DOI: http://dx.doi.org/10.26483/ijarcs.v9i2.5761

ISSN No. 0976-5697

Volume 9, No. 2, March-April 2018

International Journal of Advanced Research in Computer Science

RESEARCH PAPER

Available Online at www.ijarcs.info

GRAPHICAL PASSWORD USING 2D COORDINATES

Purshottam J. Assudani
Shri Ramdeobaba College of Engineering and Management, Nagpur
Assistant Professor, Department of Information Technology
India

Ashish V. Chandak
Shri Ramdeobaba College of Engineering and Management, Nagpur
Assistant Professor, Department of Information Technology
India

Vinisha P. Assudani
St. Vincent Palloti College of Engineering and Technology, Nagpur
Assistant Professor, Department of Computer Engineering
India

Abstract: The security is main concern in each and every application. Graphical authentication provides secure way of authorization. Goal of knowledge specific authentication system is to provide support for user in selecting passwords for greater security. Here we are using 2D coordinates to secure a picture and generate a password. Additionally the pictures in x and y coordinates change randomly and hence it is difficult to find the original picture. Our base paper provides solution against the attacks possible on these approaches "Persuasive cued click points"," Cued click points " and "Pass points". We propose a system which removes the problem of shoulder surfing.

***Keywords*:** Authentication, Security, Graphical Passwords, Knowledge-based

I. INTRODUCTION

Graphical password act as an alternative for textual passwords. Research has demonstrated that content passwords have both security and ease of use issues [14]. Graphical password is a verification framework where client select from pictures, in an a request, appeared in a graphical UI. Content passwords are anything but difficult to recollect and assault. Psychology studies states that human brain is good at recognizing and recalling images and not text [10]. Pictures don't have user's language. Graphical passwords are attractive as people remember pictures in a better way than words [8].

A graphical password system encourages strong passwords with the maintenance of memory [3]. In our system, the task of selecting a strong password is more tedious. The advantage is that users only have to remember images to access the system. This approach includes multiple images and the user needs to enter the correct coordinates of the image [12]. In the click- based password method we use a concept called as Pass Points [3,4]which consists of sequence of click points on a given image. With Cued click point, users can select points on to *some* level of images i.e., in each and every level it takes a single click point on to a single image. In Persuasive cued click points, it selects single click point on single image using persuasive technology. From the point of security, the click oriented graphical authentication suffers with hotspot and shoulder surfing problems [7].

Three-factor authentication is an authentication system which includes all the three mechanisms and depends on:

- what you have (e.g.: token),
- who you are (e.g. biometric)
- what you know (e.g. password)

For successful authentication, the user must enter a password and provide a pass code generated by the token, and scan biometric features (e.g. fingerprint or pupil). The major drawback is that identification process may be slow and such systems may be unreliable and expensive also. However, it provides the top level of security [2]. Two-factor Authentication is more attractive and practical than three-factor Authentication and is based on token based and text based authentication system. The researchers have seen shortcomings of text passwords and shifted attention to passwords with graphical objects [11]. Graphical authentication is proposed as a user-friendly alternative for password generation and authentication [6]. In this approach the user enters the password by typing both the x and y coordinates of the original image. Passwords are more likely to be recognized and remembered if they are presented as pictures rather than the characters [9]. Thus, graphical password presumably delivers a higher usability as compared to text-based password [4].

II. PASS POINTS

Pass Points-style graphical passwords have been shown to be susceptible to hot-spots, which can be exploited in human-seeded attacks, whereby human-computed data is used to facilitate efficient attacks. These attacks require that the attacker collect sufficient "human-computed" data for the target image, which is more costly for systems with multiple images [5]. Each digital image has a pixel value which describes how bright that pixel is, and what color it should be. During extraction, the image files are dividing into grids; it can be 16 by 16 grids or 8 by 8 grids. Each grid is calculated with its pixel value with a compression algorithm. Then, all grids' pixel value will be transformed

into a single value with compression algorithm once again. In this graphical authentication method, pixel value will be used as authentication key for a password. In Pass Points password a password consists of sequence with 5 to 8 different click points on single image and points are chosen by user[10].

