Asian Journal of Information Technology 14 (1): 1-10, 2015
ISSN: 1682-3915
© Medwell Journals, 2015

Graphical Authentication Using Enhanced Hybrid Graphical Authentication System

[1]M.D. Fatehah, [1]Mohd Zalisham Jali, [1]M.K. Wafa and [2]Nor Badrul Anuar
[1]Faculty of Science and Technology, Univesiti Sains Islam Malaysia (USIM),
Negeri Sembilan, Malaysia
[2]Faculty of Computer Science and Information Technology,
University of Malaya (UM), Kuala Lumpur, Malaysia

Abstract: The username/password combination is still the most widely used method albeit various user authentication techniques have been introduced. Numerous studies have been conducted to investigate the scheme and it could be summarized that despite it weaknesses, it is the most favorable scheme. Thus, to reduce the weakness, authenticating users with image or pictures (i.e., graphical password) is prop osed as one possible alternative as it was claimed that pictures were easy to remember, easy to use and has considerable security. This study presents a study carried out to investigate user's performance and feedback towards the use of hybrid graphical methods (i.e., combining two graphical methods) as a method of authentication. Initially, a survey was conducted to identify participants' drawing patterns as their secret using the paper-based method and then the graphical software prototype was developed and tested randomly by 30 participants and lastly a survey was conducted in order to identify the level of guessability (i.e., security perspective). Overall, test on the prototype showed positive results as participants enjoyed using it and able to register within tolerable time.

Key words: User authentication, graphical passwords, choice-based method, draw-based method, usability, security

INTRODUCTION

With more resources (i.e., information and services) are going online, the need for control protection for users to access such resources are critical. It is anticipated that one of many steps to achieve such protection are known as authentication and authorization. Generally, user authentication can be explained as a process of proving who the user is to the resources. While authorization is a process of giving user permission to access or utilize the resources based on their identity.

As time goes on studies have revealed that using long and complex combinations of password can cause problems with ease of use and memorability and using simple passwords resulted in a range of security problems (Morris and Thompson, 1979; Klein, 1990; Bishop and Klein, 1995; Carstens *et al*., 2004). As the consequences, alternative technologies such as the use of token (Perlman and Hanna, 2001), biometric (Clarke and Furnell, 2007), cognitive passwords as well as using sign-on and public key cryptography (Tardo and Alagappan, 1992) are gaining much attention to replace and overcoming problems in the password-based authentication. It is anticipated that each of these technologies has their own weaknesses and strengths.

Thus, observation was made to identify potential alternatives for password-based authentication by which the use of images (known as 'graphical passwords') was found. Different types of images have been used as the authenticators in graphical passwords such as faces (Brostoff and Sasse, 2000), geometric shapes (Lin *et al*., 2008; Alia *et al*., 2012), random arts (Dhamija and Perrig, 2000) and daily seen images (Jali, 2011; Seng *et al*., 2011).

As the root of graphical authentication, many psychological studies have been reported regarding the picture "superiority effects" towards words and verbal (Potter, 1976; Lin *et al*., 2007). Besinger (1998) identified that people can recognize images more steadily than recalling alphanumeric characters because pictures are represented in memory with more details than alphanumeric characters.

Based on Memory Model, graphical authentication can be classified into two; namely recognition-based and recall-based (Fulkar *et al*., 2012). However, based on user tasks, graphical authentication is classified into four main categories; namely click-based, choice-based, draw-based and hybrid based (Jali, 2011). While click-based requires users to click anywhere they prefer in given image, the choice-based method usually requires users to select their chosen image from a set of decoy images. In contrast, the

Corresponding Author: M.D. Fatehah, Faculty of Science and Technology, Univesiti Sains Islam Malaysia (USIM), Negeri Sembilan, Malaysia

draw-based method requires users to draw their secret on the provided grid/screen and the hybrid-based method is a combination of at least two of the aforementioned methods.

Many graphical authentication schemes have been implemented which design by using the choice-based method, draw-based method and also the click-based method. One of the earlier schemes that implemented the click-based method is known as the PassPoint (Wiedenbeck *et al*., 2005). However, from the PassPoint scheme, security analysis found that vulnerable to hotspots and simple geometric pattern within images (Khan *et al*., 2011; Van Oorschot and Thorpe, 2011; Golofit, 2007).

Many studies have been conducted for graphical password designed by using the choice-based method (Fulkar *et al*., 2012). In the study conducted by Thorpe and Van Oorschot (2004), they proposed a graphical password scheme based on choice-based method on PDAs. The problem arose as the password space is small, since the numbers of thumbnail photos are limited to only thirty (shorter than the length of textual password). Contrast with choice-based method, Jermyn *et al*. (1999) proposed a technique based on draw-based method known as Draw-A-Secret (DAS) where users need to draw their secret on a 2-grid using a stylus or mouse. However, previous study suggested that DAS users might tend to pick weak graphical passwords that are vulnerable to the graphical dictionary attack (Thorpe and Van Oorschot, 2004). To improve the DAS scheme, BDAS (Background Draw-A-Secret) was introduced by Dunphy and Yan (2007). BDAS uses background image rather than grid. Users need to draw their secret on a set of given images to create a password. In order to find the differences between DAS scheme and BDAS scheme, two comparative user studies was conducted. As a result, people tended to create more complicated passwords (i.e., increase passwords security and effectiveness) with the background image and by using the background image, users memorability on password also improved. Another enhanced version of DAS is known as QDAS (Qualitative Draw-A-Secret), empirically studied by Lin *et al*. (2007).

