A Knowledge Based Graphical Authentication Using X and Y Coordinates

H.Faumia, B.Abirami, K.Muthulakshmi, M.Kasthuri

Abstract- Graphical authentication is more efficient and more securable. An important usability goal for knowledge based authentication systems is to support user in selecting passwords for higher security in the sense of being from an expanded effective security space. Here we are using x and y coordinates to choose a picture password. Additionally the pictures in x and y coordinates are changing randomly and hence it is difficult to find the original picture. In our base paper the approaches used are "Persuasive cued click points"," Cued click points" and "Pass points". Main tools used here are pccp, viewport and that is used for password creation. Viewport approaches are used to memorable user chosen password and secure system generated random password that are difficult to remember. The pccp creating a less guessable password is the easiest course of action. In order to avoid "Shoulder surfing" algorithm we are going for AES (Advanced encryption standard).

Index Terms—Authentication, Security, Graphical Passwords, Knowledge-based .

I. INTRODUCTION

Authentication is an essential thing, which prevents unknown person in a computer based environment system. Text based passwords are easy to remember and easy to attack. A graphical password authentication system should encourage strong passwords while maintaining memorability. In our system the task of selecting strong password is more tedious. The advantage is that users only have to remember a master password to access the management tool. This approach includes multiple images and the user need to select the correct coordinate of the image. Graphical passwords are attractive since people usually remember pictures better than words. In pass-points method, users have to select click points on a single image. In Cued click point method, users can select click points up to n level of images i.e., in each level it takes a single click point on a single image. In the case of Persuasive cued click points (PCCP), it selects one click point on one image using persuasive technology.From the security point of view, the click based graphical authentication suffered with hotspot and shoulder surfing problems. A sequence of pictures is more memorable than a sequence of characters. Pictures are independent from user's language. There do not exist yet special dictionaries for a dictionary attack and it is very difficult to be constructed (especially for graphical passwords that have a very large password space). Automated attacks are difficult to take place.

Manuscript Received on March, 2014.

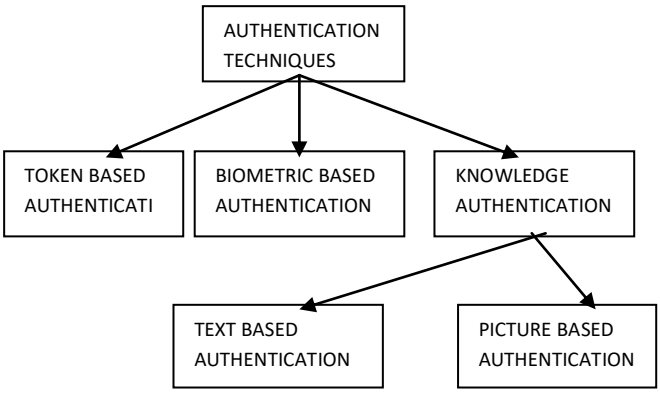
H.Faumia,Pursuing B.E degree in Tejaa Shakthi Institute of Technology For Women, Coimbatore, Tamil Nadu, India.

B.Abirami, Pursuing B.E degree in Tejaa Shakthi Institute of Technology For Women, Coimbatore, Tamil Nadu, India.

K.Muthulakshmi, Pursuing B.E degree in Tejaa Shakthi Institute of Technology For Women, Coimbatore, Tamil Nadu, India.

M.Kasthuri, Pursuing B.E degree in Tejaa Shakthi Institute of Technology For Women, Coimbatore, Tamil Nadu, India.

II. TYPES OF AUTHENTICATION



Three-factor authentication is an authentication system which includes all the three mechanisms and depends on what you have (e.g.: token), and who you are (e.g. biometric) what you know (e.g. password). To pass the authentication, the user must enter a password and provide a pass code generated by the token, and scan her biometric features (e.g.fingerprint or pupil). The major drawback of this approach the identification process can be slow and such systems can be expensive, unreliable. However, this type of technique provides the highest level of security. Two-factor Authentication is more attractive and practical than three-factor Authentication and is based on token based and text based authentication system. To overcome some of the shortcomings of the textual passwords, researchers turned their attention to passwords that utilize graphical objects. Graphical authentication has been proposed as a user-friendly alternative to password generation and authentication.In this approach the user enters the password by typing the x and y coordinates of the original image in a predefined and secret order.Passwords are more likely to be recognized and remembered if they are presented as pictures rather than as words.Thus, graphical password presumably delivers a higher usability compared to text-based password.

III. PERSUASIVE CUED CLICK POINTS

The PCCP uses persuasive technology to motivate users to select less guessable passwords and make it more difficult to select every click point as hotspot. Mainly at the time of password creation the images are shaded except viewport and it is positioned randomly to avoid hotspots. This hotspot information allows attackers to improve guesses and could have a chance to produce new hotspots. Viewport size is intended to offer a variety of distinct points but still cover only an acceptably small fraction of all possible points. Selection of click point of user must be inside the viewport only. Outside of the viewport will not respond for user clicks. The user has the flexibility to change the view-port area which is provided by the system

whenever a user doesn't satisfy with the generated viewport area. At the login phase, images are displayed without shading and users needed to select correct click points for authentication.

