International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 04 Issue: 11 | Nov -2017 www.irjet.net p-ISSN: 2395-0072

Graphical Password Authentication using Images Sequence

Muhammad Ahsan[1], Yugang Li[2]

[1]Student, School of Computer Science and Technology, Beijing Institute of Technology, Beijing, China
[2]School of Computer Science and Technology, Beijing Institute of Technology, Beijing, China

---

Abstract - *This paper proposes a new technique of user Authentication that is Graphical Password Authentication using Images Sequence. In existing environment, a very important problem in information security is user authentication. There are many authentication techniques like textual, graphical, biometric, smart card etc. The existing graphical authentication techniques based on images selection are not good enough because in these techniques images are predefined by the system. In this paper, a new technique is proposed. In this method, user will upload images from his/her personal gallery/directory for password selection and images uploaded by one user will not be visible to other user. Graphical password is used as an alternative to textual/traditional alphanumeric password. Traditional alphanumeric password is difficult to memorize and usually forget by users as times passes when user remain unattached from the system, but in case of graphical password there are less chances to forget password because people remember images more easily than text based password. There are also less chances for hackers to steal the graphical based password because hackers will be unable to access the images uploaded by the user as password. We tested this method in a Web-based application.*

Key Words: Biometric authentication, Images based password, Recall based technique, Recognition based technique, Smart card authentication.

1. INTRODUCTION

Data security and user authentication is a basic factor for information security. Internet is providing accessibility to desired information resources across the globe. Every organization, social network, or any other platform try to provide better security to their users which is accurate and more secure for users. Authentication of user is basic component of any information system because it provides the ability to the user to access the system. Old security techniques which are using from a long time, provide less security for authentication than the advance security techniques. In the perspective of information security there may be following main objectives of authentication or security.

- How to keep away an unauthorized user from gaining access to system?
- How to ensure the accessibility of authorized users to the required resources of system?
- How to communicate user with system and with other resources [1]?

As described by the researchers and psychological studies that it is nature of humans that they remember images better than text, therefore the password which is graphical based, can be used alternatively to text based password [2]. Password comprises of data which is used to access to required resources of system. Password is kept secret from other users so that an unauthorized user can't access the resources of system and can't steel the personal information of the authorized users. Authentication can be done through several techniques like Textual/Alphanumeric, Smart Card, Bio-metric, Graphical etc. [3]. Each technique provides its own ability that can be regarded as secure. In this time user authentication regarded as a key feature of information security.

2. PASSWORD TECHNIQUES AND RELATED PROBLEMS

2.1 Textual or Alphanumeric Password Authentication

Textual/Alphanumeric (it can also be called as text based password) is a string or word of combined characters which are used to prove the authorized users [1], [4]. This technique for user authentication is commonly used [1] for a long time because this technique has many advantages but in the advance time there are more chances to steal the password by hackers [5]. To minimize the risk of stealing password, the password should be minimum of eight characters with uppercase, lowercase, special characters and alphanumeric characters. Alphanumeric password should not be meaningful contents like your first or second name, your age, your date of birth, your school name etc. [6].

Lack(s): Text based password is difficult to memorize for user because for a good security, [5] password should be lengthy, alphanumeric and include special characters [6]. If user use his password on daily basis, then password will easily memorize and if user didn't use password for a long time then there is chances to forget password [7]. To minimize the risk of forget password many users save their password in text file in the computer or write down on the paper. Saved password file can also steal by other users. Hackers can break the security which is text based [5]. Attackers use some "Spy" software (Key Listener and Key Logger) which can be easily install in the computer, these soft-ware recorded the key strokes and save in the text file

and these kind of software have also ability to send the saved key strokes to email address or an outside source [1], [8]-[10].

2.2 Smart Card Authentication

This technique is also use for user authentication and this type of authentication is also providing strong security. One of the main advantage of Smart Card Authentication is that it can be combined easily with the other kinds of authentication system. Smart card authentication provides additional security protocol and protection [11]. Smart Card has a small chip. All the information of user is store in the chip of smart card [1]. User swipes his/her smart card into smart card reader for verification of identity.

Lack(s): Smart cards are small in size and can be lost easily [11], [12]. Sometimes user forget his card in his/her office or home. If the card is stolen, then it is difficult to retrieve information from the stolen smart card [7]. This authentication technique can also increase initial cost at the time of deployment.

2.3 Biometric Authentication

Biometric authentication is a technique using individual's physical characteristics [7]. In this technique bio-logical data or bodily elements are evaluated for verification of user identity [7], [12]. Biometric based authentication provides the strongest and foolproof security and protect from unauthorized user to the system than text based, graphical based or smart card authentication [12]. There are no chances for hackers to steal the pass-word which is biometric based [7].

