# An Anti-Shoulder Surfing Mechanism and its Memorability Test

Lim Kah Seng, Norafida Ithnin and Hazinah Kutty Mammi[*]

[*]*Department of Computer System & Communications*
*Faculty of Computer Science & Information Sciences*
*Universiti Teknologi Malaysia*

*lim0709@gmail.com, afida@utm.my, hazinahkm@gmail.com*

### *Abstract*

*To improve security of mobile device graphical password towards shoulder surfing attack, an anti-shoulder surfing mechanism called Painting Album Mechanism is proposed. This mechanism is constructed based on concept of painting album, and it is consists of three input schemes called Swipe Scheme, Color Scheme, and Scot Scheme. In this paper, usability of this mechanism have been verifying with the memorability test. 30 respondents were authenticating with these three input schemes with multiple authentications. Results were showing Painting Album Mechanism is usable since respondents were succeeding in recalling theirs passwords in acceptable period of time.*

***Keywords****: Authentication, Graphical Password, Shoulder Surfing Mechanism*

## 1. Introduction

Besides textual password, graphical password is another memorable authentication method for authorization. Graphical password is memorable, but it is inherently vulnerable to shoulder surfing attack [1, 2]. Regarding graphical password in mobile devices, people do believe graphical password is perfect for mobile devices, because these devices are usually supported by multi-touch technology, and graphical password is usually work perfect on those touch screen devices [3, 4, 5]. Meantime, people also believed small display screen in mobile device can protect graphical password from shoulder surfing attacks [6, 7]. However, in reality, shoulder surfing attack is still possible for mobile device graphical password [8, 9]. For an example, the case that secret password on mobile device's screen is reflected from the public transport's window. This will give full advantage to device's new owner, if those shoulder surfers are able to retrieve that device, and had remembered the password of that device.

What is shoulder surfing attack? Shoulder surfing attack is a non-technical attack, which require attacker to remember his victim's password by peep through theirs shoulder [10, 11]. This attack is usually implemented in crowded places, and it is usually difficult to discern. So far, countermeasure for this issue is to implement a mechanism so called anti-shoulder surfing mechanism, like what you can be seen in Triangle Scheme [12] or ColorLogin Scheme [13] or RGGPW Scheme [14]. Yet, literature review shows existing anti-shoulder surfing mechanism is usually applicable for graphical password scheme in wide display devices only, instead of those small mobile devices [15]. This is why, in this paper, we are trying to improve the security of graphical password for mobile devices, by proposing an anti-shoulder surfing mechanism called Painting Album Mechanism.

## 2. Painting Album Mechanism

Painting Album Mechanism is an anti-shoulder surfing mechanism, which has characteristics of both recall and recognition graphical techniques. Thus, this mechanism is also a hybrid graphical password anti-shoulder surfing mechanism. It was developed based on results of user's affinity of choices [16, 17], and through observation on the way kids are behave, while they paint the picture. When this mechanism was developed, results from user's affinity of choice survey had become the mechanism's architecture. Meantime, outcome of the observation have created this mechanism three input schemes, where we named it Swipe Scheme, Color Scheme, and Scot Scheme.

In Painting Album Mechanism, Swipe Scheme, Color Scheme, and Scot Scheme are the methods for password creation. Each input scheme is non-identical, and it is user's options to choose the input scheme they prefer. In Table 1, these three input schemes with its input methods are shown.

**Table 1. Painting Album Mechanism Input Schemes**

| **Input Schemes** | **Input Methods** |
|---|---|
| Swipe Scheme | Swipe the pictures |
| Color Scheme | Touched the picture, then, select the colored boxes. |
| Scot Scheme | Swipe the picture, meantime, touch the pictures, and picked the colored boxes |

Although users have the right to choose their favorite input scheme, however, for the sake of security, users are encouraged to have more than one input schemes, for producing their password.

### 2.1. Registration Process

Process involved in Painting Album Mechanism is rather simple. It is initiated with the step selecting a picture as theme picture. Four or more pictures were provided, and users have to select one of the pictures as the theme picture. Afterwards, each user has to register their new password with Swipe Scheme, Color Scheme, or Scot Scheme. At below, steps for registration are listed:

**Step 1**: Choose a theme picture.

**Step 2**: Select pictures, colored boxes, or both, with the available input schemes (Swipe Scheme, Color Scheme, or Scot Scheme).

