

CHAPTER 5

ChoCD EVALUATIONS

5.1 OVERVIEW

This chapter presents the studies conducted to investigate the practicability of ChoCD. Evaluations towards ChoCD authentication were conducted with regards to its usability and security. This includes the evaluation on password entropy in this scheme. Then, it was tested by a number of participants from various backgrounds and having a number of years using computer within the researcher’s institution. All of them were given a set of questionnaires’ to answer after they used the ChoCD prototype. Each study involves in the explanation of its procedure, results and findings, and discussion.

5.2 ChoCD ENTROPY EVALUATION

Previous section (refer Chapter 4, Section 4.2.2) mainly gave focus on the development and operational of ChoCD scheme that show the ease of use on this scheme. Then, this section would highlights entropy of the ChoCD for measuring the effective level of security which calculate the ChoCD’s password space. Entropy within the graphical authentication can be said as equivalent of a traditional password’s “key space” which is password lengths multiplied by the range of allowed password characters (Jali, 2011). Table 5.1 showing the entropy evaluation of ChoCD scheme.

Table 5.1: Entropy evaluation of ChoCD

Phase	Password Entropy (bits)
<i>1st Authentication: Choice-based</i> Number of secret = 2 images Total number of images per round = 25 (5x5 grid)	$2 * (\log_2 25) = 9.28$
<i>2nd Authentication:</i> <i>Click-based</i> Number of secret = min = 2 dots, max = 9 dots Total number of dots = d = 9 (points to click) <i>Draw-based</i> Number of pattern possibility = 9! = 362880	$\text{min} = 2 * (\log_2 9) = 6.34$ $\text{max} = 9 * (\log_2 9) = 28.53$ $d = (\log_2 362880) = 18.47$ $\text{min} = 6.34 + 18.47 = 24.81$ $\text{max} = 28.53 + 18.47 = 47$
Total of combination	$\text{min} = 9.28 + 24.81 = 34.09$ $\text{max} = 9.28 + 47 = 56.28$

From the result given (refer Table 5.1), entropy evaluation in ChoCD was showed as a suitable value in security aspect.

5.2.1 Comparison with Existing Schemes

To prove the value of entropy estimation in ChoCD is better, the comparison has been done by reviewed the password entropy in existing graphical authentication: Windows 8 graphical authentication, Android pattern lock and online banking system. The comparison result was showed in Table 5.2.

Table 5.2: Password entropy result between ChoCD and existing authentication schemes

Scheme	Password Entropy (bits)
ChoCD	$34.09 < E < 56.28$
Windows 8 (Robinson, 2015)	$12 < E < 26$
Android Pattern Lock (Robinson, 2015)	18.47
Online Banking (BIMB)	52.4

Based on the Table 5.2, the number of password entropy in ChoCD scheme was better than online banking scheme. It indicates that the security aspect in ChoCD was better than online banking, because the value of entropy refers to the password space, which based on how hard to crack a password (Rass et al., 2010). Although, online banking scheme was a combination of graphical authentication, it still used the text-based as the medium for authentication purpose. The limitation of text-based was mentioned in Chapter 2, Section 2.4. Therefore, ChoCD scheme was a better authentication scheme in aspect of security while it can maintain the usability.

5.3 ChoCD USER TESTING

5.3.1 Background

In this part, the prototype of ChoCD was tested using a number of participants from different backgrounds and with different experience in using authentication schemes. Participants are from Information Technology (IT) backgrounds and non-IT backgrounds. For IT backgrounds, they are from Computer Science students and non-IT backgrounds are from Religion and Da'wah students. All participants engaged in the ChoCD prototype and then answered survey questionnaire. The justification to choose two different background students because it's easy to analyse the ChoCD's user with more knowledge in IT and vice versa.