Biometric authentication is mainly implemented in such situations which have critical security requirements. Personal information and biometric data is distinct from each other [12]. Personal information can be stolen but it is very difficult for attackers to steal bio-metric data. Biometric authentication is long term security solution for any company or organization. Bio-metric authentication can be implemented in various ways like DNA Matching, Iris Scan, Retina Scan, Fingerprint Identification, Face Recognition, Hand Geometry Recognition, Signature Recognition and Voice Analysis etc. [1], [7, [10, [12]. Biometric authentication is suitable for those companies or organizations which have critical security requirements.

Lack(s): Biometric authentication is high level security [12] therefore hardware cost for biometric authentication is higher [1] compared to other authentication techniques. Sometimes biometric authentication is not suitable for arthritic persons who have no ability to put hands, eyes or fingers properly on scanner.

2.4 Graphical Password Authentication

Firstly, Graphical Password idea was given by Blonder in 1996, which states that an image should appear on given screen and user should select some regions by clicking on the image, if the selected regions of image are correct then the user will be authenticated [13]. User authentication using graphical technique is now very common. Organizations or companies are trying to adopt this authentication technique. On the web images are also using as re-captcha to know the types of user. Images as re-captcha provide advanced security [14]-[16]. Using images for authentication is easy for human and hard for robots that's why every organization or company try to adopt this technique.

In graphical password authentication images are used by the user for authentication [9], [17] user select some specific regions, select multiple images or create image etc. [8], [13], [18]-[19].

Mainly graphical password authentication based on two different techniques [5], [20]-[21].

I. Recognition Based Technique
II. Recall Based Technique

I. Recognition Based Technique

In this type of graphical authentication technique multiples images are show to user at registration phase [22], images may be in random order. User has to select some images (according to defined condition) for password selection. Selected images as password either in sequence or in random order. At the time of login user has to select images which were selected for password (sequence or randomly).

II. Recall Based Technique

In this technique user has to provide some information at the time of registration i.e. text or handwritten design. Usually it is compatible with touch screen devices, pattern selection, signature, images drawn on 2G grid, hints for password etc. Recall based technique has different categories with different methods and ways, (1) Pure recall based technique which includes Passdoodle, Draw a Secret and Signature technique. (2) Cued recall based technique which include PassPoints, Blonder, VisKey SFR, Pass-Go, Drawing Geometry and Passlogix V-Go technique [5], [10], [20]-[21]. Our research is on graphical authentication using images in sequence that's why our focus is on Recognition Based Technique.

Graphical password authentication has many advantages like it provides more security than the textual password. "Spy" software (Key Listener and Key Logger) can't be used to record images [2]. It provides human friendly interface for user authentication. It is easy to memorize images password and has less attacking chances using dictionary attacks and brute force search [9]-[10]. Biometric

[9] H. Gao, W. Jia, F. Ye, and L. Ma, "A survey on the use of graphical passwords in security," Journal of Software, vol. 8, no. 7, pp. 1678–1698, Jul. 2013.

[10] A. Bhanushali, B. Mange, H. Vyas, H. Bhanushali, and P. Bhogle, "Comparison of graphical Password authentication techniques," International Journal of Computer Applications, vol. 116, no. 1, pp. 11–14, Apr. 2015.

[11] C.-G. Ma, D. Wang, and S.-D. Zhao, "Security flaws in two improved remote user authentication schemes using smart cards," International Journal of Communication Systems, vol. 27, no. 10, pp. 2215–2227, Nov. 2012.

[12] Y. LI, "Biometric technology overview," Nuclear Science and Techniques, vol. 17, no. 2, pp. 97–105, Apr. 2006.

[13] G. E. Blonder, "Graphical Password," US5559961 A, Lucent Technologies, Inc. (Murray Hill, NJ), Sep. 1996.

[14] P. P. Doke, and S.A Nagtilak, "A survey on CAPTCHA as graphical Password," International Journal of Science and Research (IJSR), vol. 4, no. 12, pp. 2032–2036, Dec. 2015.

[15] Rashmi B J, and B. Maheshwarappa, " Improved Security Using Captcha as Graphical Password," International Journal of Advanced Research in Computer and Communication Engineering, vol. 4, issue 5, pp. 352–354, May 2015.

[16] M. Davis, Divya R, V. Paul, and Sankaranarayanan P N, "CAPCHA as Graphical Password," International Journal of Computer Science and Information Technologies, vol. 6(1), pp. 148–151, 2015.

