ISSN:0975-9646

Comparative Analysis of Recall-based (Drawmetric) and Click-based (Locimetric) Graphical Password Authentication Schemes

[#1]Km Ritu, [#2]Rajiv Ranjan Singh, [#3]Bharti Kumar

Department of Computer Science, ShyamLal College (Evening), University of Delhi, Delhi, INDIA

Abstract- The authentication process can be broken up in "identification", "verification" and "authorization" steps. For both identification and verification, passwords are simplest of the means. They are the most frequently used technique for determining whether someone or something is, in fact, who or what as being claimed. Traditionally textual passwords are used for authentication. Such passwords, apart from having the weakness of being tough to remember, are also vulnerable to many known categories of attacks such as dictionary attacks etc. This has led to introduction of graphical passwords for authentication. These passwords are easier to remember and have the capability of including extra security features into them. This paper presents a comparative analysis of two mostly used techniques in the Graphical User Authentication Algorithms: Recall-based (Drawmetric) and Click-based (Locimetric) techniques based on various features and their response to various security attacks.

Keywords - Graphical Password, User Authentication, Recall-based, Click-based, Drawmetric, Locimetric

I. INTRODUCTION

Passwords have been used for authentication for a long time now. A password can be defined as a word or combination of characters, special symbols and digits that is known to the user and the verifier who in turn will allow the user to access some resources. These kinds of passwords are also called alphanumeric passwords. The motivating factor behind the use of image based passwords is that human perform far better when remembering shapes than alphanumeric strings [1]-[4]. Survey shows that the main problem with alphanumeric password systems is that they can be guessed easily [5].If a password is difficult to guess then due to human memory limitations, it is difficult to remember. So to overcome this limitation and to improve security, graphical password scheme was proposed which uses graphics as passwords. Research has been shown that a human can remember images better than text [6].

There are many different techniques available. We focus on two schemes of Graphical User Authentication Algorithms: Drawmetric and Locimetric in order to understand their merits, limitations and security issues.

II. GRAPHICAL PASSWORDS SCHEMES

A. Drawmetric or Recall Based Graphical Password Schemes

In recall based graphical password schemes the user is asked to reproduce something (usually an image) that he or she created or selected during the registration phase. This scheme further has been divided in to two categories: pure recall based and cued recall based techniques. In pure recall based technique the user enter his or her password without any hint or clue. On the other hand in cued recall based technique the image provide some hint to the user in order to enter the password.

i. DRAW-A-SECRET (DAS) [7]

DAS was proposed by Jermyn et al. in 1999. It is a typical implementation in which user draw a design on the grid using mouse or stylus. The drawing consists of one continuous stroke or may be several strokes separated by "pen-ups", on a rectangular grid of size M*M. The drawing is then mapped to a sequence of coordinate pairs of the grid cells. For eg.lets consider a grid of size 4*4 in the figure 1.

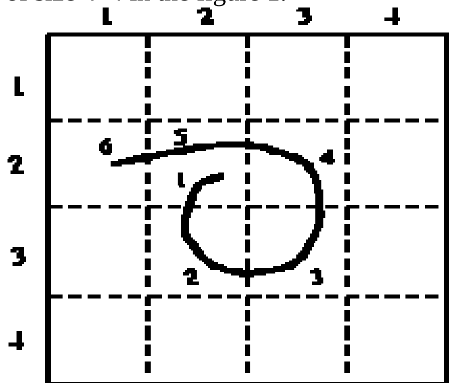

Fig1. A Sample DAS [19]

Here the coordinate sequence generated by this drawing is {(2,2),(3,2),(3,3),(2,3),(2,2),(2,1),(5,5)} where (5,5) is "pen up" indicator. These strokes separated by "pen up" events become password. In order to login successfully, the user has to draw the same pattern.

ii. Grid Selection [8]

J. Thorpe and van Oorschot further studied the impact of stroke-count and password length on the DAS password space. Results suggested that stroke-count and password length both significantly affect the effectiveness of password space but stroke-count has the largest impact on password space as compare to password length. In order to improve the security Thorpe and van Oorschot proposed Grid Selection, which consist two parts: Drawing grid and DAS password [8]. The selection grid is an initially large, fine grained grid from which the user selects a drawing grid, a rectangular region to zoom in on, in which they may enter their password. This would significantly increase the DAS password space [9].

