Password Authentication using Click based Graphical passwords and Color-Login

Manasa C

***Abstract*— *Abstract*- The growth of technology in the field of computer science & the popularity of information technology has changed the means of information exchange from letters to electronic messages. Security became a major concern with the advent of electronic messages as it led to higher possibilities of information attacks. One of the proposed solutions to this problem is the usage of passwords to protect the information. Password is a string of characters used for user authentication to prove identity or approval to gain access to a resource, which should be unknown to or kept secretive from unauthorized users. The most common types of passwords are Numeric Passcodes, Textual Passcodes or Alpha numeric Passcodes. These types of passwords are vulnerable to various kinds of attacks, such as eaves dropping, shoulder surfing, dictionary attack, spyware attack etc. This paper proposes a unique idea of AUTHENTICATING PASSWORDS using CLICK BASED GRAPHICAL PASSWORDS AND COLOR-LOGIN SCHEMES. These authentication mechanisms generate stronger passwords & hence present a more feasible way of making variation in the security level of an application depending upon the user's requirement.**

***Index Terms*— password, authentication, click points, color-login, security.**

I. INTRODUCTION

The problems of knowledge based authentication – especially text based passwords, are well known. Users often tend to create memorable passwords that are easy for the unauthorized users to guess, but strong, system-assigned passwords are difficult for the users to remember. Strong passwords must be encouraged by the Password authentication system in order to maintain ease of usage & memorability [24]. The proposed authentication schemes allow users, to choose stronger passwords. The proposed system makes the task of selecting weak passwords more tedious. Rather than increasing the burden on users, it is better to follow the application that creates a secure password – a feature lacking in most of the systems.

This approach is to create the first persuasive click based graphical password system, Persuasive Cued Click-Points (PCCP) [2], [3], and conducted user studies evaluating usability and security. This paper presents a consistent assimilation of earlier work [1], [2], [3], [4], [5] reinterprets and updates analysis incorporating larger data sets, provides new evaluation of password and extends security analysis that includes relevant recent attacks. This systematic examination provides a comprehensive and integrated evaluation of PCCP covering both usability and security issues. A novel graphical password scheme Color-Login is also proposed in this paper. Color-Login is implemented in an interesting way to weaken the boring feelings of the authentication. Color-Login uses background color, a method not previously considered, to decrease time consumption while login. Multiple colors are used to confuse the peepers, while not burdening the authorized users. Meanwhile, the scheme is resistant to shoulder surfing and as well as intersection attack to a certain extent

Manuscript received January 06, 2015.

Manasa C, M.Tech, I Sem, Department of Computer Science, M S Ramaiah Institute of Technology, Bangalore - 560054

II. RELATED WORK

Graphical password schemes [27], [28], [29], [30] are based on the concept of choosing multiple images as pass objects. It usually requires users to recognize the pre-selected pictures and repeat the select actions in sequence. As the first choice of multiple images is pass objects scheme, it is based on Hash Visualization technique [6], which authenticates a user through the ability to recognize previously registered images [7]. As a result of the random generation of candidate images, it is not convincing to conclude that graphical passwords are easier to remember and recall than text-based passwords. This scheme has proved to be effective against shoulder surfing attacks, and yet as it is alphanumeric-based scheme; it contains the inevitable drawbacks of alphanumeric passwords.

III. CLICK BASED GRAPHICAL PASSWORD

Text passwords are the most popular user authentication method, but have security and usability problems. Graphical passwords along with persuasive cued click points offer another alternative, and are the focus of this paper. Graphical password systems are kind of knowledge-based authentication that attempts to assist the human memory for visual information [8]. A review of graphical passwords is available in the reference [9]. We are here interested in cued-recall click-based graphical passwords (it is also known as locimetric [10]).Previously selected locations within one or more images are identified and targeted by the users in such systems. The images act as memory cues [11] in order to help recall. Examples for such systems are Pass-Points [12] and Cued Click- Points (CCP) [13].

