Proc. of the Intl. Conf. on Advances In Information Processing And Communication Technology - IPCT 2014.

ISBN: 978-1-63248-021-7 doi: 10.15224/ 978-1-63248-021-7-71

Pass-Coob a New Graphical Password Based on Colors and Objects

Ahmad Z. El-Rufai, Arash Habibi Lashkari

***Abstract*—Text-based password is commonly used in user authentication. Due to its complexity, users are having trouble remembering their password combination. An alternative was introduced by Blonder in 1996, called graphical password which was easier to remember because of its graphical content. Therefore usability and memorability are improved. In this paper, we propose and develop a new graphical password called Pass-Coob (Pass color and object), which uses colors and object to authenticate user for improving the security and usability aspects.**

***Keywords*— Graphical password, colors, objects, recognition-based schemes, pure recall-based schemes, cued recall-based schemes**

I. Introduction

In a world where information and data integrity, confidentiality and authenticity must be preserved, a password scheme has to be implemented to achieve that. Text-based passwords are commonly used for user authentication [1]. However this type of authentication scheme has its drawbacks, in a case where the password is short it is made easier for attackers to attack, long and complicated password on the other hand increases the strength of the password, but is difficult to remember sometimes.

Greg Blonder introduces the first graphical password back in 1996. During registration a user clicks on multiple points on an image to create a password. During login user must click on those points that were previously selected at the time of registration or close to those points [8]. Many more graphical passwords have been proposed since Blonder, most of which are not optimal in terms of security and usability. Shoulder surfing has been the ultimate issue in security. Shoulder surfing is a type of attack where the attacker watches over the shoulder of a user during login to capture the user's password.

Ahmad Z. El-Rufai / LUCT
Postgraduate Center of Studies (PGC),
Limkokwing University of creative technology (LUCT), Malaysia

Arash Habibi Lashkari / LUCT
Postgraduate Center of Studies (PGC),
Limkokwing University of creative technology (LUCT), Malaysia

II. Literature Review

Graphical password is categorized into two; recognition-based technique and recall-based technique. In recognition-based, at the time of registration user selects a set of images as password, during login user is required to identify and recognize the same set of images selected previously in order to be authenticated. Recall-based technique is furthermore categorized into two; pure recall-based and cued recall-based. In pure recall the user is required to recall the process generated earlier at the time of registration without any hint given. In cued recall user is provided with some hint to assist in recalling the previously generated password created during registration [1, 9].

In 2010 Michael et al. proposed a graphical password scheme with three stages. In the first stage user chooses click points in a provided image as password, secondly the user needs to confirm the password by re-entering their click points. If they make an error they can clear and re-enter other click points. Thirdly the login stage, during which the user clicks close to the previously chosen click points in the provided image [2]. Figure 1 shows the steps.

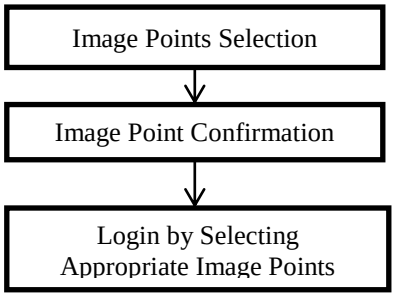

Figure 1. Steps to Create a Graphical Password

In 2011 Martin et al. developed a prototype of graphical authentication called ImagePass that uses the concept of recognition-based graphical password. Here the user enters a graphical password by clicking on a series of images representing objects. During login user is presented with the objects selected previously with additional objects as decoy. If both the sequence and the clicked objects are correct the user is allowed access [3]. Shuiab and Sobin proposed an alternative to PassPoint called Cued Click Points (CCP), which allows user to click on point in a series of 5 images rather than 5 points on a single image. The system alerts a valid user when they make a mistake while entering their latest click-point, giving the user a chance to cancel and retry from beginning [4].

Proc. of the Intl. Conf. on Advances In Information Processing And Communication Technology - IPCT 2014.

