

REFERENCES

- Ambekar, N. & Welekar, A. 2015. "Survey on Graphical Password Based on User Authentication". *International Journal of Research*. Vol. 2(3): p. 479-487. ISOAR.
- Adams, A. & Sasse, M. A. 1999. "Users are not the enemy: why users compromise computer security mechanisms and how to take remedial measures". *Communications of the ACM*, 42:41-46.
- Almuairfi, S., Veeraraghavan, P., & Chilamkurti, N. 2013. "A novel image-based implicit password authentication system (IPAS) for mobile and non-mobile devices". *Mathematical and Computer Modelling*, Volume 58, Issues 1–2, Pages 108-116, ISSN 0895-7177.
- Biddle R., Chiasson, S., & Oorschot, P.C. 2010. "Graphical Passwords: Learning from the First Twelve Years". *ACM Computing Surveys (CSUR)*. Vol. 44(4): p. 19. ACM.
- Brostoff, S. & Sasse, A. 2000. "Are Passfaces more usable than passwords? A field trial investigation". In McDonald, S. et al., (ed.) *Proceedings of HCI 2000*. Sunderland, UK Springer, pp. 405-424
- Charreau, D., Furnell, S. & Dowland, P. 2005. "PassImages: An alternative method of user authentication". *ISOneWorld*. Las Vegas, USA March 30 – April 1.
- Chiasson, S., Forget, A., Biddle, R., & Van Oorschot, P. C. 2008. "Influencing users towards better passwords: Persuasive Cued Click-Points". In *Human Computer Interaction (HCI)*, The British Computer Society.
- Chiasson, S., Van Oorschot, P., & Biddle, R. 2006. "A usability study and critique of two password managers". In *15th USENIX Security Symposium* May 8.
- De Angeli, Coventry, L., Johnson, G., and Renaud, K. 2005. "Is a picture really worth a thousand words? Exploring the feasibility of graphical authentication systems," *International Journal of Human-Computer Studies*, vol. 63, no. 1-2, pp. 128–152.
- Djamila, R. & Perrig, A. 2000. "Deja Vu: A user study using images for authentication". *Proceedings of the 9th USENIX Security Symposium*. Denver, Colorado, USA August 14-17,

2000. USENIX Association, pp. 45-58.

Elamathi, P., Saranya, S., & Elamathi, E. 2013. "Implementing Authentication Providers using Image and Sound Signature". *IJREAT International Journal of Research in Engineering & Advance Technology*, Vol 1, Issue 1.

Emanuel V. Z., Alexander D. L., Philipp J., & Heinrich H. 2015. "Easy to Draw, but Hard to Trace? On the Observability of Grid-based Unlock Patterns". In *Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems (CHI '15)*. ACM, New York, NY, USA, pp 2339–2342.

Fatehah, M.D., Jali, M. Z., Wafa M.K., & Anuar, N. B. 2015. "Graphical Authentication Using Enhanced Hybrid Graphical Authentication System". *Asian Journal of Information Technology*, pp 14: 1-10.

Fulkar, A., Sawla, S., Khan, Z., & Solanki, S. 2012. "A study of Graphical Passwords and Various Graphical Password Authentication Schemes". *World Research Journal of Human-Computer Interaction*, vol. 1, pp 04-08.

Gao, H.C., Liu, X. Y., Wang, S. D., & Dai, R. Y. 2009. "A new graphical password scheme against spyware by using CAPTCHA". In: *Proceedings of the symposium on usable privacy and security*. Mountain View, California. ACM, pp. 1-1.

Gao, H. Zhongjie, R. Chang, X. Liu, X. & Aickeln, U. 2010. "A New Graphical Password Scheme Resistant to Shoulder-Surfing". *International Conference on CyberWorlds*.

Georgakakis, E., Kommos, N., & Douligaris, C. 2012. "NAVI: Novel Authentication with Visual Information". In *the proceedings of the 2012 IEEE Symposium on Computers and Communications (ISCC)*, pp. 588-595.

Goldberg, I., Hagman, J., & Sazawal, V. 2002. "Doodling Our Way to Better Authentication," presented at *Proceedings of Human Factors in Computing Systems (CHI)*, Minneapolis, Minnesota, USA April 20.

Hinds, C. & Ekwueme, C. 2007. "Increasing security and usability of computer systems with graphical password". ACM Southeast Regional Conference. Winston-Salem, North Carolina, USA ACM New York, USA, pp. 529-530.

Hong, D., Man, S., Hawes, B., & Mathews, M. 2004. "A password scheme strongly resistant to spyware," in *Proceedings of International conference on security and management*. Las Vegas, NV.