5.3.2 ChoCD Prototype Testing

This testing is conducted two times (i.e. first week and third week). In the testing phase, participants in this study were requested to read the briefing sheet (as attached in Appendix B) before embarking into the actual test. However, in the future

implementation of ChoCD, the system would provide this briefing sheet on the system. Once completed, they were requested to register into the ChoCD system. The participants were asked to register as a new user in ChoCD authentication system prototype. Firstly, they must decided and enter their username. Then, they must choose two images from set of 25 images as a first graphical authentication and, click and draw a pattern on those images. After they finished in registration phase, the login page will appear and they must remember the previous information for login purpose. Each of the participants had to follow these following steps:

- 1) **Training Phase:** In the beginning of the testing, the researcher informed participants of its main purpose and what they would do before, during, and after the testing. Then, the researcher explained the definitions and the different authentication schemes with simple explanation to the participants. 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. ChoCD uses two random images with different pattern draw to represent the password. The position of graphical images on the grid is changed with every authentication process to avoid replay attacks or shoulder surfing (Elamathi et al., 2013). A discussion session was also held.
- 2) **Testing Phase:** To initiate, the researcher asked the participants to focus on the testing and keep silent to avoid the disruption to the other participants that can spoiled the time taken result. In this 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. The motivation for this survey is multifold. The authentication scheme based on usability and security parameters was analysed. Finally, ChoCD and existing authentication schemes in relation to usability and security issues were compared.

5.4 RESULTS AND ANALYSIS

85 participants from Universiti Sains Islam Malaysia (USIM) contributed in the study. The justification to choose 85 numbers of participants, because it was easy for the researcher to make a user testing by same participants for two times. From the questionnaire, the demographic information responses that 41 participants were from IT background and 44 were non-IT background, as in Figure 5.1. IT background participants were student of Computer Science from the Faculty of Science and Technology, USIM. While, the non-IT background participants were student of Religion and Da'wah studies from the Faculty of Leadership and Management, USIM.

In the Figure 5.2, 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".

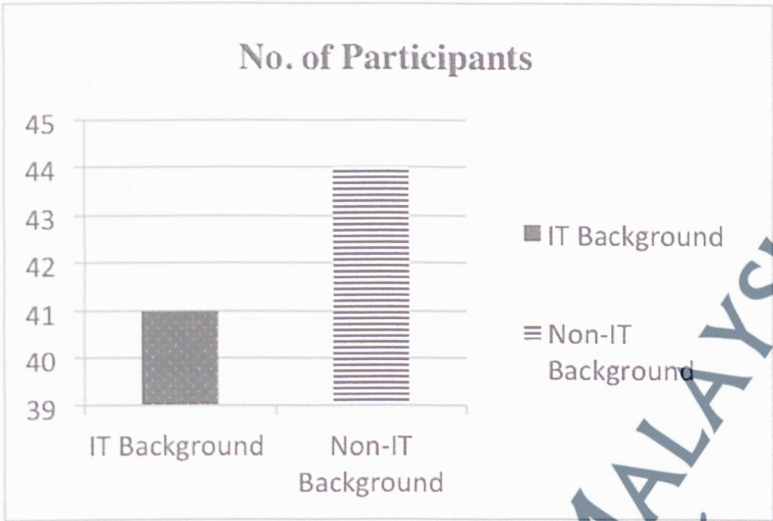


Figure 5.1: No. of participants that contribute in ChoCD questionnaire

The authentication schemes that were explained to the participants before start answering questionnaires are: the text-based authentication scheme, online-banking authentication scheme, Windows 8 graphical authentication scheme and android pattern draw authentication. The first question asked how frequently the participants deal with the graphical authentication schemes, with five response options being always, usually, often, rarely, and never.