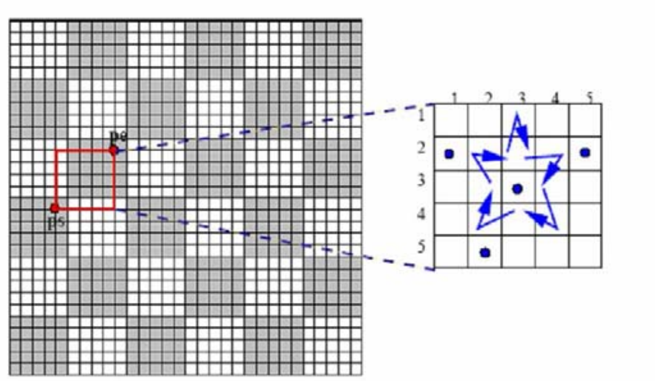

Fig2. Grid Selection Sample [20]

iii. Passdoodle [10]
In Passdoodle the user create a freehand drawing as a password without a visible grid. Then the system scale and stretch the doodle to grid and each time user login, it compare the doodle password with stored user data. Researches proved that Passdoodle passwords are difficult to crack due to a theoretically larger number of possible doodle passwords [10].

Fig3. A Sample Passdoodle [10]

iv. QDAS [11]
Lin et al. [11] presented Qualitative DAS as a variation of DAS by encoding each stroke. In this scheme, a stroke is mapped to its starting cell and the sequence of qualitative direction changes in the stroke relative to the grid. A direction change is considered when the pen cross a cell boundary in a direction different from direction of the previous crossed cell boundary. The user has to remember the starting cell index and direction order of each stroke. QDAS uses dynamic grid transformation in order to reduce shoulder surfing attack. However, this method could not solve the issue in DAS, the drawing did not pass through a crossing point [12].

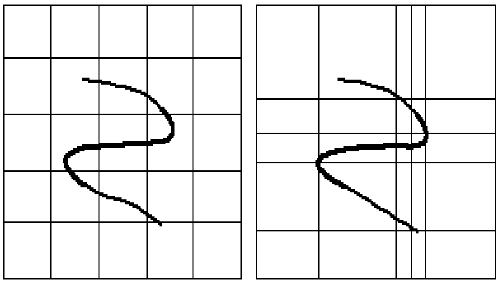

Fig4. A Sample QDAS [11]

v. BDAS [13] Background Draw- A- Secret
Background Draw- A- Secret is an extension to DAS technique proposed by Dunphy and Yan. The idea behind BDAS is to introduce a background image to DAS because drawing grids with background image are helpful in recalling. However they do not mention whether or not user's drawing influenced by the background images.

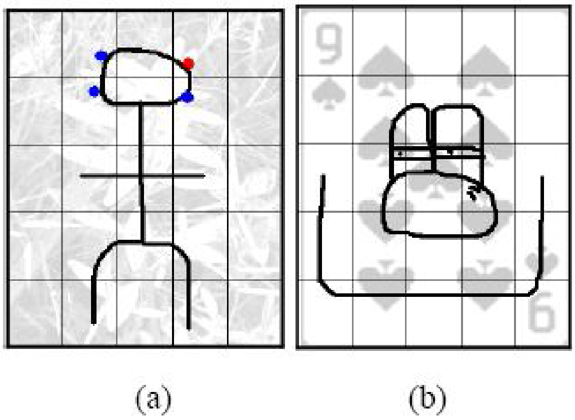

Fig5. A Sample BDAS [13]

B. Locimetric or Click-based Graphical Password Scheme

This scheme is based on loci method [14]. Click-based graphical password scheme requires a user to choose any point or place in the given image as a password click point. Successful authentication requires correct click on sequence of click points in same order as during registration stage.

i. Blonder [21]
This method was designed by Greg E. Blonder in 1996. In this method the user is provided a predetermined image with predefined click regions. For authentication the user click on predefined tag regions in a predetermined sequence. This was the first graphical password scheme that requires the user to click on already designed click regions in provided image. Although this method possess several advantages over alphanumeric passwords but it had its limitations. In this scheme the number of predetermined click regions was relatively small, as a result strong and secure password may require many clicks.

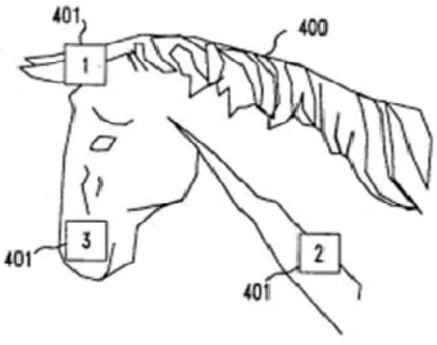

Fig6. A Sample Blonder [21]

ii. PassPoints

PassPoints [15], proposed by Wiedenbeck as an extension of Blonder's algorithm in 2005 to overcome its image limitation. It eliminates predefined boundaries and in place of artificial images any image can be used. So for password creation the user can click on any place in the image. To log in, the user must click very close (or system specified tolerance area) to the chosen click points in the correct order. Theoretically the password space of PassPoint is large but as compare to alphanumeric passwords, it is more difficult to remember the click points within tolerance in this scheme.