**Optional Step 1(Swipe Scheme):** Swipe the pictures.

**Optional Step 2(Color Scheme):** Touched the picture, then, picked those colored boxes.

**Optional Step 3(Scot Scheme):** Swipe the picture, at the same time, have to touch the pictures, and picked those colored boxes.

**Step 3:** Lastly, clicks the 'register' button at bottom.

To succeed in registration, it is important for users to ensure at least eight pictures, colored boxes, or both of these two things are chosen. Password lengths (number of pictures, colored boxes), which are shorter than eight is not acceptable in Painting Album Mechanism, similar to textual password.

### 2.2. Authentication Process

Without having to concern about the theme picture, users have to start the authentication by re-selecting all pictures, colored boxes, or both of these two things, which they have register, by follow the rules of input schemes. At below, processes for authentication are listed:

**Step 1:** Reselect pictures, colored boxes, or both of these two things that had chosen during registration phase.

**Step 2:** Clicks on ‘log-in’ button at bottom.

During authentication, users have to ensure those pictures and colored boxes are selected in correct sequence. Any mistakes in choosing the wrong pictures, colored boxes, or with the incorrect sequences, is leading to failure in authentication.

## 3. Memorability Test

Robustness of an authentication system is usually determined by these two factors: usability and security. In this paper, instead of concerning about security of Painting Album Mechanism, we are more interested in finding this mechanism’s usability, and this had been done by conducting a testing called memorability test. In this memorability test, two attributes were used for measuring this mechanism’s usability. The first attribute was the amount of time respondents had spent for recall theirs passwords. Meantime, second attribute was the number of attempt respondents had spent for each authentication. 30 respondents, who are the postgraduate students of Universiti Teknologi Malaysia, were participated in this testing. Each of them was asked to create few sets of passwords, and use them for authentications at alternate days for three times. Swipe Scheme was tested first at first stage of testing, which follows by Color Scheme, and lastly Scot Scheme. Results of these memorability tests are presented in following sections.

### 3.1. Swipe Scheme Usability

In this memorability test, three input schemes were tested separately. The input scheme that tested first is Swipe Scheme. At this stage of memorability test, respondents had created 76 passwords with Swipe Scheme, and had used it for authentications. In Figure 1, it shows the average time respondents had spent on authentications.

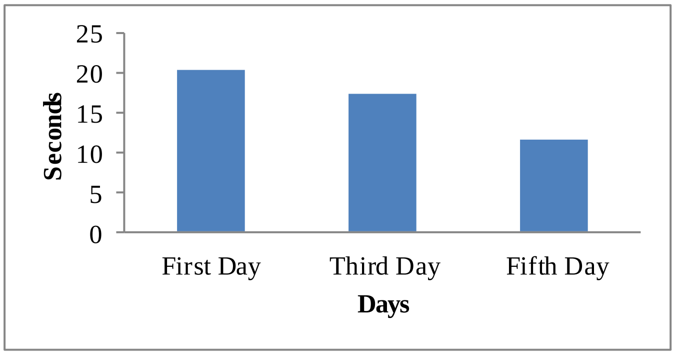

**Figure 1. Swipe Scheme Mean Time in Authentication**

As depicted in Figure 1, average time respondents had spent on authentications was about 20 seconds at the first day. Meanwhile, at third day, average time spent on authentications was decrease to 16 seconds. Lastly, at the fifth day, respondents had succeeded on authentication within 10 seconds. Results have proved respondents' learnability towards this Swipe Scheme is high, since respondents were able to master this input scheme, and they were still able to recall theirs passwords after couple of days.

### 3.2. Color Scheme Usability

At second stage of memorability test, respondents had produce 60 sets of passwords, to test on Color Scheme's usability. The average time that respondents had spent on authentications was presented in Figure 2.