A REVIEW ON THE HYBRID GRAPHICAL AUTHENTICATION METHODS

Hybrid graphical method can be best described as an attempt to combine two or more existing graphical methods for better usability and security. As an authentication system, adequate security must be provided for its intended environments; otherwise it fails to meet its primary goal (Biddle *et al*., 2012). Nevertheless, Biddle *et al*. (2012) claimed that there has been essentially no coordinated work or accepted standard to evaluate the usability of graphical passwords. The most important component in assessing the usability of the system is the target users. User's familiarity affects the usability of the system (Towhidi and Masrom, 2009). Examples of hybrid graphical method are Cued-Click Points (CCP) by Chiasson *et al*. (2007), Enhanced Graphical Authentication System (EGAS) by Jali (2011) and Triangle by Sawla *et al*. (2012).

Cued-Click Points (CCP): Chiasson *et al*. (2007) proposed the Cued Click Points (CCP) scheme as an alternative to PassPoint with one click per image. The CCP is developed based on hybrid method as combination of the click-based method and the choice-based method. In CCP, users click one point per image rather than five points per image for all selected images. Only one image will be shown at a time as the click point of the previous image will determine the next image. During login, if users failed to click on the exact point, incorrect images will be displayed onwards. Consequently, it was a disadvantage to attacker if they did not know the sequence of the images. Inspired from CCP scheme, a graphical software prototype known as Enhanced Graphical Authentication System (EGAS; combination of choice-based method and click-based method) was developed by Jali (2011) (Fig. 1).

Enhanced Graphical Authentication System (EGAS): EGAS enhanced CCP with each image is independent with each other. This mean, users have an option to choose their secret images and their preferred number of clicks but still those particular images needs to be controlled by software prototype for security reason. Studies conducted towards EGAS shown that both methods can

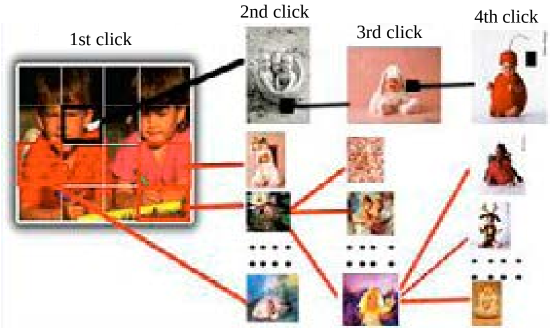


Fig. 1: In CCP, users click on one point per image and the point determine the next image (Swathi and Reddy, 2013)

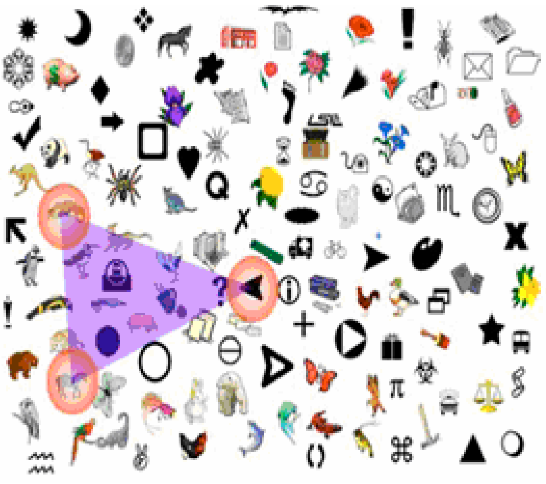


Fig. 2: Triangle scheme (Sawla *et al*., 2012)

be combined effectively (in terms of memorability, clicking accuracy, timing) without significant impediment to users. However, participants tended to choose similar and predictable images and also tended to click on guessable objects (Jali, 2011).

Triangle: Earlier in 2002, a graphical authentication scheme named Triangle which believed can overcome shoulder surfing attack was proposed. As shown in Fig. 2, the scheme randomly put a set of N objects with addition of user's objects (secrets) previously chosen on the screen. For the authentication process user must find three of their secrets and click inside the triangle created from the three objects. Each time user try to login, a different display on N objects will be displayed hence, reduce the probability clicking on the same region each time user challenge to login. Even the scheme could be resistant to shoulder surfing attack, however, the usage of large amount of object make the display look crowded. Using small number of objects somehow turn the password space smaller (Sawla *et al*., 2012).