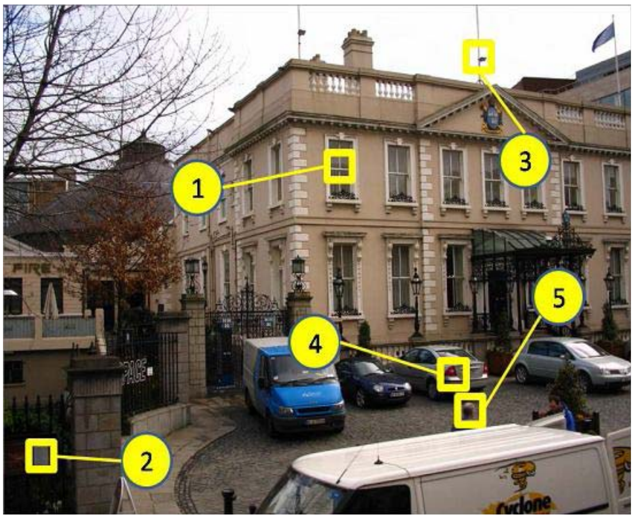

Fig7. A Sample PassPoint [15]

iii. VisKey

VisKey scheme was designed by SFR for mobile devices. It is a commercial version of PassPoints scheme. By focusing on the fact that it is difficult to click on exact spot, Viskey permits the user to define a certain tolerance area.

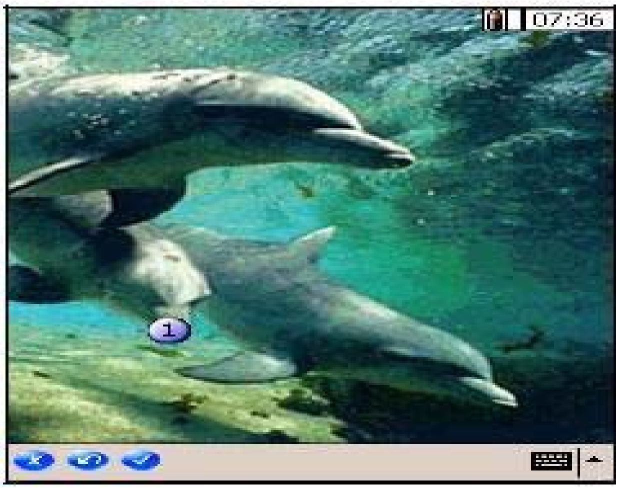

Fig8. A Sample VisKey [22]

iv. Cued Click Points (CCP)

Cued Click Points was designed [16] to reduce pattern and hotspots. In this scheme the user click on one point per image for a sequence of images. The next image is based on the location of the previous click-point. User testing and analysis showed no evidence of patterns in Cued Click-Points, so pattern-based attacks seem ineffective. Although result showed that hotspots remain a problem [17].

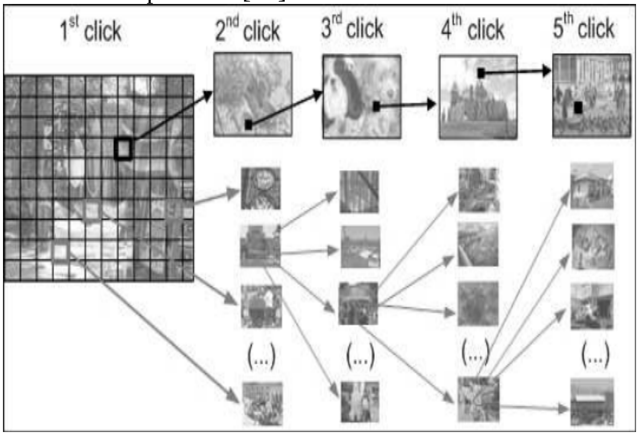

Fig9. A Sample CCP [23]

v. Persuasive Cued Click-Point (PCCP)

Persuasive Cued Click-Points scheme [18] was designed to encourage users to select less probable images as password. The main feature of PCCP is to allow the user to select a click point within the highlighted viewport of image. User is allowed to reposition the viewport until the suitable location is found. During authentication the images are displayed normally without viewport. Although it reduces the hotspot effects but shoulder surfing remain a problem.