Jali, M. Z. 2011. "A Study of Graphical Alternatives for User Authentication". (PhD Thesis). School of Computing and Mathematics, Faculty of Science and Technology, University of Plymouth.

Jansen, W. 2004. "Authenticating Mobile Device Users Through Image Selection," in *The Internet Society: Advances in Learning Commerce and Security*, vol 1, pp 183-194.

Jermyn, I., Mayer, A., Monrose, F., Reiter, M. K., & Rubin, A. D. 1999. "The Design and Analysis of Graphical Passwords," in *Proceedings of the 8th USENIX Security Symposium*. Washington DC, USA August 23-26. The USENIX Association, pp 1-14.

Jonathan W. S. 2015. "The Impact of Image Synonyms in Graphical-Based Authentication Systems". (PhD Thesis). Graduate School of Computer and Information Science, Nova Southeastern University.

Kessler, Gary C., 2002. "Passwords-Strengths and Weaknesses". Jan-1996. Scott, I., MacKenzie, "KSPC as a Characteristic of Text Entry Techniques", Dept. of Computer Science, New York University Toronto, Ontario, Canada M3J 1P3.

Obasan A., Norafida I., Jali. M. Z., Nicholas A. 2013. "Graphical Password Schemes Design: Enhancing Memorability Features Using Autobiographical Memories". In *Journal of Theoretical and Applied Information Technology*, Vol. 53 No.1.

Paivio, A. 2006. "Mind and Its Evolution", *A Dual Coding Theoretical Approach*. Lawrence Erlbaum: Mahwah, N.J.

Pilar, D. R., Jaeger, A., Gomes, C. F. & Stein, L. M. 2012. "Passwords Usage and Human Memory Limitations: A Survey Across Age and Educational Background". *PLoS ONE*. Vol. 7(12): e51067.

Rass, S., Schuller, D. & Kollmitzer, C. 2010. "Entropy of Graphical Passwords: Towards an Information-Theoretic Analysis of Face-Recognition Based Authentication". *Communications and Multimedia Security*. Springer Berlin / Heidelberg, pp. 166-177.

Ray, P. P. 2012. "Ray's Scheme: Graphical Password Based Hybrid Authentication System for Smart Hand Held Devices". *Journal of Information Engineering and Applications*, Vol. 2(2): pp. 1-11. IISTE.

Reddy, G. S., Prasad, G. V., Prasad, V. H. 2013. "Graphical Secure Password Method against Online Password Hackers (Guessing Attacks)". *International Journal of Computer Science and Mobile Computing*, Vol. 2, Issue. 8, pg.163 – 168.

Renaud, K. 2005. "Evaluating authentication mechanisms". In *Cranor, L. & Garfinkel, S. editors, Security and Usability: Designing Secure Systems That People Can Use*, chapter 6, pp.103-128. O'Reilly Media.

Robinson, P. 2015. "Secure Graphical Passwords". In *RSA Conference*, Moscone Center, San Francisco April 14. IDY-F02.

Saranya, R. & Bindhu, J. S. 2014. "A Survey on Different Graphical Password Authentication Techniques". *International Journal of Innovative Research in Computer and Communication Engineering*, Vol. 2, Issue 12, pp 7-28.

Sasse, M. & Flechais, I. 2005. "Usable Security: Why do we need it? How do we get it?" In *Cranor, L. & Garfinkel, S. editors, "Security and Usability: Designing Secure Systems That People Can Use"*, chapter 2, pp. 13-30. O'Reilly Media.

Saevarsson, F. 2012. "Combinatorics in Pattern-Based Graphical Passwords". (Master Thesis). Department of Mathematics, Kungliga Tekniska Högskolan, Stockholm, Sweden.

Schechter, S., Herley, C., & Mitzenmacher, M. 2010. "Popularity is Everything: A new Approach to Protecting Passwords from Statistical-Guessing Attacks". In *Proceeding HotSec'10 Proceedings of the 5th USENIX conference on hot topics in security*. pp. 1-8.

Seng, W. C., Khuen, Y. K., & Shing, N. L. 2011. "Enhanced Graphical Password by Using Dynamic Block-Style Scheme". *International Conference on Information and Intelligent Computing IPCSIT*. Vol. 18. p. 139-145. IACSIT Press, Singapore.

Shraddha S. Banne, Kishor N. Shedge. 2016. "CARP: CAPTCHA as A Graphical Password Based Authentication Scheme", in *International Journal of Advanced Research in Computer and Communication Engineering*, vol. 5, Issue 1. ISSN (Online) 2278-1021.