III. CUED CLICK POINTS

CCP is another option to Pass Points. Here, clients click one point on every c = 5 pictures instead of five focuses on one picture. The viewport is situated haphazardly to dodge referred to hotspots.

As with different graphical passwords, CCP is not intended for environments where shoulder-surfing is serious threat[1].

IV. PERSUASIVE CUED CLICK POINTS

The PCCP uses persuasive technology for motivating users to select passwords that are less guessable and makes it difficult to select every click point as hotspot. While creating password, the pictures are shaded, with the exception of the viewport. Viewport is arbitrarily situated to stay away from hotspots. Hotspot data enables assailants to enhance their theories and could deliver new hotspots. Selection of click point of user must be in the viewport only. By clicking outside of viewport, the system will not respond on user clicks [8]. The user can change the view-port area provided by the system when user is not satisfied with generated viewport area. At login phase, images are displayed without shading and users should select correct click points for authentication. Shoulder surfing and hotspots problem reduces the security in graphical based authentication. Attackers can be able to retrieve the passwords using the skewed password distribution [10].

V. PROPOSED SYSTEM AND IMPLEMENTATION

In this paper we present a more secure graphical password mechanism based on the random changing password technique. In Random changing coordinate password scheme, a given image password consists of sequence of different coordinate points. For password creation user needs to select any image from the group of images and for login the user need to enter series of coordinates in correct sequence in a system. The proposed authentication system consists of a sequence of “n” images and the user has to type the coordinates of original image. The user can choose up to 5 images as his password. This is to prevent incremental guessing attacks.

The proposed authentication system includes three phases:

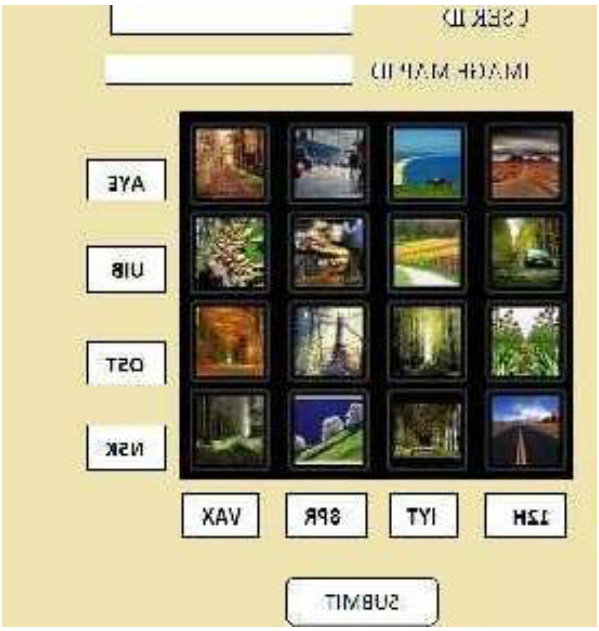
a) Registration Phase

To access the system the user first has to register. During registration, the user has to enter the user name, address, city, contact number and email id. After clicking on submit, he will be taken to the next screen where he can set up his password. The maximum number of images which can be chosen as passwords are 5 and the user need not remember them in order. Only remembering the image is sufficient, as each image is mapped according to a hidden code inside the image. The code is embedded in the image using the technique of watermarking

b)

Login Phase

In the login phase, only the registered user enters his username. The username is transmitted to the database by the server and is used as the key to retrieve the images associated with that user. The images are presented on screen in a metric form. Corresponding to them are X and Y coordinates. The user has to enter the coordinates of his image in the images map id. The user is authenticated if he enters the correct image coordinates.



c) Authentication Process

Passwords that should be confidential are readable easily when the key-stroke logs being retrieve by hacker. The password (image) has been stored in server through watermarking. The user is authenticated if the coordinates entered match his images chosen as password at the time of registration. To overcome Brute Force attack, the number of login attempts is limited. Once the attempts are over the account gets locked.