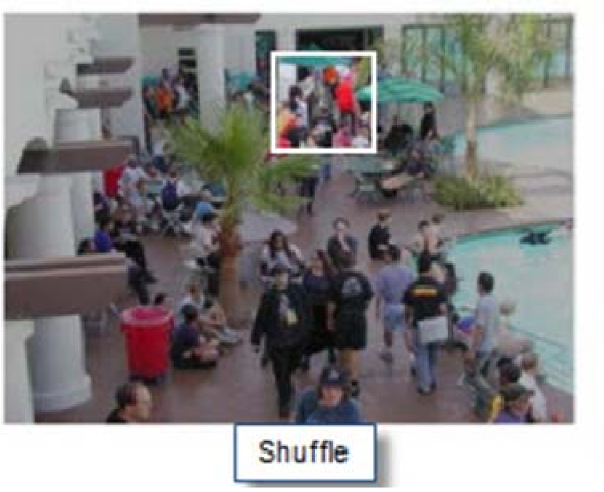

Fig10. A Sample PCCP [24]

III. Comparative Analysis Of Drawmetric And Locimetric Graphical User Authentication Algorithm

Table 1 and Table 2 shows a comparative study of Drawmetric and Locimetric graphical password algorithms respectively. The comparisons are based on their strength, weakness and security attacks.

Table I. COMPARISION of DRAWMETRIC USER AUTHENTICATION ALGORITHMS

S.No.	**Drawmetric Algorithm**	**Strength**	**Weakness**	**Security Attacks**
1	Passdoodle	Harder to crack due to a theoretically much larger number of possible doodle passwords than text passwords	Cannot recall the order of drawing doodle	Guessing, Brute Force
2	Draw A Secret	User can draw a simple image or picture on grid, of any size M*M, harder to crack as compare to Passdoodle	User cannot recall stroke order. Users tend to choose feeble passwords that are vulnerable to graphical dictionary attack.	Description, Brute Force, Spyware
3	Grid Selection	It significantly increases the DAS password space	The weakness of DAS persist	Description, Brute Force, Spyware
4	Qualitative DAS	The image which has more area of interest (Hot Spot) could be more useful as a background image	More entropy but less memorable than previous DAS	Description, Brute Force, Spyware, Guessing
5	Background DAS	Background image enhances memorability of the more complex and secure passwords.	Memory decaying over a week.	Description, Brute Force, Spyware, Guessing

Table II. COMPARISION of LOCIMETRIC USER AUTHENTICATION ALGORITHMS

S.No.	Locimetric Algorithm	Strength	Weakness	Security Attacks
1	Blonder	The method is secure according to a millions of different click regions	The password had to be quite long to be secure	Shoulder Surfing, Brute Force, Guessing
2	PassPoints	The user is choosing several points on picture in a particular order	Longer login time than alphanumerical method	Shoulder Surfing, Brute Force, Guessing
3	VisKey	Resolve the issue of difficulty in pointing to the exact spots.	Input tolerance/ Precision	Description, Dictionary
4	Cued Click Point	Message of authentication failure is displayed after the final click-point, to protect against incremental guessing attacks	False accept and false reject	Shoulder Surfing, Guessing
5	Pursuasive Cued Click-Point	Motivate and influence users to select more random passwords that are less likely to include hotspots	PCCP can be broken by capturing input sequence	Shoulder Surfing, Description

IV. DISCUSSION OF RESULTS

For the recall-based algorithms, the most common drawbacks were the difficulty to remember the sequence of authentication required to be authenticated. Hence most users tend to use weak images as passwords. Therefore “Guessing and Brute force” attacks are possible. The recall-based algorithms are most resistant to “Shoulder-Surfing and Dictionary” attacks.

For click-based algorithms, the most common drawback is hotspot problem. To overcome this issue, users were trained to choose strong image as password in PCCP. The most security attacks on click-based algorithms are Shoulder-Surfing and Guessing.

V. CONCLUSION

The main reason for using graphical password is they are more secure and can be recalled easily. In this paper we analyzed five drawmetric and Locimetric graphical password user authentication schemes based on their strengths, weaknesses and security attacks. The review shows that the current graphical password techniques are not mature enough to address the usability and security features together. Much more researches are needed for graphical password user authentication techniques in order to be more useful.

REFERENCES

[1] Kirkpatrick, E. A. (1894). An experimental study of memory. *Psychological Review*, *1*(6), 602.

