (SOGA). The SOGA attack is applied on two different schemes (a standard recognition-based scheme and the Doodles scheme that uses photographic images). Outcome of the experiment shows that predictability in case of graphical passwords has varying degree of security levels (this depends on the type of distractor algorithm that is selected). Whereas the traditional pass images scheme shows that the guess ability has increased to maximum 18 times when compared to the usual reported guess ability. Hence to maximize security of the recognition-based graphical password method, the author recommends preventing or avoiding user choice of images.

Susan Wiedenbeck et al in [10] record an interesting analyzing on the use of Pass Points on passwords which are alphanumeric. The users participated in this study created and implemented alphanumeric, graphical password. The users must try three longitudinal trials to enter password for a time period of 6 weeks. Results of this experiment showed the users who use graphical passwords were able to create a valid password with less difficulty compared to alphanumeric users. Results also show that graphical users consumed longer time and committed several wrong password inputs compared to the alphanumeric users. On considering longitudinal trials, both methods performed equally on the bases of memory of their password. The group took much time to type the correct password. The limitation is results showed that 1/5th users are facing difficulty in inputting password.

Emanuel von Zezschwitz et al in [11] established results of the study that compared the authentication performance mobile devices along with password composition. A study was proposed in lab (n = 24) and the results gave a poor performance for entering the password for mobile devices like smart phones. Core study on (n = 450) proved that passwords which are alphanumeric are increasingly used on smart phones, tablets, etc. A adverse effect on password security is proved where users prefer easier passwords to enter on the respective devices. Limitation is analysis of keystroke mentioned that speed of input becomes very slow if complexity of string increases

Andrea Bianchi et al in [12] defines that passwords are being encoded as sequence of randomized vibration pattern that is impossible for the observer to copy or identify the selected items. Experimental results of this system outperform the previous inter-faces that was used to tactile feedback to obfuscate passwords. The limitation of using randomized vibration pattern is that login and password does not provide an adequate security. A Loss or damage may happen to smartcard or portable device in the biometric cryptographic systems. Existence of the single physical location focus to the attack.

Antonella De Angeli et al in [13] proposed the Visual Identification Protocol (VIP) which is considered as an innovative solution for the authentication process. It is based on visual memory and pictures. The proposed system was compared with three other authentication systems in a longitudinal evaluation (N=61). The observation was helpful to analyse on the attitudes and behaviour of the authentication systems. Among all the authentication systems, VIP was the most preferred method by the users. At the same time it was easily destructible there is a possibility of malicious per-son stealing the user's smartcard or the portable computing device. Complete error analysis is also provided in this paper to under-stand the cause of the destruct and point out the limitations of this system.

Oakley et al in [14] described about Multi-touch lock (M-T lock) that is based on google-android pattern lock authentication system. It improves the security by mixing the tapes and strokes for the use of Mt Lock. Experimental results state that this method provides better security for mobile devices but the user is facing complexity during log-in. Future works can be done on feedback of user for the usage of MT-lock.

M. Martinez-Diaz et al in [15] presented a doodle database and pseudo signature. The performance was compared between pseudo and hand written signature. An acquisition protocol that enables the user devices to request permission is being implemented. Experimental results state that this method provides better security against forgeries. The verification principle itself is unverifiable: it isn't a tautology nor can it be proved viaexperience. Future works can be based on the complexity of skilled forgeries.

Zheng et al in [16] proposed an authentication scheme based on stroke concept on the grid as origin password. The main aim of this technique is to map the strokes against grids as original password and later enter the characters in the authentication process. Limitations in this method is that users adapt weak strokes as their passwords and hence creating passwords is vulnerable than login. Future studies can be based on providing security against camera based and brute force attacks.

V.Roth et al in [17] proposed a new technique called stegnography technique. The secrete message is protected or safe guarded using another message so as to avoid shoulder surfing attack. He discussed about semagrams that is used for hiding the PIN from attackers. Here the PIN is secured using signs and symbols. Two keypads are provided one is regular keypad and other is a challenge keypad which is used for OTP. Limitation is two keypads results in confusion to user.

The most frequently used authentication method in computer is user name and password. There are several vulnerabilities in this method that are known to all. The crucial step in this approach is to remember the passwords and then recall them during the authentication process. Studies say that users always prefer to choose short passwords or passwords that can be remembered easily [18]. Unfortunately, these passwords are broken very easily.

K. Gilhooly et al in [19] deal with problem of traditional username and password approach, and implemented biometrics. The main limitation in biometric authentication is the systems are not 100% accurate and it requires an additional hardware and it cannot be reset once done.

Adams and M. A. Sasse mentioned in [20] about an article published in the Computerworld news article where a company ran a password cracker. Within 30 seconds it was able to hack around 80% user passwords. Study has concluded, users can remember only a few number of passwords and they used the same passwords for various accounts. This paper deals with this alternative approach and the use of pictures as passwords. It takes too much of time for the password registration and login process. Required much more space then text password and shoulder surfing.