ISBN: 978-1-63248-021-7 doi: 10.15224/ 978-1-63248-021-7-71

In 2000 Dhamija and Perrig proposed a new graphical authentication scheme called Déjà vu algorithm. During registration, user will choose a certain number of images from a collection of random non-describable abstract pictures. During login the user is required to recognize and identify the images he/she selected earlier during registration in order to be authenticated. The average registration and login time of this approach is much longer than the traditional text-based approach [1, 10].

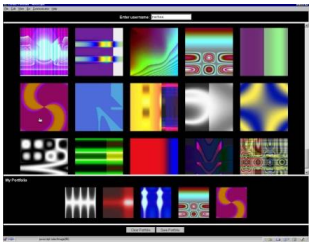

Figure 2. An Example of the Déjà Vu Algorithm

In 2002 Sobrado and Birget developed a new graphical password scheme called Triangle algorithm which is designed to handle the shoulder surfing problem. During registration phase user choose a number of pass objects from 1000 proposed objects. At login the system displays a variety of objects on the screen, and the user will click inside the area that the previously selected objects form. The procedure is repeated several times, each time the objects will be repositioned on the screen. The disadvantage of this approach is a very crowded display and user will find it difficult to identify the objects easily [1].

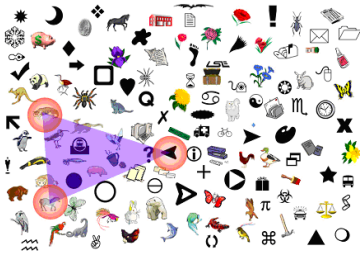

Figure 3. An Example of the Triangle Algorithm

In 2000 Brostoff and Sasse proposed a new graphical authentication scheme that is called Passface algorithm. During registration a user will choose a number of images of human faces from the picture database. To authenticate, user is required to identify previously chosen faces in order to be authenticated. The user recognizes and clicks the known faces and the step is repeated several times [1].

Figure 4. An Example of the Passface Algorithm

In 2008, Eiji Hayashi et al proposed a new graphical authentication scheme called use your illusion (UYI). Their proposed system consists of three phases: portfolio creation, practice and authentication. During the portfolio creation user is required to create a set p images that they want use for authentication. Once the images are created and transfer to the authentication device, they are distorted. The purpose of distorting the images is to make it difficult for attackers to attack. The resulting set of p distorted images is now the user's portfolio. Both the original and distorted images are shown to the user simultaneously so that user can mentally associate the two images. At the practice phase, a set portfolio images and decoy is presented to the user so that user can practice and the system provides immediate feedback on whether the selection is correct or wrong. During the authentication phase the user must correctly select their p portfolio images from the set. Decoy images are produced using original images, and the distortion levels are high enough that most details of the original images are obscured [18].

Figure 5. An Example of Use Your Illusion (UYI)

In 2012 Alia et al. proposed a new graphical password that is based on basic shapes. At registration phase user selects a number of shapes that are shown in the standard shape bar, user is required to select a minimum of five shapes and form his/her password. During authentication the user is required to draw the previously drawn shapes in order to be authenticated [4, 6].

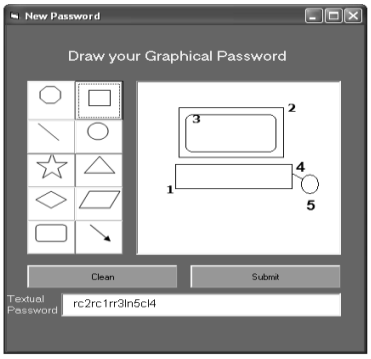

Figure 6. An Example of the Alia et al. algorithm

In 2013 Sriram and Swetha proposed a new graphical password scheme, for traditional desktop, smart phones and other web applications. In their proposed system user will enter his/her desired username and an alphanumeric password. Then the user will be shown a 6 by 6 grid where the user will assume an imaginary pattern line across the randomly colored squares and enter the character in the squares through which his pattern line passes. To login user will inter his/her

Proc. of the Intl. Conf. on Advances In Information Processing And Communication Technology - IPCT 2014.