VI. ADVANTAGES

This authentication method brings a lot of benefits. First, key-logger is unable to capture the Technique used. Second, multilevel authentication will protect login page from brute-force attack or dictionary attacks or shoulder surfing attacks.

VII. CONCLUSION

The authentication is the fundamental component in most security contexts. In this paper, we propose a more secure graphical authentication system. The system combines graphical password scheme along with random changing images and XY coordinates. This authentication system ensures the protection from threats such as key loggers, hotspot, and shoulder surfing etc. Random changing image coordinate value is a more secure authentication scheme.

REFERENCES

[1] S.Chiasson, P. van Oorschot, and R. iddle, "Graphical Password Authentication Using Cued Click Points," Proc. European Symp. Research in Computer Security (ESORICS), pp. 359-374, Sept. 2007

[2] L. O'Gorman, "Comparing Passwords, Tokens, and Biometrics for User Authentication," Proc. IEEE, vol. 91, no. 12, pp. 2019-2020, Dec. 2003.

[3] S. Wiedenbeck, J. Waters, J. Birget, A.Brodskiy, and N. Memon, "Pass Points: Design and Longitudinal Evaluation of a Graphical Password System," Int'l J. Human-Computer Studies, vol. 63, nos. 1/2, pp. 102-127, 2005.

[4] S. Wiedenbeck, J. Waters, J. Birget, A. Brodskiy, and N. Memon, "Authentication Using Graphical Passwords: Effects of Tolerance and Image Choice," SOUPS '05 Proceedings of the 2005 symposium on Usable privacy and security, pp.1-12, July 2005.

[5] P.C. van Oorschot, A. Salehi-Abari, and J. Thorpe, "Purely Automated Attacks on PassPoints-Style Graphical Passwords," IEEE Trans. Information Forensics and Security, vol. 5, no. 3, pp. 393- 405, Sept. 2010.

[6] H.Faumia, B.Abirami, K.Muthulakshmi, M. Kasthuri, "A Knowledge Based Graphical Authentication Using X and Y Coordinates", International Journal of Soft Computing and Engineering (IJSCE) ISSN: 2231-2307, Volume-4, Issue-1, March 2014

[7] Aakansha Gokhalea, Vijaya Waghmare, "The shoulder Surfing Resistant Graphical Password Authentication Technique", 7th International Conference on Communication, Computing and Virtualization, ELSEVIER, pp. 490-498, 2016

[8] R. Shepard, "Recognition memory for words, sentences,and pictures", Journal of Verbal Learning and VerbalBehavior, 6:156-163, 1967.

[9] W. Jansen, S. Gavrila, V. Korolev, R. Ayers, and R. Swanstrom, "Picture Password: A Visual Login Technique for Mobile Devices," National Institute of Standards and Technology Interagency Report NISTIR 7030, 2003.

[10] Martin Mihajlov, Borka Jerman, Marko Ilievski, "Image Pass - Designing Graphical Authentication for Security" 7th International Conference on Next Generation Web Services Practices, October 2011.

[11] Christopher Varenhorst, Larry Rudolph, "Passdoodles; a Lightweight Authentication Method", Massachusetts Institute of Technology, Research Science Institute, July 2004.

[12] Md. Asraful Haque, Babbar Imam, "A New Graphical Password: Combination of Recall & Recognition Based Approach", International Journal of Computer, Information, Systems and Control Engineering, Vol: 8 No: 2, 2014, pp.320-324.

[13] Sayli Chavan, Shardul Gaikwad, Prathama Parab, Govind Wakure, "Graphical Password Authentication System", International Journal of Computer Science and Mobile Computing, Vol.4 Issue.4, April- 2015, pg. 324-329

[14] S. Chiasson, A. Forget, R. Biddle, and P. C. van Oorschot, "Influencing users towards better passwords: persuasive cued click-points", in Proc. British HCI Group Annual Conference on People and Computers: Culture, Creativity, Interaction, vol. 1, 2008, pp. 121-130.