Other hybrid schemes: Other than the aforementioned schemes, there are many hybrid schemes that have been proposed. Contrast with hybrid graphical password defined by Jali (2011), researchers combined two methods consists of graphical password and textual password. Zheng *et al*. (2010) proposed a scheme based on the Hybrid Graphical Method that the idea is to make a graphical map from shape to text and textual password. The aims were to provide large password space and resistant to shoulder-surfing attack.

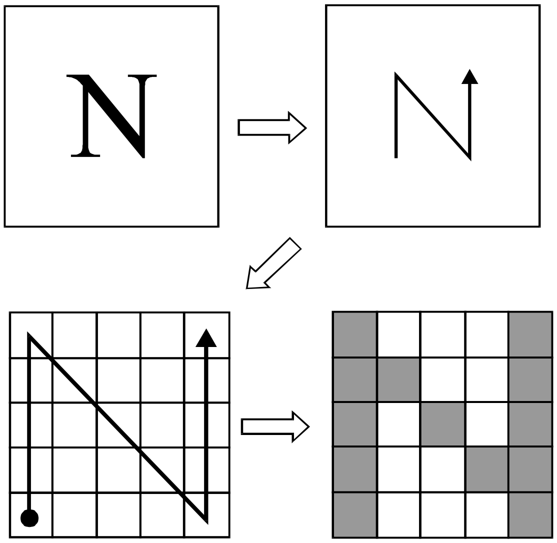
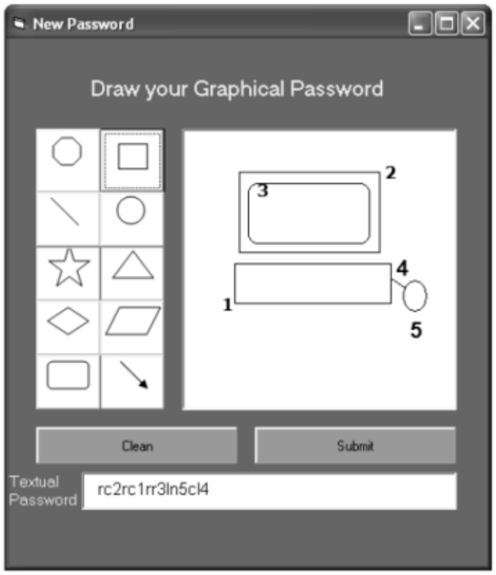


Fig. 3: Hybrid scheme by Zheng *et al*. (2010)

However, the scheme has some weaknesses in terms of familiarity, vulnerability and also the time taken is longer as compared with to other graphical schemes. Alia *et al*. (2012) conducted a study enhancing (Zheng *et al*., 2010) hybrid scheme. Users have to compose the passwords based on ten series of standard shapes as shown in the standard shape bar below. Once the drawing process completed, the textual password will be created according to the drawn shapes and will be displayed in the textual password field as shown above. The scheme proposed was believed as more efficient than others graphical password scheme as it was easy to remember. On the other hand, Khan *et al*. (2011) proposed a scheme for mobile devices which combining textual password and hybrid graphical password (combining choice-based and draw-based method). The scheme was claimed as resistance to shoulder surfing attack and secure from threats (Fig. 3).

ENHANCED HYBRID GRAPHICAL AUTHENTICATION SYSTEM (EHGAS)

In the hybrid graphical scheme, it was found that many studies published so far relate to both click-based and choice based methods with less study reported for the draw based approach. Nevertheless, users' familiarity and usability of the schemes were still the main issues. Motivated with the aforementioned studies and inspired by the BDAS scheme, a study was conducted to enhance the EGAS System and evaluate the role of new and Novel Hybrid Graphical Methods by designing and developing graphical scheme and finally assessing this scheme in terms of usability perspectives. The new hybrid scheme



Textual Password: rc2rc1rr3ln5cl4

Fig. 4: Draw a new password as by Alia *et al*. (2012)

known as Enhanced Hybrid Graphical Authentication System (EHGAS) combines two graphical methods (i.e., choice-based and draw-based method) (Fig. 4).

EHGAS evaluations: The objective of this study is to obtain users' opinion and preference towards the use of Hybrid Graphical Methods (i.e., combining the choice-based and draw-based methods) as the method for authentication. Three evaluations were conducted. Initially, a survey was conducted to investigate and justify participants' secret drawing pattern by then used as the basis for developing the prototype. The EHGAS later tested by participants (i.e., covering both usability and security) in order to evaluate it potential as the alternative user authentication.

Drawing pattern survey

Method: This survey was conducted in order to obtain favorable pattern as a basis to develop the Hybrid Graphical System (combining the choice-based and draw-based method). The images were chosen from the set of most popular images in BDAS study (Dunphy and Yan, 2007). Three images used in the survey are shown in Fig. 5. These images (with 7.95×7.95 cm size) were printed on the A4-sized paper and distributed to participants. Participants were brief about Graphical Password Method and later were asked to draw their secret pattern (using three straight lines) on each of the given images. This activity took approximately, 2-3 min to complete, depending on participants' understanding to complete the task.