Hotspots and shoulder surfing problem reduces the security in the graphical based authentication. Attackers can retrieve the passwords using skewed password distribution.

IV. CUED CLICK POINTS

By adding a persuasive feature to CCP, PCCP encourages users to select less predictable passwords, and makes it more difficult to select passwords where all five click-points are hotspots. Specifically, when users create a password, the images are slightly shaded except for a Viewport. The viewport is positioned randomly, rather than specifically to avoid known hotspots, since such information might allow attackers to improve guesses and could lead to the formation of new hotspots. The viewport's size is intended to offer a variety of distinct points but still cover only an acceptably small fraction of all possible points. Users must select a click-point within this highlighted viewport and cannot click outside of the viewport, unless they press the shuffle button to randomly reposition the viewport. While users may shuffle as often as desired, this significantly slows password creation. The viewport and shuffle button appear only during password creation. During later password entry, the images are displayed normally, without shading or the viewport, and users may click anywhere on the images. Like Pass Points and CCP, login click-points must be within the defined tolerance squares of the original points.

V. PASS POINTS

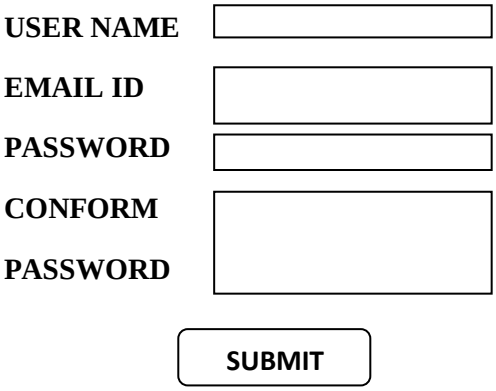
Each digital image files stored inside a computer has a pixel value which describes how bright that pixel is, and what color it should be. During extraction, the image files are dividing into grids; it can be 16 by 16 grids or 8 by 8 grids. Each grid is being calculated its pixel value with compression algorithm. Then, all grids' pixel value will be transform into a single value with compression algorithm once again. This is how pixel value is being produce and acquire from an image. In this graphical authentication method, pixel value will be used as authentication key for a password. Pass Points graphical password scheme, in which a password consists of sequence of 5 to 8 different click points on a single image and the click points are chosen by the user. The image is displayed on the screen by the system. The image is not secure and has no role other than helping the user remember the click points. Any pixel value in the image is a candidate for a click point. Pass-Point comes over click based graphical password scheme.

VI. PROPOSED SYSTEM

In this paper we present a more secure graphical password mechanism based on the random changing password technique. Random changing coordinate password scheme is the one in which a given image password consists of a sequence of different coordinate points. For password creation user selects any image in the group of images and for login the user has to enter the same series of coordinates in correct sequence within a system. The proposed authentication system consists of a sequence of "n" images and the user has type the coordinates of original image. This is to prevent incremental guessing attacks. The proposed authentication system includes three phases. We introduce the details of these three phases respectively.

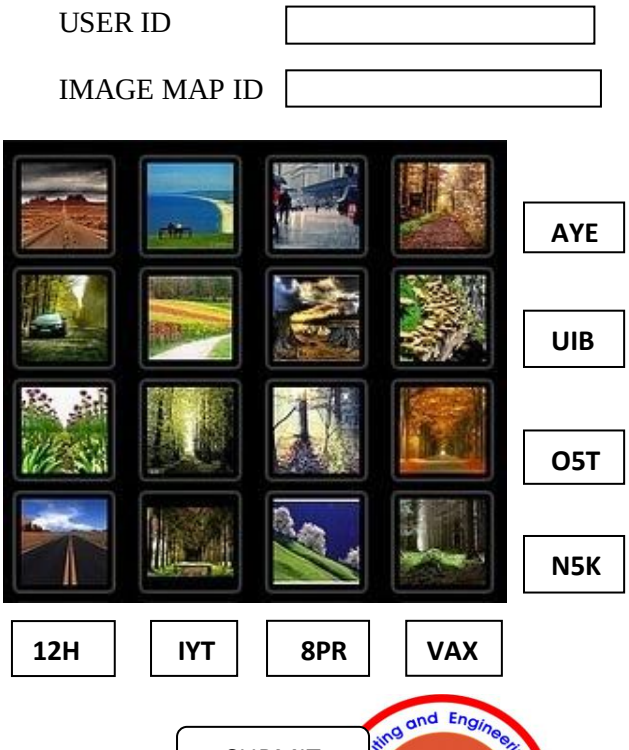
a) Registration Phase

The user to get access to the website and to get privileged to access the services, the first is to register to the website. During registration, the user wants to enter the user name,mail id,password and conformation password.After entering the above details, a random verification code will be sent to the above email address mentioned.Again the user name and the password are verified and it enters into the login form. The encryption and decryption are also performed by using AES algorithm.