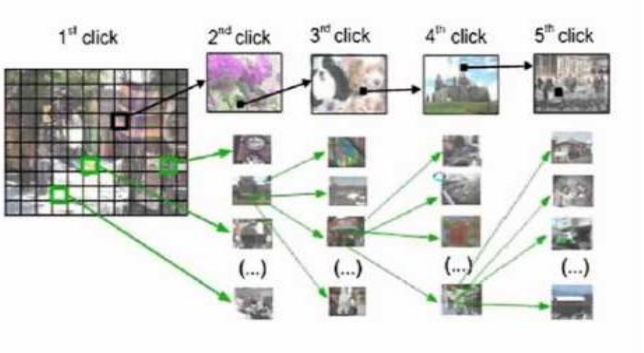

Figure.1: A user navigates through images to form a CCP password. Each click determines the next image.

In Pass-Points, passwords comprises of a sequence of five click-points on a given image. Users have the liberty to select any pixels in the image for their password as click-points. In order to log in, they will have to repeat the sequence of clicks in the correct order, within a defined tolerance square of the original click-points. Although Pass-Points are relatively usable [1], [12], [14], in few applications security weaknesses make passwords to be predicted easily by attackers. Hotspots [15], [16], [17], [18] are areas of the image that have higher chances of being clicked by users as password click-points. Attackers who have knowledge of these hotspots through building sample passwords in the first instance can build attack dictionaries and successfully guess Pass-Points passwords [16], [17].

A precursor to PCCP, Cued Click Points [13] was introduced to reduce patterns and to reduce the advantage of hotspots for attackers. Instead of five click-points on one image, CCP uses only one click-point on five different images shown serially. The location of the previously entered click-point (Figure.1) influences the next image to be displayed, creating a path through image set. Users select their images only to the extent that their click-point determines the next image. Creating a new password with different click-points will result in a different image sequence.

3.1. Persuasive Technology

Persuasive Technology was first introduced by Fogg [19] as a technology to motivate and influence people to behave in a desired manner. An authentication system which uses Persuasive Technology should guide and encourage users to select stronger passwords, but not use system-generated passwords. In order to be effective, the users must not ignore the persuasive elements and the resulting passwords must be memorable. PCCP accomplishes this by making the aspect of selecting a weak password more tedious and time consuming. Selecting a stronger password is the path of least resistance for users. The formation of hotspots across users is minimized since click-points are more randomly distributed. PCCP's design follows Fogg's Principle of Reduction by choosing a strong password in easiest way and the Principle of Suggestion by embedding suggestions for a strong password directly within the process of choosing a password.

3.2. Persuasive cued click points

From the above study we can observe that hotspots and patterns reduce the security of click-based graphical passwords, as attackers can use skewed password distributions to predict and give priority to the higher probability passwords for more successful guessing attacks. Visual attention research [20] shows that different people are attracted towards the same predictable areas of an image. This suggests that if users select their own graphical passwords which are click based without guidance, hotspots will remain an issue. Davis et al. [21] suggest that user choice in all types of graphical passwords is not advisable due to predictability. Investigation has been done [2], [3], [4], [5] whether the system could influence users to select more random click-points while maintaining the usability. The goal was to develop more secure behavior by making less secure choices of selecting weak passwords. In effect, incorporating more secure passwords became the safe path of least resistance [2]. By adding a persuasive feature to CCP [13], PCCP [2] encouraged the users to select less predictable passwords, and selecting password is more difficult where all five click-points are hotspots. Specifically, when users create a password, the images are slightly shaded except for area which is called viewport (Figure.2). The viewport is positioned randomly, rather than particularly at a specific location to avoid known hotspots, since such information might allow unauthorized users to improve guesses and could help in the formation of new hotspots.

Figure.2:Create password interface for PCCP.

IV. DESIGN OF COLOR-LOGIN

In Color-Login, there are four security levels called as low, medium, high and self-define respectively. There are six parameters, R, C, k, N, C, h and n wherein R, C, k and n are determined by the levels defined above.