ISBN: 978-1-63248-021-7 doi: 10.15224/ 978-1-63248-021-7-71

username, then enter the first letter of the color of the squares in which the password letters lie [5].

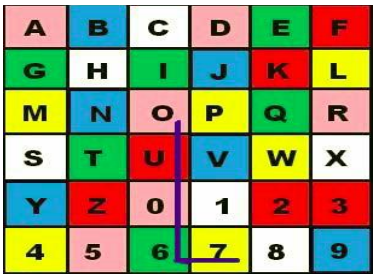

Figure 7. An Example of the Pattern Line

In 2014 Moraskar et al. proposed a new graphical password that is based on cued click point. The system consists of three modules; user registration module, picture selection module and system login module. During registration user enters the username and other details which will be saved in the database to be used during login for verification. In picture selection module pictures are selected by the user from the hard disk or any other image supported devices. Then pictures are selected by the user from the database of the password system. In picture selection phase user select any image as password and consist of a sequence of five click-points on a given image and proceed to next image. During login phase, images are displayed normally without shading or viewport, user repeat the sequence of clicks as previous in the correct order, within a system-defined tolerance square of original click-points [6].

Figure 8. An Example of the Moraskar et al. algorithm

In 2014 Yesseyeya et al. proposed a new graphical user authentication scheme called Tri-Pass. The system based on the two techniques mentioned earlier, PassPoint and Triangle algorithms. To create a password user has to choose one image from the library of pictures and then select any three points by clicking on the image (password point). To login user has to imaging an invisible triangle around the area of the first "password point" and click on any three points that will form a triangle. User will do the same for the second and third "password point" [1, 10].

Figure 9. An Example of the Tri-Pass Algorithm

III. SECURITY

Security is the most important aspect in any user authentication system. There are many ways to attack these systems; unfortunately none of these systems has a perfect security mechanism. Thus schemes must be evaluated according to their vulnerabilities and susceptibility to different attacks [1, 11].

Brute force attack deciphers a password by searching and testing for all possible combinations of alphanumeric characters until it finds the correct key. The most effective way to prevent brute force search attack in some graphical password is to enlarge the password space. Graphical passwords are less vulnerable to brute force search attack than traditional text-based approach at large. However recall-based methods of authentication have tendency of larger password space than recognition-based methods.

Dictionary attack expose a password by running through a possible series of dictionary words that are compiled based on knowledge or assumptions considering the user's typical behavior. Graphical passwords are less vulnerable to dictionary attacks than traditional text-based approach. In recognition-based method, users normally use a mouse for input, so there is no reason to carry out a dictionary attacks against this kind of graphical authentication.

Shoulder surfing attack gain user's password of a user during login by direct observation or external recording devices. Text-based password and most of the graphical password scheme are vulnerable to shoulder attack. Although few some of the recognition-based techniques have resistance to shoulder surfing attack and none of the recall-based techniques are considered to have resistance to shoulder surfing.

Guessing attack is a common problem in both textual and graphical authentication approaches. Because users create a simple and short password, it gives a chance for guessing attack.

Spyware attack is any unauthorized software installed without the user's permission, which collects information about the user's computational behavior by tracking the keyboard input. In general, graphical passwords are less vulnerable to spyware attacks the traditional text-based approach. Graphical password users' uses the mouse for input, so through the mouse motion alone is not enough to break graphical passwords.

Social engineering attack is any method used to gain access to a system under false pretenses by exploiting human

Proc. of the Intl. Conf. on Advances In Information Processing And Communication Technology - IPCT 2014.