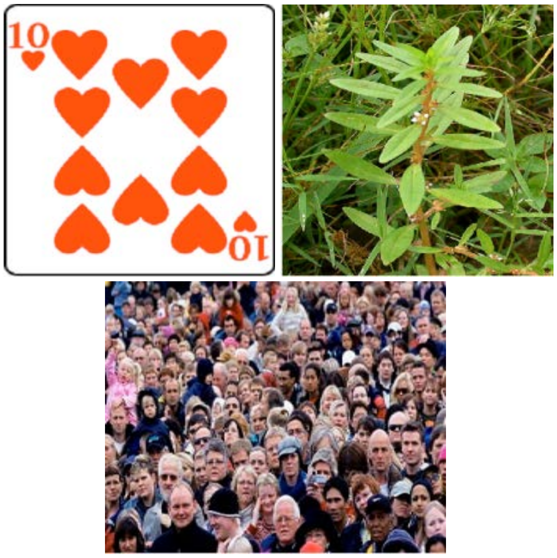


Fig. 5: Image of card, plant and people used by Dunphy and Yan (2007)

Result: A total of hundred students (23 male, 77 female) from students of the Faculty of Science and Technology, USIM participated with the average age of 22 years old. Initially, there exist participants that confused with the instruction given in the questionnaire as some of them had never used any graphical authentication scheme before. However, after some explanations, they managed to complete the task successfully. From the pattern of drawing drawn by participant, it can be related that the drawing shape drawn by participants can be classified into three; namely line, shape and curve. Table 1 shows number of participants for each pattern. From Table 1, it can be seen that the most popular pattern drawn on the images given is the line pattern. Examples of popular pattern drawn on the given images are shown on Fig. 6.

EHGAS-evaluation on the usability

EHGAS prototype: The prototype was developed based on the Hybrid Graphical Method (combining the choice-based and draw-based methods). Basically, the system was developed using Microsoft Visual Basic 2010 with Microsoft Access 2007 used for storage. In contrast with EGAS, the prototype allow user to draw three lines per image rather than one click per image. The image for drawing a secret was displayed at 800×480 pixel resolution replicating the average screen size of the smart phone at the time. By enabling the user to choose one image per theme, it improves the security of the system due to the fact that users' own images were weak and predictable (Tullis and Tedesco, 2005).

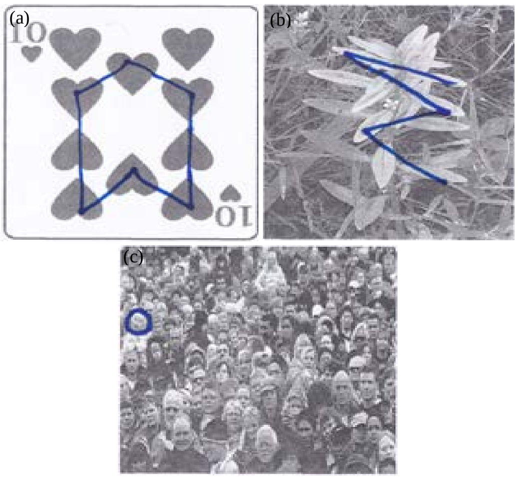


Fig. 6: Popular patterns created by participants on the given images: a) card; b) plant and c) crowd

Table 1: Popular pattern drawing with their associated figure

	Patterns		
Images	Line	Shape	Curve
Card	48	44	8
Plant	40	47	13
People	49	35	16

Two main tasks needed to complete by participants; register and login. In the first module, participants need to register by choosing three images for the choice-based method and later draw pattern on each of the images for the draw-based type. The location of initial and final point for each line in the pattern will take into account. Examples screenshots of the prototype are shown in Fig. 7 and 8.

With the login tasks, users will be prompted to enter username and if validated, users will be given the first image initially chosen in the registration phase. Then, they need to draw the lines with exact sequence before they can proceed with the second image and the third image, respectively. It was predicted that these steps can reduce the time taken for login as challenging the user to identify their secret images within the decoy images assigned by system would take longer time. Challenge with random image is said could provide extra security. Steps each participant needs to undergo when login are illustrated in Fig. 9.