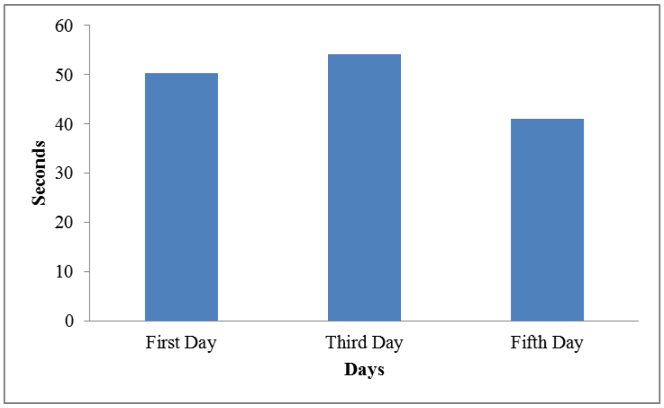

**Figure 2. Color Scheme Mean Time in Authentication**

As shown in Figure 2, respondents had spent about 50 seconds on authentications, when Color Scheme was introduce to them. At third day, average time spent on authentications was increase, by which they had took more than 50 seconds on authentications. At fifth day, the average of time taken on authentications was decrease, which result was showing that respondents had to spend about 40 seconds on authentications. According to observation, we found that most respondents dislike this input scheme. They had complained a lot about this proposed Color Scheme, and saying this input scheme is much more complex than previous Swipe Scheme. This has explained why most respondents were facing difficulty in learning this input scheme, and remembered theirs passwords.

### 3.3. Scot Scheme Usability

At final stage of memorability test, respondents had created 41 sets of passwords with the proposed Scot Scheme. These 41 sets of passwords had been used on authentications, and the average time that they had took for each authentication was presented in Figure 3.

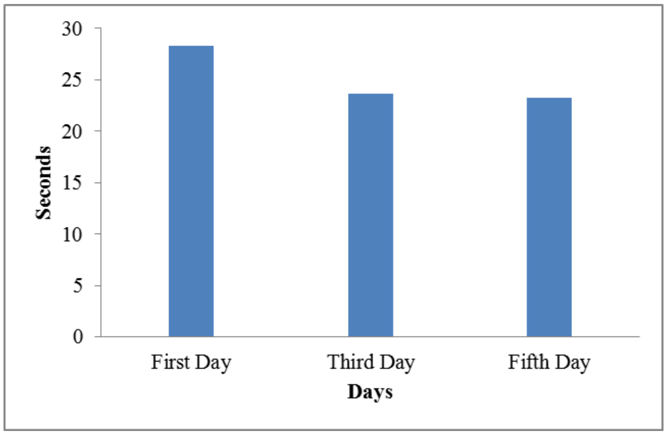

**Figure 3. Scot Scheme Mean Time in Authentication**

As depicted in Figure 3, at first day, respondents had taken about 27 seconds on authentications. At third day, the average time spent on authentications was reduce, which was about 23 seconds. At fifth day, the average time respondents had spent on authentication was continuing decrease to 22 seconds only. Result of this memorability test shows respondents was having difficulty in learning Scot Scheme, when this input scheme was introduced to them for the first time. However, this did not mean this input scheme is difficult to them. This has been proved from result above, by which time spent on authentications was continuously decrease from first to fifth days.

### 3.4. Extended Memorability Test Results

At this section, usability of Swipe Scheme, Color Scheme, and Scot Scheme were further validated, by measurement the number of attempts that respondents had took on each authentication. In Table 2, results of this extended memorability test were shown.

**Table 2. Mean attempt(s) taken for authentication**

| Input Schemes | Mean Attempt(s) |
|---|---|
| Swipe Scheme | 3 out of 76 trials |
| Color Scheme | 1 out of 60 trials |
| Scot Scheme | 1 out of 41 trials |

According to data collected, we found that each respondent needs about three attempts for succeed on authentication, when they choose to had Swipe Scheme as the input method. Meantime, for Color Scheme and Scot Scheme, respondents were usually able to log-in within one attempt. Despite the fact that the number of passwords that respondents had used for evaluating Swipe, Color, and Scot Schemes' usability is different, results showing that Color Scheme and Scot Scheme were more usable than Swipe Scheme. Moreover, there were respondents, who were failing to remember theirs passwords, when the tested input schemes were Swipe Scheme and Color Scheme. However, in Scot Scheme's memorability test, there were no failures in passwords memorization.

## 4. Discussion

It is not a fresh news that graphical password is inherently vulnerable to shoulder surfing attacks. Although there might be some opinions that graphical password in mobile device does not need any protection from an anti-shoulder surfing mechanism. As mention early, the fact is, graphical passwords in mobile device still need protection from anti-shoulder surfing mechanism, as others graphical password schemes.