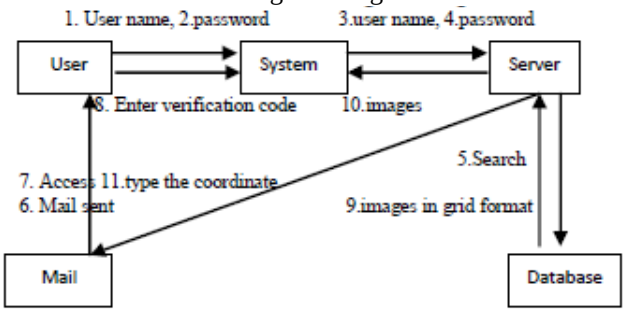
b) Login Phase

In the login phase, the user submits the username to the website. The username transmitted to the database by the server is used as the key to retrieve the images associated with that user. One image among the "n" is chosen randomly and is provided to the server. The user is asked to choose the original image password as shown in figure. The user is authenticated if the user selects the correct image. The incorrect image leads to the unsuccessful authentication.



c) Authentication Process

Passwords that should be confidential are readable easily when the key-stroke logs being retrieve by hacker. The password has been stored in server and the extracted image file through AES algorithm(ADVANCED ENCRYPTION STANDARD).It is kept secretly on database and even user have no idea about the coordinates. This authentication method bring a lot of benefits which is :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. The proposed system includes number of images and in that the users want to select the original image.



VII. ADVANTAGES

Proposed system is more secure and privacy, its concentrate on all attributes of security and privacy. It prevents the user from selecting the wrong cue point,instead he can enter the exact cue point image were others can unable to guess the process to offer different levels of privacy to cloud customers.

VIII. CONCLUSIONS

User authentication is a fundamental component in most computer security contexts. In this paper, we propose a more secure graphical authentication system. The system combines graphical password scheme along with random changing images. 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 securable authentication factor.

REFERRENCES

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,” Proc. First Symp. Usable Privacy and Security (SOUPS), 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. S. Chiasson, E. Stobert, A. Forget, R. Biddle, and P. van Oorschot, “Persuasive Cued Click-Points: Design, Implementation, and Evaluation of a Knowledge-Based Authentication Mechanism,” Technical Report TR-11-03, School of Computer Science, Carleton Univ., Feb. 2011.
7. A. Forget, S. Chiasson, and R. Biddle, “Shoulder-Surfing Resistance with Eye-Gaze Entry in Click-Based Graphical Passwords,” Proc. ACM SIGCHI Conf. Human Factors in Computing Systems (CHI), 2010.
8. B. Pinkas and T. Sander, “Securing Passwords against Dictionary Attacks,” Proc. Ninth ACM Conf. Computer and Comm. Security (CCS), Nov. 2002.
9. Alireza Pirayesh Sabzevar and Angelos Stavrou, “Universal Multi-Factor Authentication Using Graphical Passwords,” in IEEE International Conference on Signal Image Technology and Internet Based Systems, 2008.
10. Ahmad Almulhem, “A Graphical Password Authentication System,” in 978-0-9564263-7/6/$25.00 IEEE, 2011
11. S. Man, D. Hong, and M. Mathews, "A shoulder-surfing resistant graphical password scheme," in Proceedings of International conference on security and management. Las Vegas, NV, 2003
12. Birget, J.C., D. Hong, And N. Memon, “Graphical Passwords Based On Robust Discretization” IEEE Trans. Info. Forensics And Security, 1(3), September 2006.
13. Thorpe, J. and P.C. van Oorschot. Human-Seeded Attacks and Exploiting HotSpots in Graphical Passwords. 16th USENIX Security Symposium, 2007.
14. Zhi Li, Qibin Sun, Yong Lian, and D. D. Giusto, 2005, „An Association-Based Graphical Password Design Resistant to Shoulder Surfing Attack“, IEEE International Conference on Multimedia and Expo (ICME).

AUTHOR PROFILE

H.FAUMIA,Pursuing B.E degree in Tejaa Shakthi Institute of Technology For Women, Coimbatore, Tamil Nadu, India.

B.ABIRAMI, Pursuing B.E degree in Tejaa Shakthi Institute of Technology For Women, Coimbatore, Tamil Nadu, India.

K.MUTHULAKSHMI, Pursuing B.E degree in Tejaa Shakthi Institute of Technology For Women, Coimbatore, Tamil Nadu, India.

M.KASTHURI Pursuing B.E degree in Tejaa Shakthi Institute of Technology For Women, Coimbatore, Tamil Nadu, India.