[17] A. H. Lashkari, and S. Farmand, "A survey on usability and security features in graphical user authentication algorithms," IJCSNS International Journal of Computer Science and Network Security, vol. 9, no 9, pp. 195–204, Sep. 2009.

[18] S. Sathish, A. B Joshi, and G. I Shidaganti, "User Authentication Methods and Techniques by Graphical Password: A Survey," International Journal of Computer Applications & Information Technology, vol. 2, issue 3, pp. 1–4, Apr. 2013.

[19] P. C. van Oorschot and J. Thorpe, "Exploiting predictability in click-based graphical passwords*," Journal of Computer Security, vol. 19, no. 4, pp. 669–702, Jun. 2011.

[20] E. E. K. Ugochukwu, and Y. Y. Jusoh, "A review on the graphical user authentication algorithm: Recognition-based and recall-based," International Journal of Information Processing and Management, vol. 4, no. 3, pp. 238–252, May 2013.

[21] D.Aarthi, and Dr. K. Elangovan, "A Survey on Recall-Based Graphical User Authentications Algorithms," International Journal of Computer Science and Mobile Applications, vol. 2, issue 2, pp. 89–99, Feb. 2014.

[22] F. Towhidi, and M. Masrom, "A Survey on Recognition-Based Graphical User Authentication Algorithms," International Journal of Computer Science and Information Security, Vol. 6, No. 2, pp. 119–127, 2009.

[23] K. Rao and S. Yalamanchili, "Novel Shoulder-Surfing resistant authentication schemes using text-graphical passwords," International Journal of Information and Network Security (IJINS), vol. 1, pp. 163-170, no. 3, Jul. 2012.

[24] Mokal P. H., and Devikar R. N., "A Survey on Shoulder Surfing Resistant Text Based Graphical Password Schemes," International Journal of Science and Research (IJSR), vol. 3, issue 4, pp. 747–750, Apr 2014.

[25] M. Bendale, N. Singh, S. Baid, and A. Maurya, "A Simple Text Based Graphical Password Scheme to Overcome Shoulder Surfing Attacks," International Journal of Advanced Research in Computer and Communication Engineering, vol. 4, issue 3, pp. 364–366, Mar. 2015.

[26] A. M. Nikam, and S. N. Shelke, "Graphical Password Method Based on Text to Protect from Shoulder Surfing.," International Journal of Advance Foundation and Research in Computer (IJAFRC), vol. 1, issue 11, pp. 47–50, Nov. 2014.

[27] Thorawade M.B., and Patil S.M., "Authentication Scheme Resistant to Shoulder Surfing Attack Using Image Retrieval," International Journal of Knowledge Engineering, vol. 3, issue 2, pp. 197–201, Nov. 2012.

[28] M. S. Umar, M. Q. Rafiq, and J. A. Ansari, "Graphical user authentication: A time interval based approach," 2012 IEEE International Conference on Signal Processing, Computing and Control, Mar. 2012.

[29] P. Rane, N. Shaikh, and P. Modak, "Secure authentication using click draw based graphical Password scheme," International Journal of Advanced Engineering Research and Science, vol. 4, no. 1, pp. 1–4, 2016.

[30] M. R. Albayati and A. H. Lashkari, "A new graphical Password based on decoy image portions (GP-DIP)," 2014 International Conference on Mathematics and Computers in Sciences and in Industry, Sep. 2014.

[31] S. Sayed, A. Mohid, M. Pal, and M. Haji, "Graphical Password based authentication system with sound sequence," International Journal of Computer Applications, vol. 138, no. 12, pp. 38–43, Mar. 2016.

[32] P. Gunde, and U. Kokate, "Graphical Password authentication by using persuasive click point method,"

International Journal of Science and Research (IJSR), vol. 5, no. 2, pp. 2138–2140, Feb. 2016.

[33] T. M.L., C. D. N., A. I., and D. Atsaam, "An enhanced Password-Username authentication system using cryptographic hashing and recognition based graphical Password," IOSR Journal of Computer Engineering, vol. 18, no. 04, pp. 54–58, Apr. 2016.

[34] "Shoulder surfing and Keylogger resistance using Two step graphical Password scheme," International Journal of Science and Research (IJSR), vol. 5, no. 6, pp. 2395–2399, Jun. 2016.

BIOGRAPHIES

Muhammad Ahsan is a student of Master in Computer Science and Technology in Beijing Institute of Technology, China. He completed his Bachelor degree in Software Engineering from University of Agriculture Faisalabad, Pakistan.

Yugang Li is Ph.D in School of Computer Science and Technology in Beijing Institute of Technology, China.