To protect graphical password from shoulder surfing attack, techniques such as: providing large collection of pictures (in Triangle and Intersection Scheme); randomizing the pictures in graphical password scheme (in RGGPW Scheme); or having multi authentication methods in an authentication system (in S3PAS Scheme), are usually used. Experiment had proved these mechanisms are effective in preventing shoulder surfing attack. But, problem is these mechanisms could be a burden to users, and mobile devices with low specification. Users might not able to remember theirs password from a complicated authentication system. At the same time, those low specification mobile devices might not able processed complicated tasks of those authentication systems. Thus, in this paper, we proposed this Painting Album Mechanism, by which its processes of registration and authentication are memorable to users, meantime, suitable for mobile devices. We have successfully achieving these objectives by using human behaviors as our mechanism's input methods, while assuring this authentication system is in small size, and is needs no support from advanced technology.

Although Painting Album Mechanism's security from shoulder surfing attack is still undefined at this moment, however, the memorability test had told this Painting Album Mechanism's usability. In this memorability test, Painting Album Mechanism's input schemes were tested separately. Swipe Scheme was the first input scheme that was tested. Regarding this input scheme, steps involve in registration and authentication is simple. However, results shown this input scheme are not easy to learn. This is because respondents able to recall his password fast, but were not able log-in easily. For Color Scheme, it is in the opposite. Respondents agreed that password produced by Color Scheme was difficult to recall, but this input scheme is easy to learn. Lastly, for Scot Scheme, result from the test shown this input scheme is simple in term of password memorability, and it is simple to learn. After comparing the results of these memorability tests, we conclude that Scot Scheme is the most usable input scheme, which follows by Swipe Scheme, and lastly Color Scheme.

However, the memorability test conducted only involved the proposed Painting Album Mechanism only. Whether this mechanism is usable than the others existing mechanisms, or vice versa, is unknown. Thus, there is a suggestion to has another memorability test to compare usability of those existing mechanisms and Painting Album Mechanism by using the methodology. At the same time, it is believed this Painting Album Mechanism is still not usable as native mobile device graphical password, those mobile device graphical passwords that without the anti-shoulder surfing mechanism. This is because users still have to go through those input schemes that a little complex and confusing.

No matter what, at this moment, we conclude that Painting Album Mechanism is considers usable. This is because respondents, who had participated in the memorability test, were able to recall their password, and had succeeded in authentication under acceptable range of time.

## 5. Conclusion

In this paper, an effort to improve mobile device graphical password's security towards shoulder surfing mechanism was made by proposing an anti-shoulder surfing mechanism called Painting Album Mechanism. Although this mechanism's security from shoulder surfing attack still unidentified, however, results from the memorability test had told this mechanism is usable. Respondents were able to recall theirs passwords under acceptable duration of time, and they were fast in learning this mechanism, were the good proves for this conclusion. Besides this, we suggest having further tests on this mechanism, like comparing performance of those existing mechanisms with Painting Album Mechanism, or tests this Painting Album Mechanism with larger sample size. For instance, conduct this experiment with the longer duration, instead of just five days per person. Last but not least, in future, it is our plan to conduct an experiment to verify effectiveness of this Painting Album Mechanism's in securing graphical password in mobile device from shoulder surfing attack. At the same time, we are trying to obtain communities' feedback towards this mechanism by having a survey.

## Appendix

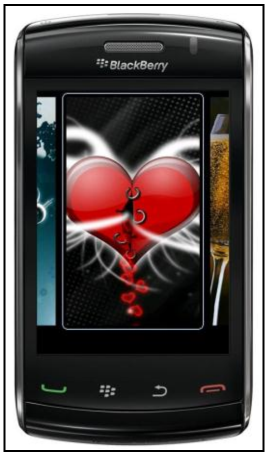

**Figure 4. Painting Album Mechanism in Blackberry Storm 2**

## Acknowledgement

This research is support by Universiti Teknologi Malaysia GUP grant, with vote number Q.J130000.2526.01J52.

## References

[1] J. Thorpe and P. C. Van Oorschot, “Towards Secure Design Choices for Implementing Graphical Passwords”, Proceedings of the 20th Annual Computer Security Applications Conference (ACSAC ’04), IEEE Computer Society, **(2004)**, Washington, DC, USA, pp. 50-60.

[2] X. Liu, “A Novel Cued-recall Graphical Password Scheme”, Sixth International Conference on Image and Graphics (ICIG), **(2011)**, August 12th – 15th, pp. 949-956.

[3] F. Monrose, M.K.R. “Graphical Password.” //adrem.ua.ac.be/sites/adrem.ua.ac.be/files/chapter9-gp.pdf, (**2011**) July 19th.