Method: A test was conducted to get users' performance and feedback on the prototype. Participants were asked to use the prototype displayed on a 14 inch laptop screen and a mouse as their input device and then provide feedback. Steps each participant was asked to undertake are creating an account, log into the system and finally answer feedback questionnaire. In detail, there are three images need to be chosen, one from each theme; people, plant and food. Upon completion of the tasks (registration and login), participants were asked to answer

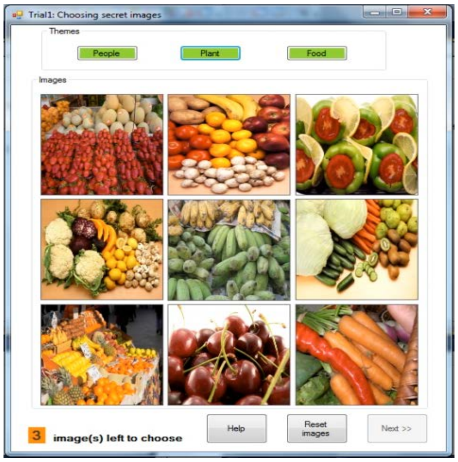


Fig. 7: Screenshot of registration task (image selection)

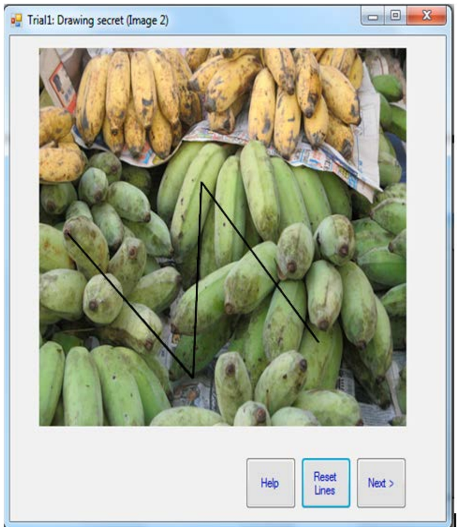


Fig. 8: Screenshot of login task (drawing secret)

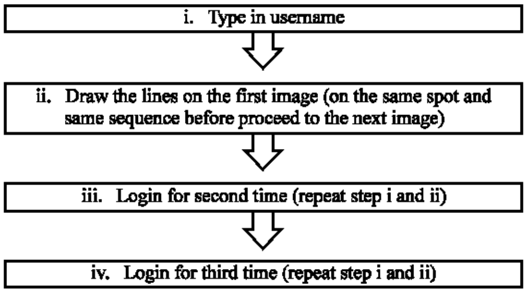

i. Type in username
ii. Draw the lines on the first image (on the same spot and same sequence before proceed to the next image)
iii. Login for second time (repeat step i and ii)
iv. Login for third time (repeat step i and ii)

Fig. 9: Steps needed to follow for login task

feedback questionnaire. Basically, the questionnaire focused on users' feedback, suggestion and familiarity with graphical passwords. The feedback question is based on the questionnaire used in previous study by Jali (2011).

Result: Based on the previous result in the prototype of hybrid graphical authentication was developed. The initial prototype comes with few restrictions where users need to draw on the images with three lines (considering the size of passwords) as result suggested that line shape as the most favorable drawn pattern. Participants need to remember the drawing and the sequence of the point when drawing the line.

Thirty students of Faculty of Science and Technology, USIM participated in this study with the maximum age was 24 years old. All of them were expected to have experienced in using computers >5 years. The following results and analysis will only report on the users' usability performance and feedback. In this study, several points will be discussed (i.e., number of attempts made by participants, time took to create their account, their level of accuracy during both registration and login, identified patterns and also their feedback and suggestions).

Number of attempts: During the test, users' number of registration and login were all recorded. All participants managed to create their account successfully. The 30 usernames were successfully registered in the prototype while 6 more were uncompleted. It was due to participants' unfamiliarity with the graphical authentication and inability to remember the secrets. Furthermore, during confirmation phase, only 11 participants managed to recreate their secrets successfully. Others needed to re-register and after 2 to 3 attempts they managed to register their account completely. From the investigation, it was found that most of the participants were able to complete the registration task after the first failure (i.e., they needed only 2 attempts to complete the registration once familiar with the method).

In the login phase, 26 of the participants successfully completed their login task with only single attempt due to familiarity with the technique during registration tasks. Whereas 4 were unable to complete the task at the first time and needed second attempt as they cannot remember location of the secrets correctly (Table 2).

Table 2: Number of attempts for registration and login tasks

	Number of attempts		
Tasks	1	2	3
Registration	11	17	2
Login	26	4	0

Table 3: Registration, confirmation and login time

	Tasks		
Time	Registration	Confirmation	Login
Shortest	1 min 48 sec	18 sec	20 sec
Longest	5 min 32 sce	1 min 10 sec	56 sec
Mean	2 min 53 sec	41 sec	34 sec

Timing: Participants' performances when using the software prototype was determined based on their time taken during the registration, confirmation and login tasks. The time for participants completing the registration task was taken from the moment they keyed in the usernames until they successfully finish the confirmation tasks. Confirmation task was part of the registration task where the time is measured when participant start drawing the secrets on the first image until finished the last drawing on the last image. While for the login task, the time is taken once the participant entered the username until successfully finish the last drawing (the last secret). Results are shown in Table 3.

From the Table 3, it can be seen that the time taken is decreasing throughout the tasks (from the registration task until the login time). The mean shows that during registration, participants took longest time compared to the login times. This is considering the time taken to choose secret images and also since participants still unfamiliar with the method and how the prototype work. Looking at the login mean times, it can be suggested that once participants were familiar with the methods of prototype, only a short time is needed to finish up the task (i.e., login). Even though, the registration time is surpassing the usual traditional authentication time, it can be accepted since participants needed to undergo series of task that were unusual to them (i.e., image selection, drawing secrets on the images).