- R is the number of rounds for authentication, which ranges from 1 to 3 respectively to define low, medium and high security levels.
- C is the number of colors used, which ranges from 3 to 5.
- k is the number of pass-icons.
- NC is the number of total icons per color is present in the database for different values of C. N3 =40, N4 =72 and
- N5 =112.
- h is the number of pass-icons shown on each screen,
- n is the number of rows or columns, and n=9, 12 or 15

Figure.3: A set of chosen color icons displayed to the user to create pass icons.

In the registration phase, shown in Figure.3, the operations of the user can be divided into three steps:

- Choose a security level needed.
- Choose one color from the C colors randomly provided by system.
- Choose k images from the sets of the chosen color as pass-icons (i.e. password).

The generation process of each round in the authentication phase is described as below:

- Randomly generate the ith round screen, where the icon groups are distributed by a sequence of sliding color. In each group, icons which are randomly chosen from the database form a single color icon square, but they are not permanent. On the whole screen, there would be C number of such color squares, filling in the coarse grid. And each icon on the screen will be different.
- When the icons are distributed, h of the k pass-icons will be displayed randomly in h different lines. For example, in Figure.4 (a), there are two of the three pass-icons lying in two different lines in the authentication round.
- Wait for the user to click on the pass-icon and replace all icons on the line with icons substituted.
- In order to authenticate the user gather the input information.

4.a) The Displayed screen

4.b) A Complete round

Figure.4: A completed authentication round is shown here (R = 1, C = 3, n = 9, h = 2). It contains two pass-icons in two lines. When the user clicks on a line, the icons in that line are replaced by the substituted icon.

In each login, the system challenges a user who wants to be authenticated. The challenge is conducted in R round and each round will provide the random icons that are displayed on the screen. An example of such a challenge round is shown in Figure 4; in which blue and green are inducing ones while red is the focused color. A pass-icon is chosen correctly when the user clicks on the row which contains the pass-icon. Then the icons in that row are all replaced by a substituted Lock icon to resist against the shoulder-surfing attack. A round is considered to be a successful indication when all the h hiding pass-icons are correctly chosen as shown in Figure 4. In order to reduce users' memory burden, it is not necessary for them to choose in a particular order. The login screen is divided into C×C background color squares. Once a user chooses his color, both colors and their positions shown on each screen for the same user would be fixed. The icons for each color are randomly chosen from the database and all are different. The h pass-icons which are randomly chosen are displayed on different rows. Considering usability and security, we set h=2. If h=1, the probability of an attacker's successful login will be greater. And if h≥3, the time period for legal users to find pass-icons will be longer.

V. ANALYSIS OF THE COLOR-LOGIN SCHEME

5.1. Background Color

Most of the time is spent in locating the pass-icons from large number of icons which are randomly placed while users log into the schemes which choose multiple images as pass-icons. Color is one of the most important features of images. But it has been never before considered in previous multiple image choice schemes. First the background color of images is proposed and then used in Color-Login. In Color-Login, the icons on the screen can be distinguished clearly by different colors. When users have to recognize the pass-icons in the authentication phase, they only need to concentrate on the icons of the predefined color rather than all the icons displayed. As shown in Figure 4, 81 icons are present and users only need to search for the pass-icons from 27 red icons. Thus, relative to similar schemes without background colors introduction of colors can cut workload of

2/3. This is just an instance at the lowest level. More colors are introduced with a decreased workload in case of higher levels. At most, 5 colors can be used in Color-Login scheme and 4/5 of the workload can be reduced. It can be concluded that the login time can be reduced greatly. Further, if the authentication procedure is tedious, it may create difficulties in memorizing. The use of background colors can create a friendly user interface, which helps users escape from the confusion of large numbers of icons.

5.2. Resistance to Shoulder Surfing

Color-Login scheme is resistant to shoulders surfing attack [23], [25]. In this scheme, there are different icons on the screen in each login round. Neither the icons nor the pass-icons displayed are fixed. When the user finds a pass-icon, he has to click on the line where the pass-icon is present, rather than the pass-icon itself. After the mouse action, the icons in the clicked line will be replaced by icons substituted. Although such replacement is of no use in resisting shoulder surfing when the process is video tape recorded, it is very helpful to resist shoulder watchers, where the peepers cannot remember the icons in a short period of time.