[4] N. H. Zakaria, S. Brostoff and J. Yan, “Shoulder Surfing Defence for Recall-based Graphical Passwords”, Proceedings of the Seventh Symposium on Usable Privacy and Security, **(2011)**, Pottsburgh, Pennsylvania. pp. 1-12.

[5] T. -Y. Chang, C. -J. Tsai and J. -H. Lin, “A Graphical-based Password keystroke Dynamic Authentication System for Touch Screen Handheld Mobile Devices”, International Journal of Systems and Software, vol. 5, no. 85, **(2012)**, pp. 1157-1165.

[6] B. Hoanca and K. Mock, “Secure Graphical Password System for High Traffic Public Areas”, Proceedings of the Symposium on Eye Tracking Research & Applications, **(2006)**, New York, USA, pp. 35-35.

[7] S. Brostoff and M. A. Sasse, “Are Passfaces More Usable than Password? A Field Trial Investigation”, Proceedings of HCI, **(2000)**, pp. 1-20.

[8] I. Nazir, “User Authentication for Mobile Device through Image Selection”, First International Conference on Networked Digital Technologies, **(2009)**, pp. 518-520.

[9] T. Perkovic, and M. Cagalj, “SSSL: Shoulder Surfing Safe Login”, International Conference on Telecommunications & Computer Networks, **(2009)**, pp. 270-275.

[10] P. Shi, B. Zhu and A. Youssef, “A PIN Entry Scheme Resistant to Recording-Based Shoulder Surfing”, International Conference of Emerging Security Information, Systems, and Technologies, **(2009)**, pp. 237-241.

[11] A. H. Lashkari and S. Farmand, “A Survey on Usability and Security Features in Graphical User Authentication Algorithms”, International Journal of Computer Science and Network Security, vol. 9, no. 9, **(2009)**.

[12] L. Sabrado and J. Birget, “Graphical Password. The Rutgers Scholar”, **(2002)**. Rutgers Universiti, Camden New Jersey 081024.

[13] H. Gao, X. Liu, R. Dai, S. Wang and X. Chang, “Analysis and Evaluation of the ColorLogin Graphical Password Scheme”, Proceedings of the Fifth International Conference on Image and Graphics, **(2009)**.

[14] P. -L. Lin, L.-T. Weng and P.-W. Huang, “Graphical Passwords Using Images with Random Tracks of Geometric Shapes”, Proceedings of Image and Signal Processing Congress, **(2008)**, pp. 27-31.

[15] L. K. Seng, N. Ithnin and H. K. Mammi, “Identifying the Reusability of Triangle Scheme and Intersection Scheme on Mobile Device”, International Journal of Computer and Information Science, vol. 4, no. 4, **(2011)**.

[16] L. K. Seng, N. Ithnin and H. K. Mammi, “User’s Affinity of Choice: Features of Mobile Device Graphical Password Scheme’s Anti-Shoulder Surfing Mechanism”, International Journal of Computer Science Issues, vol. 2, no. 8, **(2011)**.

[17] M. D. H. Abdullah, N. Ithnin and H. K. Mammi, “Grapical Password: User’s Affinity of Choice-An Analysis of Picture Attribute Selection”, International Symposium on Information and Technology, **(2008)**, pp. 1-6.

## Authors

**Lim Kah Seng** is currently a M.Sc candidate in Department of Computer System and Communications, Faculty of Computer Science and Information Systems at Universiti Teknologi Malaysia, Johor, Malaysia. He received B.Sc degree of Science (Computer Science) from Universiti Teknologi Malaysia in 2009. His research interests include computer security, authentication, and mobile applications.

**Dr. Norafida Ithnin** is a senior lecturer at Universiti Teknologi Malaysia. She received her B.Sc degree in computer science from Universiti Teknologi Malaysia in 1995, her M.Sc degree in Information Teknologi from University Kebangsaan Malaysia in 1998 and her PHD degree in computer science from UMIST, Manchester in 2004. Her primary research interests are in security, network, Mobile ad-hoc networks, Vehicular Ad Hoc Networks.

**Hazinah Kutty Mammi** is a lecturer at Universiti Teknologi Malaysia. She received her B.Sc degree in computer science from Universiti Teknologi Malaysia in 1997, her M.Sc degree in computer science from University of Essex, United Kingdom in 1998. Her primary research interests are in authentication, risks, policies, forensics, and education.