ISBN: 978-1-63248-021-7 doi: 10.15224/ 978-1-63248-021-7-71

psychology. Table 1 show that, in general, graphical passwords are less vulnerable to social engineering attacks than traditional text-based approach. It also reduces the possible password revealing because explanation of graphical password in verbal to another person difficult [1, 12, 13, 14, 15].

Table 1: The Attacks Resistance in GP Algorithms

Algorithms		Attacks					
		Brute force	Dictionary	Shoulder surfing	Guessing	Spyware	Social engineering
Recognition -based	Image Points	👎	👎	-	👍	-	👍
	ImagePass	👍	👎	-	👍	-	👍
	Colored Grid	👍	👎	-	👎	-	👍
	Tri-Pass	👍	👍	👍	-	👎	👍
	Déjà vu	👎	-	👎	-	👍	👍
	Triangle	👎	👍	-	👎	👍	-
	Passface	👎	👎	👎	👎	👍	👍
	UYI	👍	👍	-	👍	-	-
	Basic Shapes	👍	-	👍	👎	👍	👎
	Pass-coob	👍	👎	👍	👍	👍	-
Pure recall -based	DAS	👍	👎	👎	👎	👍	👍
	Grid selection	-	-	👎	-	-	👎
	Syukri et al.	👍	👎	👎	-	👍	👍
Cued recall -based	Blonder	👎	👍	👎	👎	👍	👍
	Passlogix v-Go	👎	-	👎	👎	-	-
	Cued Click Point	👍	👎	-	👍	-	👍
	PassPoint	👎	👍	-	👎	-	👍

IV. Proposed algorithm

In our proposed algorithm we try to focus more on security, especially the shoulder surfing attack. There are two phases to this system; (A) Registration phase and (B) login phase.

A. *Registration phase*

In this phase user is required to create his/her password by selecting four colors from eight available colors provided by the system and click submit (Figure 9). Next the user will select two objects of which have the same colors as the last two colors selected previously (Figure 10).

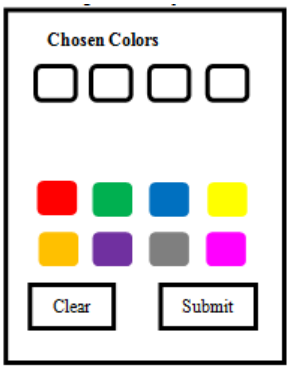

Figure 9: Example of Registration Phase 1of 1

Figure 10: Example of Registration Phase 2 Of 1

B. *Login phase*

In this phase the system displays sixteen different colors, eight from the registration phase and other eights colors as decoy (Figure 11). User can login by selecting the previously selected colors and click submit, and then select the two objects previously selected during registration. If both the colors and sequence of selection is correct, then user is allowed access into the system (Figure 12).

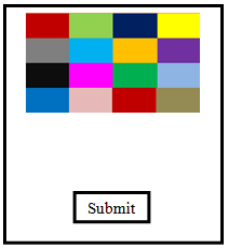

Figure 11: Example of Login Phase 1 Of 2

Figure 12: Example of Login Phase 2 Of 2

ISBN: 978-1-63248-021-7 doi: 10.15224/ 978-1-63248-021-7-71

v. Conclusion

We have reviewed eight different algorithms on recognition-based, pure recall-based and cued recall-based methods. We studied the usability problems of graphical password including six common attacks as shown in Table 1, most of the graphical password scheme are vulnerable to brute force search attack, shoulder surfing and guessing attacks. Our research shows that usability and security of an authentication scheme is of a primary importance. We proposed a new algorithm for graphical user authentication called Pass-Coob, which uses the combination of colors and objects for authenticating user. Future work should be focused on improving the Pass-Coob algorithm for more efficient graphical user authentication and include exploring more feasibility and usability features, improve the system for better shoulder surfing resistance. More research can be carried out.

ACKNOWLEDGEMENTS

I would like to thank Dr. Arash Habibi Lashkari for his encouragement, supervision, kind advice and great support he has given me. Also we would like to express our appreciation to all respondents who participated in our survey for their valuable contribution.