VI. CONCLUSION

The proposed authentication schemes influence users to choose stronger passwords. Users can successfully login by giving the right password. This system, when compared to the existing text-based authentication systems, is less prone to shoulder surfing attacks. The approaches discussed in this paper present a middle ground approach between insecure but memorable chosen passwords and secure system generated passwords that are difficult to remember. In PCCP, creating a password that is less guessable (by selecting a click-point within the first few system-suggested viewport positions) is the easiest course of action that could be made. Users still make a choice but they are constrained in their selection. Color-Login is a graphical passwords method to develop more effective, user friendly and secure passwords. In this paper, image background color is introduced as a means of reducing the user's login time, which is considered to be crucial to the usability of a password scheme. It aims to motivate the user with a friendly interface designed to improve user experience and provide login time which is acceptable. Color-Login is a promising technique which can be developed further by studies.

VII. ACKNOWLEDGEMENT

I consider it is a privilege to express my gratitude and respect to all those who guided me in the completion of technical paper. The research presented in this paper is supported by management of M.S.Ramaiah Institute of Technology. It's a great privilege to place on record my deep sense of gratitude to our HOD Dr. K. G. Srinivas, of Computer Science & Engineering, M.S.Ramaiah Institute of Technology. I am grateful to thank to Dr. S.Y.Kulkarni, Principal, M.S.Ramaiah Institute of Technology. I am grateful to Dr. Monica R Mundada, Associate Professor, Computer Science & Engineering Department, M.S.Ramaiah Institute of Technology, for her invaluable support and guidance. I would like to thank the reviewers for their time and expertise, constructive comments and valuable insights.