Sobrado, L. & Birget, J. C. 2002. "Graphical passwords". *The Rutgers Scholar: An Electronic Bulletin for Undergraduate Research*, Rutgers University, New Jersey, vol. 4.

Stobert, E., & Biddle, R. (2013). "Memory retrieval and graphical passwords". *Paper presented at the Proceedings of the Ninth Symposium on Usable Privacy and Security*, Newcastle, United Kingdom July 24 – 26.

Takada, T. & Koike, H. 2003. "Awase-E: Image-based Authentication for Mobile Phones using User's Favorite Images," in *Human-Computer Interaction with Mobile Devices and Services*, vol. 2795 / 2003: Springer-Verlag GmbH, pp. 347 - 351.

Tullis, Thomas S., Tedesco, Donna P., McCaffrey, Kate E. 2011. "Can users remember their pictorial passwords six years later". In: *Proceedings of ACM CHI 2011 Conference on Human Factors in Computing Systems*, pp. 1789-1794.

Umar, M. S. & Rafiq, M. Q. 2012. "Select-to-Spawn: A Novel Recognition Based User Authentication Scheme". *IEEE International Conference on Signal Processing, Computing and Control*, pp. 1 – 5.

Vrunda B. 2013. "Graphical Authentication Based Techniques". In *International Journal of Scientific and Research Publications*, Volume 3, Issue 7. ISSN 2250-3153.

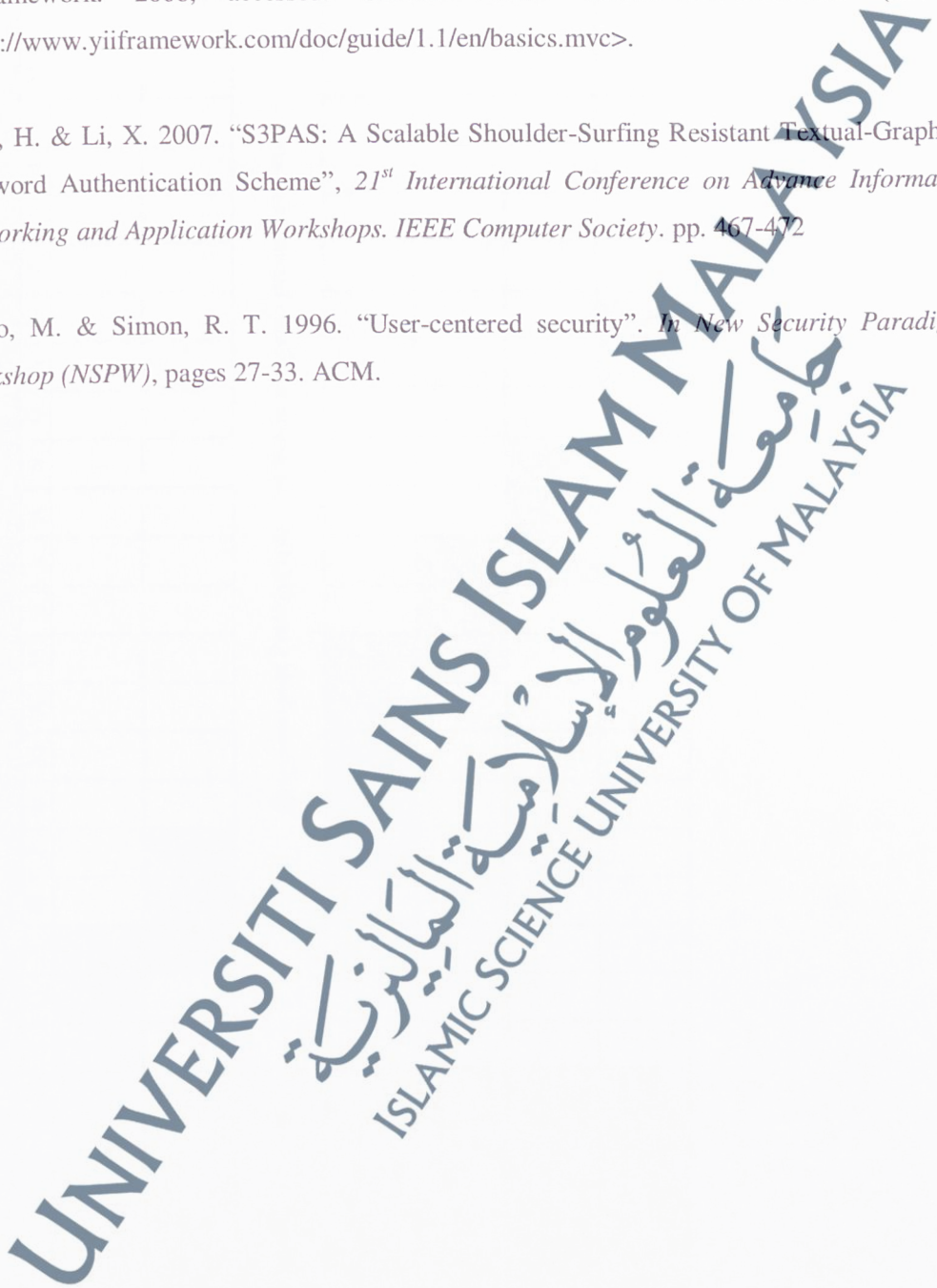
Whitten, A. & Tygar, J. 1999. "Why Johnny can't encrypt: A usability evaluation of PGP 5.0" In *8th USENIX Security Symposium*, Washington, D.C. August 23 – 26.