Drawing accuracy: For the drawing accuracy, the initial and the end points of each single line of the secrets and the sequence of the line drawn were taken into account. From study, it can be seen that participants managed to draw the line with the initial and the end points of the lines have been drawn within 0-6 pixels of the originals (difference between the original point and point taken during login).

Figure 10 shows the difference in number of pixels between the original secrets (drawn during registration) with secrets that have been drawn during the login tasks (i.e., differences between the initial point and the end points of the lines drawn during registration and during login). The totals of 540 points were recorded (6 points×3 images×30 participants) within a single task

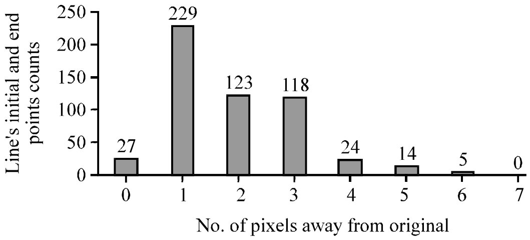


Fig. 10: Frequency of accuracy

(e.g., registration and login). From the results, it can be concluded that most of the secrets were drawn within 1×1 pixels away from the original initial and end points. Fortunately, only several were drawn between 6×6 pixels from the original points. It can be suggested that participants were accurate within 6×6 pixels (note that the study use a tolerance of 7×7 pixels). The results eventually support results in previous study (Jali *et al*., 2011).

Pattern: In this study, user preferences on images' types and drawing shapes will be discussed profusely. Steps taken to investigate users' image selection are similar to those applied by Jali (2011):

- The most popular image for each theme is determined and its frequency is calculated
- Identify participants' drawing areas towards popular images
- Determine and investigate the drawing patterns and hotspot occurrences

Images used in the prototype were divided into three themes; namely people, food and plant. Figure 11-13 show results of the most popular image and their frequency for each theme. Further, investigations towards the result found that participants tended to choose image with more obvious points. It is anticipated since participants need to remember the start and end points of each line when drawing the secret, image with clickable points were preferable.

Users' feedback

General observations: Twenty eight out of 30 participants agreed that they could remember well the images chosen in the choice-based method during the authentication task. Furthermore, half of them preferred images with pointy objects (e.g., stars, pencils, houses and trees). Besides, 21 of them felt secured with the use of images in authentication. Contrary with the previous result, 20 of the participants found that it was hard to remember the

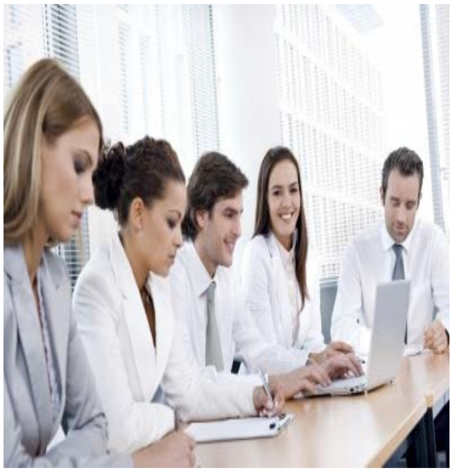


Fig. 11: Image popular for people theme (12 participants)

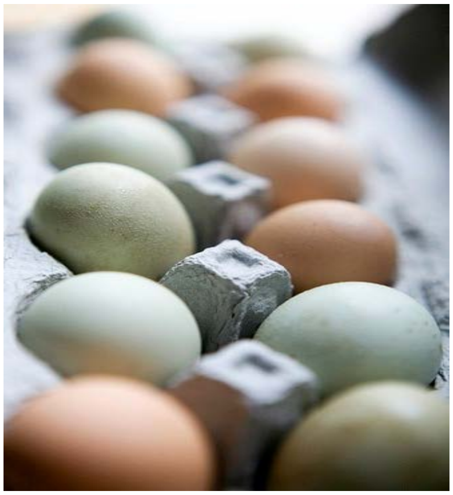


Fig. 12: Image popular for food theme (8 participants)

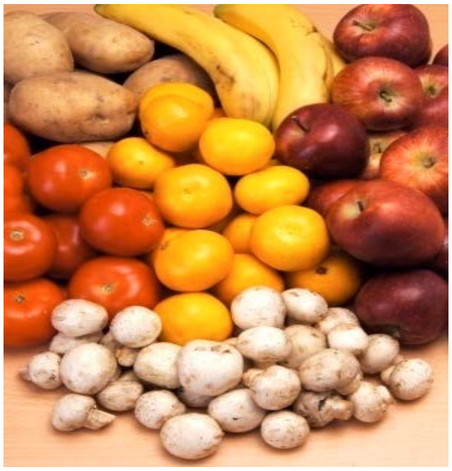


Fig. 13: Image popular for plant theme (9 participants)

secret drawing in the draw-based method at the first time. However, 25 of them felt that it were quite easy to draw the secret after familiar with the method.