4. Conclusion

The existing literature works gives sample evidence to justify that textual passwords do not provide better security platforms. Additional techniques like captcha and other graphical authentication methods are introduced to enhance the strength of text password authentication. The major concern in implementing CAPTCHA is that even after multiple attempts the user may not be able to understand the CAPTCHA correctly. In order to replace this concept of CAPTCHA, images are displayed to the users to select one, now the object is extracted from the image using K-means clustering algorithm and user has to select one object. Now during login the user has to select the same object. The object name will be sent to users mobile and mail-ids so as to inform about the object selection to the user. The object is further encrypted using RSA algorithm to reduce shoulder surfing attack. The proposed method and existing authentication methods are compared by calculating the trustworthy values using Naive-Bayes algorithm based on the authentication attributes and can be implemented for secure file transmission.

References

[1] Sun, Hung-Min, "A shoulder surfing resistant graphicalauthentication system," IEEE Transactions onDependable andSecure Computing (2016).

[2] S. Gurav, L. Gawade, P. Rane, and N. Khochare, “Graphical password authentication: Cloud securing scheme,” InternationalConference on, in Electronic Systems, Signal Processing andComputing Technologies (ICESC),IEEE Jan 2014.

[3] L. Wang, X. Chang, Z. Ren, H. Gao, X. Liu, and U. Aickelin, “Against spyware using captcha in graphical password scheme,” in 24th International Conference on Advanced Information Networking and Applications, IEEE, 2010.

[4] T. Takada, “fakepointer: An authentication scheme for improving security against peeping attacks using video cameras,” in Mobile Ubiquitous Computing, Systems, and Technologies, Second International Conference on IEEE 2008.

[5] Ms GrinalTuscano “Graphical password authentication using Pass faces” Int. Journal of Engineering Research and Applications March 2015.

[6] Bianchi, Andrea, et al. "The phone lock: audio and haptic shoulder-surfing resistant PIN entry methods for mobile devices." Proceedings of the fifth international conference on Tangible, embedded, and embodied interaction. ACM, 2011.

[7] Khamis, Mohamed, et al. "GTmoPass: two-factor authentication on public displays using gaze-touch passwords and personal mobile devices:" Proceedings of the 6th ACM International Conference on Pervasive Displays, 2017.

[8] D. Tan, P. Keyani, and M. Czerwinski, “Spy-resistant keyboard: Towards more secure password entry on publicly observable touch screens,” in Proceedings of OZCHI-Computer-Human Interaction Special Interest Group (CHISIG) of Australia. Canberra, Australia:ACM Press,2005

[9] Rosanne, and Ron Poet. "Measuring the revised guessability of graphical passwords" 5th International Conference on. Network and System Security (NSS), IEEE, 2011.

[10] S. Wiedenbeck, J. Waters, J. Birget, A. Brodskiy, and N. Memon, “Passpoints: Design and longitudinal evaluation of a graphical password system,” International Journal of Human-Computer Studies, 2005

[11] E. von Zezschwitz, A. De Luca, and H. Hussmann, “Honey,ishrunk the keys: Influences of mobile devices on password composition and authentication performance,” in Proceedings of the 8th Conference on Human-Computer Interaction: Fun, Fast, Foundational, New York, NY, USA: ACM, 2014.

[12] Bianchi, I. Oakley, and D. S. Kwon, “The secure haptic keypad: A tactile password system,” in Proceedings of the SIGCHI Conference on Human Factors in Computing Systems, New York, NY, USA: ACM, 2010.

[13] Antonella De Angeli, Lynne Coventry, Graham Johnson & Mike Coutts” USABILITY AND USER AUTHENTICATION: PICTORIALPASSWORDS VS. PIN” NCR-FSD AdvancedTechnology& Research, Discovery Centre, 3 Fulton Road Dundee DD2 4SW.

[14] Oakley and A. Bianchi, “Multi-touch passwords for mobile device access,” in Proceedings of the ACM Conference on Ubiquitous Computing, New York, NY, USA: ACM, 2012.

[15] M. Martinez-Diaz, J. Fierrez, and J. Galbally, “The doodb graphical password database: Data analysis and benchmark results,” Access, IEEE, 2013.

[16] Zheng, Ziran, "A stroke-based textual password authentication scheme." Education Technology and Computer Science, 2009.ETCS'09.First International Workshop on.Vol.3. IEEE, 2009.

[17] V. Roth, K. Richter, and R. Freidinger, “A pin-entry method resilient against shoulder surfing,” in Proceedings of the 11th ACM conference on Computer and communications security,ACM, 2004.

[18] Gilhooly, "Biometrics: Getting Back to Business," in Computerworld, May 09, 2005.

[19] Adams and M. A. Sasse, "Users are not the enemy: why users compromise computer security mechanisms and how to take remedial measures," Communications of the ACM, vol. 42, pp. 41-46, 1999.