REFERENCES

[1]. S. Chiasson, R. Biddle, and P. van Oorschot, "A Second Look at the Usability of Click-Based Graphical Passwords," Proc. ACM Symp. Usable Privacy and Security (SOUPS), July 2007.
[2]. S. Chiasson, A. Forget, R. Biddle, and P. van Oorschot, "Influencing Users towards Better Passwords: Persuasive Cued Click- Points," Proc. British HCI Group Ann. Conf. People and Computers: Culture, Creativity, Interaction, Sept. 2008.
[3]. S. Chiasson, A. Forget, E. Stobert, P. van Oorschot, and R. Biddle, "Multiple Password Interference in Text and Click-Based Graphical Passwords," Proc. ACM Conf. Computer and Comm. Security (CCS), Nov. 2009.
[4]. E. Stobert, A. Forget, S. Chiasson, P. van Oorschot, and R. Biddle, "Exploring Usability Effects of Increasing Security in Click-Based Graphical Passwords," Proc. Ann. Computer Security Applications Conf. (ACSAC), 2010.
[5]. S. Chiasson, A. Forget, R. Biddle, and P.C. van Oorschot, "User Interface Design Affects Security: Patterns in Click-Based Graphical Passwords," Int'l J. Information Security, vol. 8, no. 6, pp. 387- 398, 2009.
[6]. Perrig A. and Song D., Hash Visualization: A New Technique to Improve Real-World Security. In Proceedings of the 1999 International Workshop on Cryptographic Techniques and E-Commerce, 1999.
[7]. Dhamija R. and Perrig A., Déjà Vu: A User Study Using Images for Authentication.In Proceedings of 9th USENIX Security Symposium, 2000.
[8]. D. Nelson, V. Reed, and J. Walling, "Pictorial Superiority Effect,"J. Experimental Psychology: Human Learning and Memory, vol. 2,no. 5, pp. 523-528, 1976.
[9]. R. Biddle, S. Chiasson, and P. van Oorschot, "Graphical Passwords: Learning from the First Twelve Years," to be published in ACM Computing Surveys, vol. 44, no. 4, 2012.
[10]. A. De Angeli, L. Coventry, G. Johnson, and K. Renaud, "Is a Picture Really Worth a Thousand Words? Exploring the Feasibility of Graphical Authentication Systems," Int'l J. Human-Computer Studies, vol. 63, nos. 1/2, pp. 128-152, 2005
[11]. E. Tulving and Z. Pearlstone, "Availability versus Accessibility of Information in Memory for Words," J. Verbal Learning and Verbal Behavior, vol. 5, pp. 381-391, 1966.
[12]. S. Wiedenbeck, J. Waters, J. Birget, A. Brodskiy, and N. Memon,"PassPoints: Design and Longitudinal Evaluation of a GraphicalPassword System," Int'l J. Human-Computer Studies, vol. 63,nos. 1/2, pp. 102-127, 2005.
[13]. S. Chiasson, P. van Oorschot, and R. Biddle, "Graphical Password Authentication Using Cued Click Points," Proc. European Symp. Research in Computer Security (ESORICS), pp. 359-374, Sept. 2007.
[14]. 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.
[15]. K. Golofit, "Click Passwords under Investigation," Proc. 12th European Symp. Research in Computer Security (ESORICS), Sept.2007.
[16]. A. Dirik, N. Menon, and J. Birget, "Modeling User Choice in the Passpoints Graphical Password Scheme," Proc. Third ACM Symp.Usable Privacy and Security (SOUPS), July 2007.
[17]. J. Thorpe and P.C. van Oorschot, "Human-Seeded Attacks and Exploiting Hot-Spots in Graphical Passwords," Proc. 16th USENIX Security Symp., Aug. 2007.
[18]. A. Salehi-Abari, J. Thorpe, and P. van Oorschot, "On Purely Automated Attacks and Click-Based Graphical Passwords," Proc. Ann. Computer Security Applications Conf. (ACSAC), 2008.
[19]. B. Fogg, Persuasive Technologies: Using Computers to Change What We Think and Do. Morgan Kaufmann Publishers, 2003.
[20]. J. Wolf, "Visual Attention," Seeing, K. De Valois, ed., pp. 335-386,Academic Press, 2000.
[21]. D. Davis, F. Monrose, and M. Reiter, "On User Choice in Graphical Password Schemes," Proc. 13th USENIX Security Symp., 2004.
[22]. Klein, D., Foiling the Cracker: A Survey of, and Improvements to, Password Security. In Proceedings of the USENIX Security Workshop, pp.5-14, 1990.

[23]. Roth, V., Richter, K., and Freidinger, R., A PIN-Entry Method Resilient Against Shoulder Surfing. In Conference on Computer and Communications Security,pp.236-245. 2004.
[24]. Paivio, A., Rogers, T.B., and Smythe, P.C., Why are pictures easier to recall then words? Psychonomic Science,11(4), pp.137-138, 1976.
[25]. Man S., Hong D., and Mathews M., A shoulder surfing resistant graphical password scheme. SAM 2003.
[26]. Haichang Gao, Xuewu Guo, Xiaoping Chen, Liming Wang, and Xiyang Liu, YAGP: Yet Another Graphical Password Strategy, ACSAC, California, USA, pp. 121-129,2008.
[27]. Blonder G. E., Graphical passwords. In Lucent Technologies, Inc., Murray Hill, NJ, U. S. Patent 5559961, Ed. United States, 1996.
[28]. Ian, J., Mayer, A., Monrose, F., Reiter, M.K., Rubin, A.D.: The Design and Analysis of Graphical Passwords. In: Proceedings of The Eighth USENIX Security Symposium, pp.1–14. USENIX Association, 1999.
[29]. Lashkari, A.H., Towhidi, F.: Graphical User Authentication (GUA). Lambert Academic Publishing, Germany, ISBN: 978-3-8433-8072-0,2010.
[30]. Sobrado, L., Birget, J.-C.: Graphical Passwords. The Rutgers Scholar, an Electronic Bulletin for Undergraduate Research 4, 2002

Manasa C, M.Tech, I Sem, Department of Computer Science, M S Ramaiah Institute of Technology, Bangalore-560054