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 pp. 102-127.

Yiiframework. 2008, accessed: Oktober 2016. "Model-View-Controller (MVC)". <<http://www.yiiframework.com/doc/guide/1.1/en/basics.mvc>>.

Zhao, H. & Li, X. 2007. "S3PAS: A Scalable Shoulder-Surfing Resistant Textual-Graphical Password Authentication Scheme", *21st International Conference on Advance Information Networking and Application Workshops*. IEEE Computer Society. pp. 467-472

Zurko, M. & Simon, R. T. 1996. "User-centered security". *In New Security Paradigms Workshop (NSPW)*, pages 27-33. ACM.



APPENDIX B: BRIEFING SHEET

About ChoCD

ChoCD is an alternative graphical authentication scheme. This prototype uses the combination of user actions' (i.e. choice, click and draw). ChoCD scheme offers benefits of security and usability for the users. The operational framework of the design process was discussed in two different stages: password creation step (registration) and authentication step (login).

Password Creation Step

- i. The first step is to enter the user ID that would be stored in the database (i.e. username must be 'unique').
- ii. For the second step random images are displayed to the user and user must select only two images from the 25 of images in 5x5 grid form. This is done by using the recognition-based schemes.
- iii. The two selected images are then appearing on screen and user must click two points on each images and draw a pattern on it, which are stored as password in the database with the specific user ID.

Authentication Step

- i. During the authentication phase, user must enter user ID and the system displays 5x5 grids form that containing random type of images. User must choose two-selected images. Then, if the user ID exists and the selected images matched, the two-selected images would be appearing behind the pattern-draw authentication. Finally, user must click points on image and draw a pattern on it.

Important

In the authentication step, during the first authentication, if user failed to attempt a graphical password more than three times, the system requires user to solve CAPTCHA, while in the second authentication, once the attempt failed to pass, the system will bring user to the first authentication back.

APPENDIX C: ChoCD QUESTIONNAIRE

ChocD Authentication System Prototype Questionnaire						
	Question	1	2	3	4	5
PART 1		Always	Usually	Often	Rarely	Never
1	How frequently do you deal with the graphical authentication schemes?					
		Very Easy	Easy	Moderate	Difficult	Very Difficult
2	How do you evaluate the graphical authentication scheme from an ease-of-use perspective?					
		Not Secure	Less Secure	Moderate	Secure	Very Secure
3	How do you evaluate the graphical authentication scheme from a security perspective?					
PART 2		Very Easy	Easy	Moderate	Difficult	Very Difficult
1	How do you evaluate ChoCD from an easy-to-use perspective?					
		Not Secure	Less Secure	Moderate	Secure	Very Secure
2	How do you evaluate ChoCD from a security perspective?					
		Always	Usually	Often	Rarely	Never
3	Do you remember the username and graphical "password" for the next testing phase?					
		Very Unhelpful	Unhelpful	Moderate	Helpful	Very Helpful
4	What do you think about the documentation given in the ChoCD testing?					
		Very Confusing	Confusing	Moderate	Clear	Very Clear
5	What do you think about the graphical images in 5x5 grid?					
		Always	Usually	Often	Rarely	Never
6	Is it the performing task is straightforward?					
		Always	Usually	Often	Rarely	Never
7	ChoCD is designed for all level of users?					
		Always	Usually	Often	Rarely	Never
8	Is it the terminology related to task?					
		Very Slow	Slow	Moderate	Fast	Very Fast
9	How about the system speed for overall authentication system prototype?					
		Very Easy	Easy	Moderate	Difficult	Very Difficult
10	How do you evaluate for learning to operate the system?					