References

[1] E. Yesseyeva, K. Yesseyeva, M.M. Abdulrazaq, A. H. Lashkari, and M. Sadeghi (2014), "Tri-Pass: a new graphical user authentication scheme", International Journal of Circuits, Systems and Signal Processing, Vol 8, P:61-67

[2] M. Kimwele, W. Mwangi, and S Kimani (2010), “Strength of a colored graphical password scheme”, International Journal of Reviews in Computing

[3] M. Mihajlov, B J. Blazic, and M. Ilievski (2011), “ImagePass-Designing Graphical Authentication for Security”, 27th International Conference on Next Generation Web Services Practices

[4] M A. Alia, A A. Hnaif, H K. Al-Anie, and A A. Tamimi (2012) , “Graphical Password Based On Standard Shapes”, Science Series Data Report Vol. 4, No. 2; Feb 2012

[5] P.V.V Sriram and G.Sri Swetha (2013), “A Novel 2 Step Random Colored Grid Graphical Password Authentication System”, International Journal of Computer Science & Engineering Technology (IJCSET) ISSN: 2229-3345, Vol. 4 N0. 04 Apr 2013

[6] V. Moraskar, S Jaikaiyani, M Saiyyed, J Gurnani, and K. Pendke (2014), “Cued Click Point Technique for Graphical Password Authentication”, IJCSMC, Vol. 3, Issue 1, January 2014, pg.166-172

[7] Gao, H., Liu, X., Dai, R., Wang, S. and Liu, H. (2009), “Design and Analysis of a Graphical Password Scheme”, Fourth International Conference on Innovative Computing, Information and Control

[8] Blonder, G.E (1996), “Graphical Password”, United States Patent 5,559,961

[9] Thorpe, J. and Oorschot, P. (2004), “Towards Secure Design Choices for Implementing Graphical Passwords”, 20th Annual Computer Security Applications Conference, IEEE

[10] Lashkari, A. H., Towhidi, F., Saleh, R. and Farmand, S. (2009), “A complete comparison on Pure and Cued Recall-Based Graphical User Authentication Algorithms”, Second International Conference on Computer and Electrical Engineering (ICCEE'09)

[11] Sabzevar, A. and Stavrou, A. (2008), “Universal Multi-Factor Authentication Using Graphical Passwords”, IEEE International Conference on Signal Image Technology and Internet Based Systems

[12] Lashkari, A. and Towhidi, F. (2010) Graphical User Authentication (GUA), LAP LAMBERT Academic Publishing, ISBN 978-3843380720, Germany

[13] Lashkari A.H. and Farmand S. (2009), “A survey on usability and security features in graphical user authentication algorithms”, International Journal of Computer Science and Network Security (IJCSNS), VOL.9 No.9, Singapore

[14] Masrom M., Towhidi F., Lashkari A.H. (2009), “Pure and cued recall-based graphical user authentication”, Application of Information and Communication Technologies (AICT)

[15] Lashkari A.H., Saleh R., Farmand F., and Zakaria O.B. (2009), “A Wide range Survey on Recall Based Graphical User Authentications Algorithms Based on ISO and Attack Patterns“, International Journal of Computer Science and Information Security (IJCSIS), Vol. 6, No. 3

[16] Zheng, Z, Liu, X. Yin, L. and Liu, Z. (2010), “A Hybrid Password Authentication Scheme Based on Shape and Text”, Journal of Computers, Vol. 5, No. 5

[17] H. K. Sarohi, F. U. Khan (2013), “Graphical Password Authentication Scheme: Current Status and Key Issues. International Journal of Computer Science Issues, Vol. 10, Issue 2, No 1, March 2013

[18] E. Hayashi, N. Christin, R. Dhamija and A. Perrig, (2008) “Use Your Illusion: Secure Authentication Usable Anywhere”, Proceedings of the 4th symposium on Usable privacy and security (SOUPS '08)