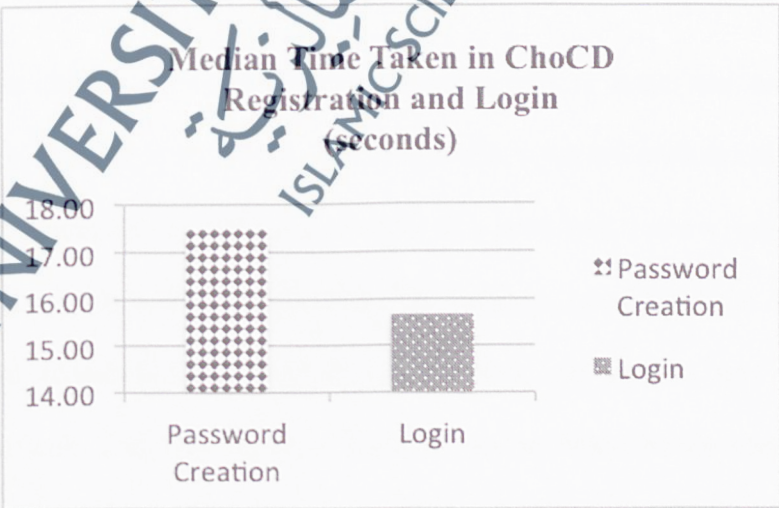


Figure 5.2: Median time taken in ChoCD process

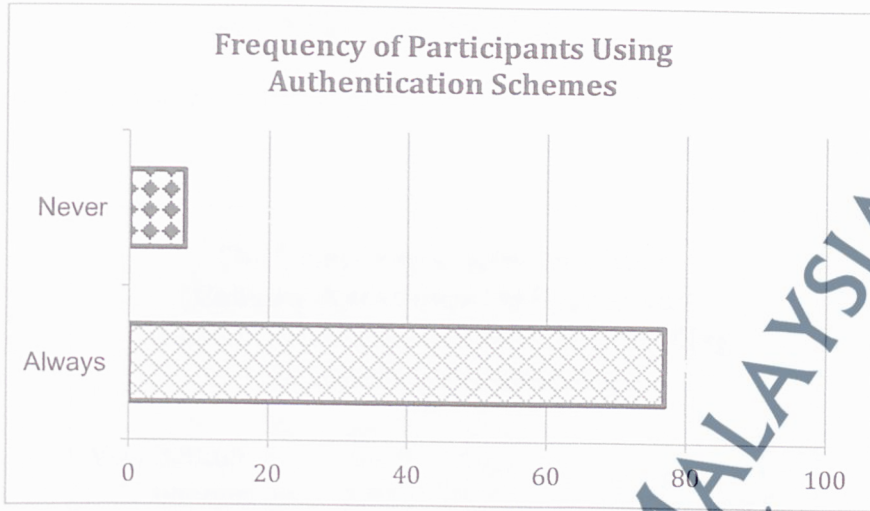


Figure 5.3: Frequency of participants using existing authentication schemes

In response to the question as to how frequently the participants used the authentication schemes. Figure 5.3 shows that seven participants answered never. This indicates that, 78 participants that are majority of the participants were frequent user dealt for authentication schemes. The next questions were designed to evaluate the usability and security of the current graphical authentication schemes in order to compare them with ChoCD, which is the aim in this thesis.

5.4.1 Usability Perception Towards ChoCD

Usability refers to the degree to which a system is easy to learn, use, and meets the user's needs (Chasson et al., 2006). 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 splitted into five stages: very easy, easy, moderate, difficult, and very difficult. ChoCD was included in the survey and was explained to be measure with other authentication schemes. Figure 5.4 shows the results, and it indicated that ChoCD is perceived as an easy authentication method by

the participants. When asked which part they liked the most of ChoCD, participants responded that they like the user interface as it quite user friendly.