[2] Madigan, S. (2014). Picture memory. *Imagery, memory and cognition*, 65-89.

[3] Paivio, A., Rogers, T. B., &Smythe, P. C. (1968). Why are pictures easier to recall than words?. *Psychonomic Science*, *11*(4), 137-138.

[4] Shepard, R. N. (1967). Recognition memory for words, sentences, and pictures.*Journal of verbal Learning and verbal Behavior*, *6*(1), 156-163.

[5] Feldmeier, D. C., &Karn, P. R. (1990, January). Unix password security-ten years later. In *Advances in Cryptology—CRYPTO’89 Proceedings* (pp. 44-63). Springer New York.

[6] Shepard, R. N. (1967). Recognition memory for words, sentences, and pictures.*Journal of verbal Learning and verbal Behavior*, *6*(1), 156-163.

[7] Jermyn, I., Mayer, A. J., Monrose, F., Reiter, M. K., & Rubin, A. D. (1999, August). The Design and Analysis of Graphical Passwords.In *Usenix Security*.

[8] Thorpe, J., & Van Oorschot, P. (2004, December). Towards secure design choices for implementing graphical passwords.In *Computer Security Applications Conference, 2004. 20th Annual* (pp. 50-60). IEEE.

[9] Lashkari, A. H., Saleh, D., Farmand, S., Zakaria, D., & Bin, O. (2010). A Wide range Survey on Recall Based Graphical User Authentications Algorithms Based on ISO and Attack Patterns. *arXiv preprint arXiv:1001.1962*.

[10] Varenhorst, C., Kleek, M. V., & Rudolph, L. (2004).Passdoodles: A lightweight authentication method. *Research Science Institute*.

[11] Lin, D., Dunphy, P., Olivier, P., & Yan, J. (2007, July). Graphical passwords & qualitative spatial relations.In *Proceedings of the 3rd symposium on Usable privacy and security* (pp. 161-162).ACM.

[12] Gao, H., Jia, W., Ye, F., & Ma, L. (2013). A survey on the use of graphical passwords in security. *Journal of software*, *8*(7), 1678-1698.

[13] Dunphy, P., & Yan, J. (2007, October). Do background images improve Draw a Secret graphical passwords?.In *Proceedings of the 14th ACM conference on Computer and communications security* (pp. 36-47).ACM.

[14] Higbee, K. L. (1977). *Your memory: How it works and how to improve it*. Englewood Cliffs, NJ: Prentice-Hall.

[15] Wiedenbeck, S., Waters, J., Birget, J. C., Brodskiy, A., &Memon, N. (2005). PassPoints: Design and longitudinal evaluation of a graphical password system.*International Journal of Human-Computer Studies*, *63*(1), 102-127.

[16] Chiasson, S., Forget, A., Biddle, R., & van Oorschot, P. C. (2008, September). Influencing users towards better passwords: persuasive cued click-points

. In*Proceedings of the 22nd British HCI Group Annual Conference on People and Computers: Culture, Creativity, Interaction-Volume 1* (pp. 121-130). British Computer Society.

[17] Dhapade, M. S. L. (2013, June). Implementation of Persuasive Cued Click-Points Techniques for Folder Security using Secure Hash Algorithm.In*International Journal of Engineering Research and Technology* (Vol. 2, No. 6 (June-2013)).ESRSA Publications.

[18] Chiasson, S., Forget, A., Biddle, R., & van Oorschot, P. C. (2008, September). Influencing users towards better passwords: persuasive cued click-points.In*Proceedings of the 22nd British HCI Group Annual Conference on People and Computers: Culture, Creativity, Interaction-Volume 1* (pp. 121-130). British Computer Society.

[19]https://www.usenix.org/legacy/events/sec99/full_papers/jermyn/jermyn_html/img31.gif

[20]http://lib.znate.ru/pars_docs/refs/58/57351/57351_html_6d4aa969.gif

[21] Blonder, G. E. (1996). *U.S. Patent No. 5,559,961*. Washington, DC: U.S. Patent and Trademark Office.

[22] Ugochukwu, E. E. K., &Jusoh, Y. Y. (2013). A review on the graphical user authentication algorithm: recognition-based and recall-based. *International Journal of Information Processing and Management*, *4*(3), 238-252.

[23] Chiasson, S., van Oorschot, P. C., & Biddle, R. (2007). Graphical password authentication using cued click points. In *Computer Security–ESORICS 2007*(pp. 359-374).Springer Berlin Heidelberg.

[24]http://hotsoft.carleton.ca/~sonia/content/pro_pccp_screenshot_sm.jpg