APPENDIX E: COPY OF PUBLISHED PAPER

ChoCD: Usable and Secure Graphical Password Authentication Scheme

Radhi Rafiee Afandi

Faculty of Science and Technology

Universiti Sains Islam Malaysia (USIM)

71800, Bandar Baru Nilai, Nilai, Negeri Sembilan, Malaysia

e-mail:mr.didie92@gmail.com

Mohd Zalisham Jali

Faculty of Science and Technology

Universiti Sains Islam Malaysia (USIM)

71800, Bandar Baru Nilai, Nilai, Negeri Sembilan, Malaysia

e-mail:zalisham@usim.edu.my

Abstract

Since designing effective graphical password authentication schemes is of vital important, this paper attempts to address the need by providing a new way for designing and developing hybrid graphical scheme named ChoCD. ChoCD combines the method of "Click-based", "Choice-based", and "Draw-based". By combining these, it is anticipated that it will offer better usability and security. An evaluation towards ChoCD was conducted to measure its viability and practicality as the alternative user authentication. From these conduct of evaluations, it was found that ChoCD is easy to use and provides more security than other existing schemes and thus potentially be used for user authentication.

Keywords: *Graphical password, Password, User Authentication Security, Usability*

1. Introduction

Nowadays, all of the user authentication purpose in computer security depends on password [1]. In this regards, the main method that can be used to guarantee information security is authentication, and password authentication is the most often used and handy method of authentication. Password refers to the secret use for authentication [2]. This is the most frequently used method for authentication by identifying a computer system's users. In this light, Graphical password is also known as 'graphical user authentication' (GUA) which refers system used for authentication where the users will have to choose images in a particular sequence, which is presented through a GUI (graphical user interface). Inherently, GUA ad GUI can replace the conventional alphanumeric passwords where instead of typing alphanumeric strings, the users will authenticate themselves by clicking on images.

This paper is arranged as follows, it starts with a review of graphical password. The next section describes ChoCD design and development which is the core of this paper. Then, the next section explains initial evaluation of ChoCD based on its security level and usability from the

perspective of the users. Finally, the last section summarizes the proposed scheme and conduct of experiments.

2. Graphical Password Classifications

This paper proposes the Graphical-based password technique as a prospective substitute to the text-based techniques. In this regard, this proposal is based on the well known fact that images can be remembered by humans compared to the text-based [3]. Thus, it is believed that schemes with graphical-based authentication, compared to the present method for authentication, will have higher level of memorability. Furthermore, compared with the token-based and text-based authentications, graphical passwords are more difficult to break through the use of normal attacks such as brute force, dictionary attack, and spyware [4]. Consequently, it is claimed that this method has a higher level of security compared to others [5].

In the graphical passwords scheme, the user is required to select memorable images. The process of selecting memorable images is based on the disposition of image processing and the precise click location's sequence. Therefore, image content should be meaningful so that it is memorized by the user, as random content may be less memorable. In this regard, this paper proposes graphical-based passwords as an alternative to the conventional password method. This is because, compared to texts, pictures are easier to remember. Consequently, past researchers coined this as "picture superiority effect" [6]. From our findings, majority of literatures on graphical password (1994- January 2016) mentioned that graphical password authentication can be put into three groups. This group is based on memory classification. In the pure Recall-Based category, users are required to recall their passwords without any form of gestures, reminder or hints. This category can be perceived as convenient and simple, however, at times, the users are having difficulty in remembering their passwords. Such scheme includes the Draw a Secret (DAS) and qualitative DAS [7].

Meanwhile, the Cued Recall Based category outlines a framework which comprise of strategies that can assist the users to recall their passwords or to make more accurate recall such as hints, reminder, and gestures. Examples of authentication belong to this category are Blonder algorithm [8] and Passpoint [9]. Other category known as Recognition-based, where users select icons, symbols or pictures from the set of given images. In this regard, the users are required to identify their registration choice from a set of prospective images during the authentication process [10]. Meanwhile, authentication using the hybrid schemes category typically combine two or more schemes which are adopted to overcome the limitation of a single scheme, which might not be able to single handedly protect against spyware, guessing attack, brute force search and shoulder surfing. The example of hybrid scheme is the authentication for online banking system, which combine graphical images authentication and textual-based password [11],

Another classification for graphical password is based on the users' action: named as click-based, draw based and choice-based. Briefly, the user of a choice based scheme needs to memorize a set of images in a prescribed category. Meanwhile, the click based scheme entails the user to set a password by choosing certain spot on a prescribed image. As they log in, the user needs to re-click the spot they clicked either randomly or in a sequential order. Finally, draw based scheme requires user to sketch, draw on given image background.