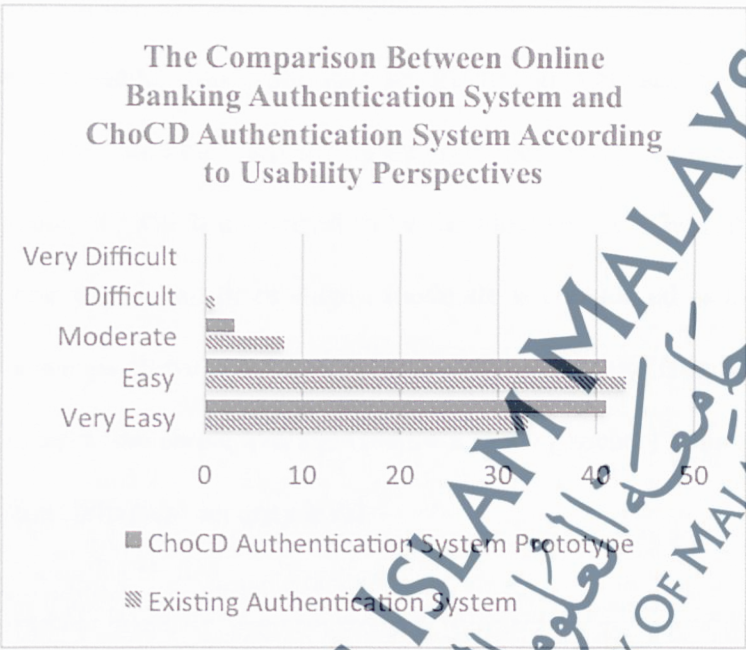


Figure 5.4: The comparison of usability between existing authentication schemes and ChoCD.

76 participants voted that usability of online banking authentication scheme were considering as easy to be used as shown in Table 5.3. While, in relation to ChoCD, 82 participants indicated it was easy to use. From the result, it shows that ChoCD was a better graphical authentication scheme as it better in the usability perspective.

Table 5.3: Classification of usability scale by participants

Scale \ Scheme	Easy	Very Easy	Total
Online Banking Authentication Scheme	43	33	76
ChoCD Authentication Scheme	41	41	82

5.4.2 Security Perception Towards ChoCD

The participants’ thought on the different authentication schemes security level was prompted in this survey. As shown in Figure 5.5, 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.

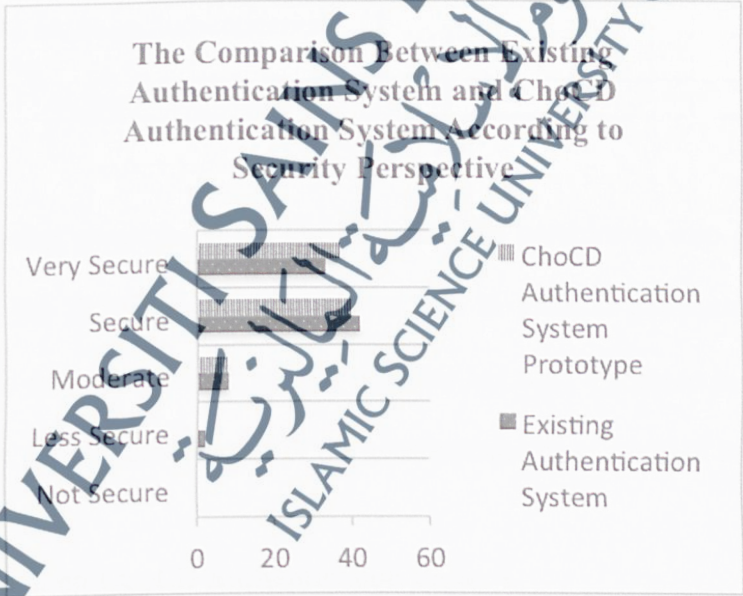


Figure 5.5: The comparison of security between existing authentication schemes and ChoCD

Table 5.4 analysed 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 scheme scored was an acceptable in level of security. This further indicates that in comparison to the online banking authentication scheme, the entropy of password for ChoCD scheme is suitable. Therefore, ChoCD has shown an anticipated balance between security and usability that can be used as a new enhancement of authentication scheme. From this security perception, it can be answered that the number (bits) of password entropy in ChoCD is better than the existing graphical authentications.