User comments:

- "I recommend reducing number of images. Too many to remember" (user A)
- "At first, I was a bit confused. But once familiar, I managed to do it faster" (user B)
- "I prefer images with more obvious point so that it is easy for me to draw the lines" (user C)
- "There is no hint if someone forgot his password" (user D)

The feedback above reflected participants' positive and negative responds towards the EHGAS scheme. User A and D give a suggestion and comment that may help improved EHGAS scheme. However, it is obvious that user C tend to draw on easily guessed points which may create patterns. Nevertheless, the suggestion can be taken into account meanwhile a level of control system is needed.

EHGAS scheme: Overall, participants felt that EHGAS scheme was quite applicable, although, there are flaws in the prototype which can be improved. Most of them preferred easy images (images with more points to be drawn on) and suggested providing hint for those who forgot their passwords.

EHGAS-security evaluation

Method: Studies have found that most of the graphical authentication schemes are vulnerable to hotspots, simple geometric pattern within images and leaks from other verifiers (Khan *et al.*, 2011; Klein, 1990; Potter, 1976). Thus, a survey was conducted in order to identify EHGAS level of security particularly in terms of guessability (i.e., ability to guess the passwords). A group of popular images (3 images) identified from EHGAS usability study were printed on the A4 paper. First of all, participants were briefed on the tasks they needed to undergo during the study. Participants were asked to guess the password created by drawing three lines on each image. Figure 11-13 show the images used in this evaluation.

Result: There were 10 participants participated. Results indicate that most of them tended to draw on the obvious and around the same point drawn in the aforementioned study. But none of them managed to draw the secrets with exact sequences and shapes drawn by the participants in the usability evaluation. Hence, it can be suggested that the use of three lines to draw the secret with different three themes (randomly challenged) of images help to reduce the guessability and improve the security of the scheme.

CONCLUSION

This study presented a study to investigate and evaluate the usability of new graphical method known as EHGAS. The EHGAS inspired from the EGAS and BDAS schemes and are based on the methods of draw-based and choice-based. From the collected data, it can be reported that participants took long time to log into the prototype due to the type of device used to draw the secrets and number of images used as secrets. However, the time taken for login is shorter compared to the confirmation time taken. Thus, this finding reflects participants' familiarity with the software prototype as they used it regularly.

Finally, the results have shown that most of the participants managed to draw their secrets on the exact sequence and with fewer failed attempts. Overall, it was suggested that number of images is reduced even though, the memorability was maintained. Furthermore, since the number of participants is small, it was suggested that the number of participants and average age of participants are increased as it may reflects the results of the study. In the near future, researchers plan to extend this study with participants mainly from the primary school students and to perform the test on mobile platform.

ACKNOWLEDGEMENTS

Researchers of the study wish to thank all participants who participated in the study. This project is funded by USIM under the grant code of PPP/FST/SKTS30/13612.

REFERENCES

Alia, M.A., A.A. Hnaif, H.K. Al-Anie and A.A. Tamimi, 2012. Graphical password based on standard shapes. Sci. Ser. Data Rep., 4: 71-79.

Besinger, D., 1998. Human memory and the graphical password. Passlogix White Paper, Passlogix Inc., pp: 2.

Biddle, R., S. Chiasson and P.C. Van Oorschot, 2012. Graphical passwords: Learning from the first twelve years. ACM Comput. Surv. (CSUR), Vol. 44. 10.1145/2333112.2333114.

Bishop, M. and D.V. Klein, 1995. Improving system security via proactive password checking. Comput. Secur., 14: 233-249.

Brostoff, S. and M.A. Sasse, 2000. Are Passfaces More Usable than Passwords? A Field Trial Investigation. In: People and Computers XIV-Usability or Else, McDonald, S., Y. Waern and G. Cockton (Eds.). Springer, London, UK., ISBN-13: 978-1-85233-318-8, pp: 405-424.

Carstens, D.S., P.R. McCauley-Bell, L.C. Malone and R.F. DeMara, 2004. Evaluation of the human impact of password authentication practices on information security. Inform. Sci.: Int. J. Emerg. Transdiscipline, 7: 67-85.

Chiasson, S., P.C. van Oorschot and R. Biddle, 2007. Graphical Password Authentication Using Cued Click Points. In: Research in Computer Security, Biskup, J. and J. Lopez (Eds.). Springer, Berlin, Germany, pp: 359-374.

Clarke, N.L. and S.M. Furnell, 2007. Advanced user authentication for mobile devices. Comput. Secur., 26: 109-119.

Dhamija, R. and A. Perrig, 2000. Deja Vu: A user study using images for authentication. Proceedings of the 9th USENIX Security Symposium, August 14-17, 2000, Denver, Colorado, USA., pp: 45-58.