3. ChoCD

Motivated by the hybrid scheme, the graphical password authentication system named ChoCD is developed. The idea of ChoCD is to give an experience to user to log into their accounts using username and graphical password rather than using conventional text-based passwords. It is

intended not only for desktop use, but it can also be used in the mobile devices. ChoCD’s generic conception comprise of three forms of authentication, starting from choice-based, followed by the click-based and finally, draw based authentication. The flow is generally easy and uncomplicated to construct. Consequently, it can be used to guide the users to easily use and implement this scheme. There are two steps in the whole process, password creation and login. For the basic scheme, a simple example can be used to describe both stages. This authentication is beneficial as only the correct user would remember the passwords (graphical images, position-for-click and pattern draw). In this light, as the users’ memory can be triggered by the images, this method is more memorable and secure as compared to other types of graphical password. Figures 1 and 2 present the illustration of the interface of the ChoCD prototype.

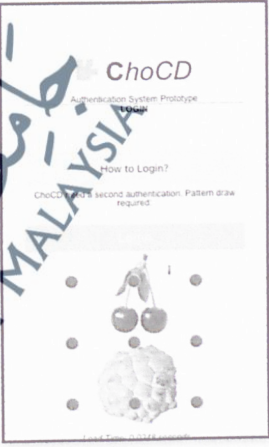
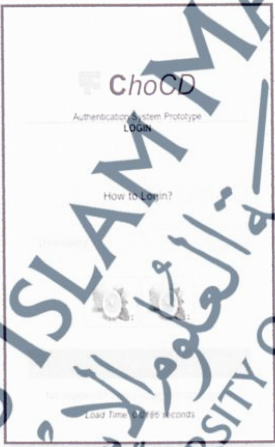
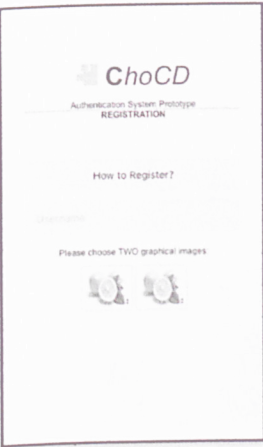


Figure 1. Screenshot of the Password Creation Step

Figure 2. Screenshot of the Login Step

4. Evaluation

Evaluations towards ChoCD authentication were conducted with regards to its usability and security. It was tested by a number of participants from various backgrounds and having a number of years using computer within authors’ institution. All of them were given a set of questionnaires’ to answer after they used the ChoCD prototype.

4.1 Procedures and Steps

Participants in the study were requested to read the briefing sheet before embarking into the actual test. Once completed, they were requested to register into the ChoCD system. Each of the participants had to follow these following steps:

Step 1: Training Phase

The participants were briefed about the primary purpose of this research, as well as what they were expected to do. The briefing covers definitions of the range of different schemes such as token, biometric, text-based and graphical password schemes. Later, they were presented with an overview of the testing steps, ChoCD itself, and questionnaire. The participants were also

presented with a number of graphical images and were briefed on how to draw a pattern on the image. A discussion session was also held.

Step 2: Testing Phase

Two sessions involved. First session dealt with registration and the second session focused on login. Times taken for both phases were recorded through the system prototype. The participants were asked to register before they could login. The questionnaire for the prototype was presented to each participant. Briefly, participants were requested to answer the questionnaire related to the security and usability of the scheme.

4.2 Results

The evaluation involved 41 participants from the IT background and 44 participants from non-IT background; as presented in the Figure 3. In the Figure 4, it can be seen that the median time taken for participants was 17.50 seconds for password creation and 15.66 seconds for login. Basically, the default measure of centrality is the mean, but when the distribution is skewed, the median will better match to the intuitive meaning of "middle".