Table 5.4: Classification of security scale by participants

Scale	Secure	Very Secure	Total
Scheme			
Online Banking Authentication Scheme	43	32	75
ChoCD Authentication Scheme	41	36	77

For the remaining questions in the questionnaire, the participants also give a worthy feedback for the development and ease of use in ChoCD authentication system prototype. The analysis of the remaining question has been discussed in section 5.4.4. As a reference, the complete results of the questionnaire were attached in Appendix D.

5.4.3 Evaluation on ChoCD Authentication Pattern

This analysis was conducted in order to obtain favourable secret that selected by participants. The secrets were recorded in the database as the combination of most favourable images, click-position and pattern-draw. Favourable secrets were obtained with purposes to get popular images, click-position and pattern-draw, and for security

enhancement.

5.4.3.1 Observation for Choice-based Phase

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, strawberry and grape 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 in sequence. For example, they would choose the image from top to bottom or from left to right grid. Table 5.5 shows popular images chosen by participants.

Table 5.5: Popular images picked by participants

1 st Graphical image	No. of participants
Lemon	40
Strawberry	31
Grape	14
2 nd Graphical image	No. of participants
Apple	37
Banana	25
Strawberry	12
Coconut	11

From the popular images chosen by participants above, it could be concluded that the images can be classified into two groups; namely colour and shape. Colour refers to the striking of colour on the provided fruits in 5x5 grid. Shape refers to the nature of each fruit, where each fruits have a different curve and edge. From the table, it can be seen that the most popular images on the first authentication are lemon and apple, which are that fruits striking in colour (i.e. light yellow and light green respectively)

and have a circle shape. For the security reason, the researcher will take note all of this results for the future works, because the popular images are the ‘hot images’ that chose by participants. In the authentication system, the ‘hot images’ must be avoided to prevent the guessing attack.

5.4.3.2 Observation for Click-based and Draw-based Phase

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 the starting point that participants drawing secret were similar to the point during the click-based secret. For example, participants chose to start click on the point from the left side then they would draw a pattern from the left side too. Figure 5.6 shows example of click and draw made by a number of participants.

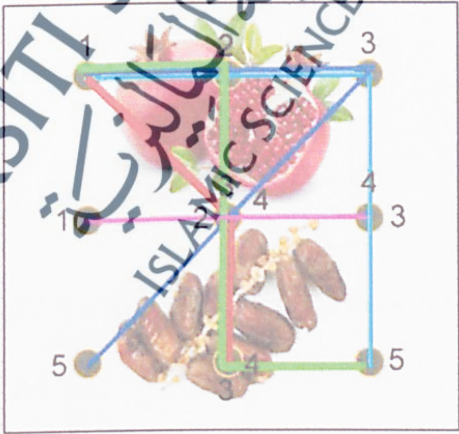


Figure 5.6: Samples of clicks and draws made by participants

From the pattern of drawing drawn by participants, it could be indicated, that the patterns can be classified into three pattern-line categories that were horizontal,

vertical and diagonal. As mentioned above, the participants start draw a pattern-line based on at which point they click on the dot-position on 3x3 grid. Figure 5.7, 5.8, 5.9 and 5.10 shows the different of users' secret in the second authentication, selected from four random participants.



Figure 5.7: Horizontal line



Figure 5.8: Horizontal and vertical lines combination

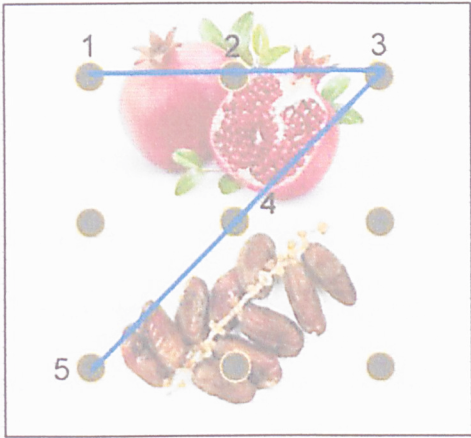


Figure 5.9: Horizontal and diagonal lines combination



Figure 5.10: Diagonal and vertical lines combination

From the four figure above, it can be concluded that the chosen of click position and direction of pattern, drawn by user was based on the common language they understand (i.e. they written from left-to-right for Malay and English language). However, the pattern might be difference if the participants were become accustomed with other language that are Arabic, Farsi, Hebrew, and Urdu, which are written from right-to-left.