Dunphy, P. and J. Yan, 2007. Do background images improve Draw a Secret graphical passwords? Proceedings of the 14th Conference on Computer and Communications Security, October 29-November 2, 2007, Alexandria, VA., USA., pp: 36-47.

Fulkar, A., S. Sawla, Z. Khan and S. Solanki, 2012. A study of graphical passwords and various graphical password authentication schemes. World Res. J. Hum. Comput. Interact., 1: 4-8.

Golofit, K., 2007. Click passwords under investigation. Proceedings of the 12th European Symposium on Research in Computer Security, September 24-26, 2007, Dresden, Germany, pp: 343-358.

Jali, M.Z., 2011. A study of graphical alternatives for user authentication. Ph.D. Thesis, School of Computing and Mathematics, Plymouth University, UK.

Jali, M.Z., S. Furnell and P. Dowland, 2011. Quantifying the effect of graphical password guidelines for better security. In: Future Challenges in Security and Privacy for Academia and Industry, Camenisch, J. S. Fischer-Hubner, Y. Murayama, A. Portmann and C. Rieder (Eds.). Springer, Berlin, Germany, ISBN-13: 978-3-642-21423-3, pp: 80-91.

Jermyn, I., A.J. Mayer, F. Monrose, M.K. Reiter and A.D. Rubin, 1999. The design and analysis of graphical passwords. Proceedings of the 8th USENIX Security Symposium, August 23-26, 1999, Washington, DC., USA., pp: 1-15.

Khan, W.Z., Y. Xiang, M.Y. Aalsalem and Q. Arshad, 2011. A hybrid graphical password based system. Proceedings of the 11th International Conference on Algorithms and Architectures for Parallel Processing, October 24-26, 2011, Melbourne, Australia, pp: 153-164.

Klein, D.V., 1990. Foiling the cracker: A survey of and improvements to, password security. Proceedings of the 2nd USENIX Security Workshop, August 27-28, 1990, Portland, OR., USA., pp: 5-14.

Lin, D., P. Dunphy, P. Olivier and J. Yan, 2007. Graphical passwords and qualitative spatial relations. Proceedings of the 3rd Symposium on Usable Privacy and Security, July 18-20, 2007, Pittsburgh, PA., USA., pp: 161-162.

Lin, P.L., L.T. Weng and P.W. Huang, 2008. Graphical passwords using images with random tracks of geometric shapes. Proceedings of the Congress on Image and Signal Processing, Volume 3, May 27-30, 2008, Sanya, China, pp: 27-31.

Morris, R. and K. Thompson, 1979. Password security: A case history. Commun. ACM, 22: 594-597.

Perlman, R.J. and S.R. Hanna, 2001. Methods and systems for establishing a shared secret using an authentication token. U.S. Patent No. US6173400 B1. http://www.google.com/patents/US6173400.

Potter, M.C., 1976. Short-term conceptual memory for pictures. J. Exp. Psychol.: Hum. Learn. Memory, 2: 509-522.

Sawla, S., A. Fulkar, Z. Khan and S. Solanki, 2012. Graphical password authentication system in an implicit manner. Int. J. Cryptogr. Secur., 2: 27-31.

Seng, W.C., Y.K. Khuen and N.L. Shing, 2011. Enhanced graphical password by using dynamic block-style scheme. Proceedings of the International Conference on Information and Intelligent Computing, (ICIIC'11), Singapore, pp: 139-145.

Swathi, M. and M.J. Reddy, 2013. Authentication using persuasive cued click points. Int. J. Eng. Res. Technol., Vol. 2.

Tardo, J.J. and K. Alagappan, 1992. SPX: Global authentication using public key certificates. J. Comput. Secur., 1: 295-316.

Thorpe, J. and P.C. Van Oorschot, 2004. Graphical dictionaries and the memorable space of graphical passwords. Proceedings of the 13th USENIX Security Symposium, August 9-13, 2004, San Diego, CA., USA., pp: 135-150.

Towhidi, F. and M. Masrom, 2009. A survey on recognition based graphical user authentication algorithms. Int. J. Comput. Sci. Inform. Secur., 6: 119-127.

Tullis, T.S. and D.P. Tedesco, 2005. Using personal photos as pictorial passwords. Proceedings of the Extended Abstracts on Human Factors in Computing Systems, April 2-7, 2005, Portland, OR., USA., pp: 1841-1844.

Van Oorschot, P.C. and J. Thorpe, 2011. Exploiting predictability in click-based graphical passwords. J. Comput. Secur., 19: 669-702.

Wiedenbeck, S., J. Waters, J.C. Birget, A. Brodskiy and N. Memon, 2005. PassPoints: Design and longitudinal evaluation of a graphical password system. Int. J. Hum. Comput. Stud., 63: 102-127.

Zheng, Z., X. Liu, L. Yin and Z. Liu, 2010. A hybrid password authentication scheme based on shape and text. J. Comput., 5: 765-772.