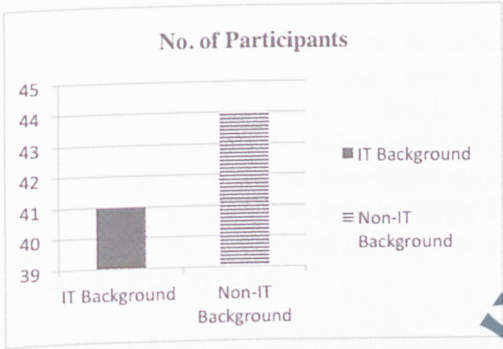


Figure 4. Number of Participants Participated

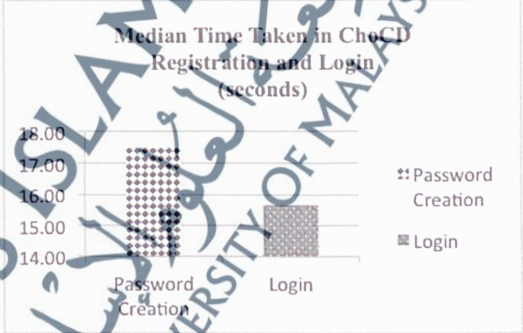


Figure 4. Median time for Register and Login

4.3 Usability Perception Towards ChoCD

Usability means how easy it is to learn, to use a system and the extent of how it can fulfil users' needs [12]. Despite there are various authentication schemes proposed that claimed to increase the strength of a password, these systems' usability is still unexplored. Thus, a scale was used to investigate users' feedback on a range of authentication schemes. This scale is split into five stages: *very easy*, *easy*, *moderate*, *difficult*, and *very' difficult*. ChoCD was included in the survey and was explained to measure other authentication schemes. Figure 5 results indicated that ChoCD is perceived as an easy authentication method by the participants. When asked which part they liked most of ChoCD, participants responded that they like the user interface as it quite user friendly.

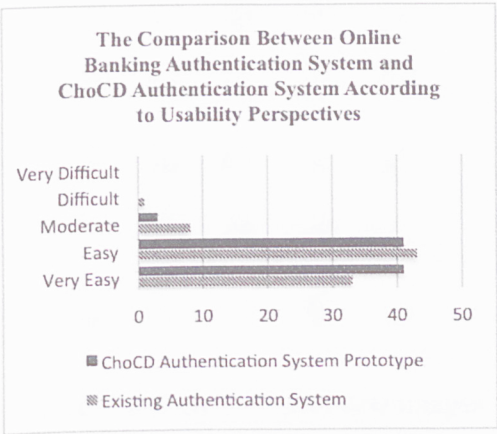


Figure 5. The comparison of usability between existing authentication schemes and ChoCD

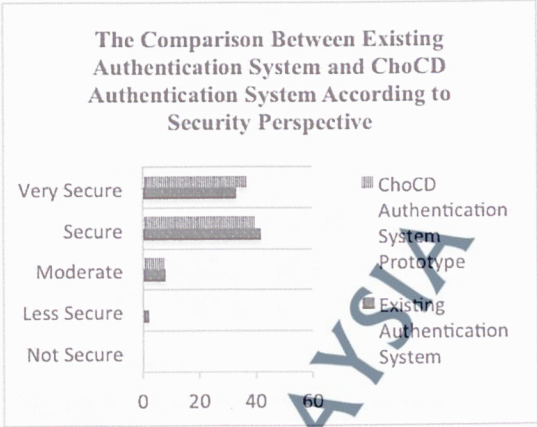


Figure 6. The comparison of security between existing authentication schemes and ChoCD

4.4 Security Perception Towards ChoCD

The participants’ thought on the different authentication schemes security level was prompted in this survey. The participants were given these options; *Not Secure, Secure, Moderate, Very Secure and Strongly Secure*. ChoCD, along with present online banking authentication schemes were included to see the authentication scheme, which is deemed to be the most secure. Then, the stages were reviewed and rearranged into three stages. *Moderate* is considered as Average, *Secure* and *Very Secure* means Above Average, *Not Secure* and *Less Secure* is indicated as below average. In this light, the above average (secure and very secure) values were used to evaluate particular schemes’ security level.

Figure 6 shows that ChoCD authentication scheme is deemed as the most secure by 77 participants. Meanwhile, 75 participants ranked the present authentication system as the most secure. These responses indicate that in general, participants think that ChoCD is most secure scheme. Moreover, it shows that ChoCD authentication system prototype scheme and scored an acceptable level of security. This further indicates that in comparison to the text-based password, the entropy of password in graphical password schemes is longer. Therefore, ChoCD has shown an anticipated balance between security and usability that can be used as a new enhancement of authentication scheme.

4.5 Pattern of ChoCD

In term of secret chosen by the participants, it was observed that the chosen image was predominantly affected by the sequence that appeared earlier. For the first graphical image secret, the participants most probably select lemon, grape and strawberry images, while for the second graphical image secret, participants most likely to select the image from the next row or grid. They would choose the image by sequence. For example, they would choose the image from top to bottom or from left to right grid. Table 1 shows popular images chosen by participants.



Figure 7. 5x5 Grid of graphical images



Figure 8. Samples of clicks and draws.