5.4.4 General Participants' Feedback

In general, participants had different perceptions for each question of the whole survey. After two weeks, participants were tested again if they can remember their graphical password for ChoCD. Among all 85 participants, 71 were able to remember their graphical passwords and managed to successfully login. While, 14 other participants needed to recall their graphical password and needed several attempts until they can successfully login. In this part, if participants failed to attempt more than three times, the system will block the users in several minutes. In addition, once they failed to attempt, the system will bring them to the first authentication back.

For the briefing sheet given during ChoCD testing, 66 out of 85 participants agreed that they could understand the flow of ChoCD; how to register as a new user and how to login into the system. In addition, majority of them said, the briefing sheet was very helpful since they use the ChoCD prototype for the first time. However, 19 participants needed more understanding by asking the researcher before they can start use ChoCD prototype.

71 out of 85 participants agreed the set of 25 images in 5x5 grid in the first authentication was clear and easy for them to choose. Furthermore, majority of them preferred images of lemon and apple as their graphical authentication (refer Table 5.5). Besides, 14 participants claimed that they were confused and cannot recognize the several types of provided images. It because, some of images on 5x5 grid, same in colour and shape, and several type of images not popular for them.

Table 5.6: Number of participants for several questions in ChoCD questionnaire

Descriptions	No. of Participants
Task is straightforward	77
Terminology related to task	68
Suitable for all users	73

Based on Table 5.6, performing user testing in ChoCD was quiet easy and straightforward. It was because 77 participants agreed that task for register and login in ChoCD prototype was straightforward while, 68 out of 85 participants understand the terminology used on the prototype’s screen. 17 participants were in average group, because all of them confused with the terms of ‘password creation step ’ and ‘ authentication step’. Actually, two of the terms were ‘registration’ and ‘login’ respectively. As a result, the researcher explains every single term in the ChoCD prototype. This prototype also said suitable for all level of users because 73 participants felt ChoCD was user friendly and all level of users can use it. This suggests that graphical authentication scheme was well received by the participants. So that it can be implemented widely in the future.

In addition, the execution time of the ChoCD prototype was embedded on the system. Every single execution on this prototype was displayed on the screen. Therefore, 79 participants agreed, the system speed for overall authentication in this prototype was fast. However, 6 of the participants have some problem with their desktop (i.e. their desktop not running well and running too many processes in one time). Asked about how they experience to operate ChoCD, 72 out of 85 participants claimed that it easy to learn and easy to embark into the user testing on ChoCD.

From the results of questionnaire by 85 participants, it can be said that a number of them were not familiar with graphical authentication. After a brief explanation, all of them were able to carry out all required tasks. The good feedback received by the participants after used ChoCD for two times (i.e. they can remember their password for two weeks ago and used the prototype easily).

5.5 SUMMARY

In this chapter, 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 are easy to remember. In addition to this, ChoCD is said to maintain the usability and security simultaneously. Certainly, there were a few constraints and inadequate results of this study, like participants should from public, not students only, and there was not much findings on the aspect of security. For the future, the researcher will conduct more users testing on ChoCD scheme to public and analyse extensively all of the data from the result in order to make further enhancement.

Currently, no studies have been reported and published specifically on combining of three graphical methods: choice-based, click-based, and draw-based. But in this thesis, the researcher has proven that hybrid scheme namely ChoCD has potential to be implemented more widely in the future. The final chapter will summarise the overall thesis by presenting achievements with respect to the conduct of this research. In addition, it will also highlight the limitations identified while the research had been

conducted, and finally presents potential future works for improving the limitation of the present research, in order to balance the usability, memorability and security of hybrid scheme in graphical authentication.