Table 1. Popular image picked by participants

1 st Graphical image	Frequency of participants
Lemon	40
Grape	14
Strawberry	31
2 nd Graphical image	No. of participants
Strawberry	42
Banana	25
Apple	37
Coconut	11

For the click-based secret, which requires the participants to select any click-points on the 3x3 pattern draw given, it was found that most of the participants preferred to click on left side first. For the draw-based secret, where they were required to draw a line on the screen, it was found that participants drawing secret were similar to the pattern during the click-based secret. For example, participants chose to start click the dot from the left side then they would draw a pattern from the left side too. Figures 7 and 8 show examples of click and draw made by a number of participants.

5. Conclusion

This paper presents a new graphical scheme based on the hybrid scheme combination named ChoCD. The prototype of ChoCD authentication system was developed and gave to users to test the prototype. Based on the evaluations, findings suggest that majority of participants agreed ChoCD prototype is user friendly and the “secrets” is easy to remember. In addition to this, ChoCD is said to maintain the usability and security simultaneously. For the future, we will conduct more users testing on ChoCD scheme and analyze extensively all of the data from the result in order to make further enhancement. We hope that the new hybrid scheme, ChoCD will be used widely for all system’s user according to the accomplishment of usability’ and security perspectives in this scheme.

6. Acknowledgements

Authors wish to thank all participants who participated in the study. This research is funded by the Ministry of Higher Education of Malaysia and Research Management Centre of USIM via grant research with code USIM/FRGS/FST/32/50315.

7. References

- [1] Shraddha S. Banne, Kishor N. Shedge. "CARP: CAPTCHA as A Graphical Password Based Authentication Scheme", in International Journal of Advanced Research in Computer and Communication Engineering Vol. 5, Issue 1, January 2016.
- [2] K. Renaud. "Evaluating authentication mechanisms", in L.Cranor and S. Garinkel, editors, Security and Usability: Designing Secure Systems That People Can Use, chapter 6, pp.103-128. O'Reilly Media, 2005.
- [3] Xiaoyuan S, Ying Z et al. "Graphical passwords: a survey", in: 21st annual computer security applications conference, pp 463–472, 2005.
- [4] Wells J, Hutchinson D, Pierce J. "Enhanced security for preventing man-in-the-middle attacks in authentication, data entry and transaction verification", in Australian information security management conference. Paper 58, 2008.
- [5] Almuairfi S, Veeraraghavan P and Chilamkurti N. "IPAS: User Test Phase and Evaluation", in Frontier and Innovation in Future Computing and Communications, Lecture Notes in Electrical Engineering 301, DOI: 10.1007/978-94-017-8798-7_2, Springer Science+Business Media Dordrecht, 2014.
- [6] S. Chiasson, A. Forget, R. Biddle, and P. C. van Oorschot. "Influencing users towards better passwords: Persuasive Cued Click-Points". In Human Computer Interaction (HCI), The British Computer Society, September 2008.
- [7] I. Jermyn, A. Mayer, F. Monroe, M. Reiter and A. Rubin. "The design and analysis of graphical passwords". In Proceedings of the 8th USENIX Security Symposium, August 1999.
- [8] G. E. Blonder, "Graphical passwords," in Lucent Technologies, Inc., Murray Hill, NJ, U. S. Patent, Ed. United States, 1996.
- [9] S. Wiedenbeck, J. Waters, J. C. Birget, A. Brodskiy, and N. Memon, "Authentication using graphical passwords: Basic results," in Human-Computer Interaction International (HCII 2005), Las Vegas, NV, 2005.
- [10] H.C.Gao, X.Y.Liu, S.D.Wang, R.Y.Dai. "A new graphical password scheme against spyware by using CAPTCHA", in: Proceedings of the symposium on usable privacy and security, 15-17 July, 2009.
- [11] H. Alsaiani, M. Papadaki, P.S. Dowland and S.M. Furnell. "Alternative Graphical Authentication for Online Banking Environments", in Proceedings of the 8th International Symposium on Human Aspects of Information Security & Assurance (HAISA), 2014.
- [12] S. Chiasson, P. van Oorschot, and R. Biddle. "A usability study and critique of two password managers", in 15th USENIX Security Symposium, August 2006.

Authors

Radhi Rafiee Afandi

*Faculty of Science and Technology,
USIM, 71800, Nilai, Negeri Sembilan, Malaysia.
e-mail:mr.didie92@gmail.com*

Mohd Zalisham Jali

*Faculty of Science and Technology,
USIM, 71800, Nilai, Negeri Sembilan, Malaysia.
e-mail:zalisham@usim.edu.my*

UNIVERSITI SAINS ISLAM MALAYSIA
جامعة العلوم الإسلامية الماليزية
ISLAMIC SCIENCE UNIVERSITY OF MALAYSIA