Information & Computer Security

Evaluating the effect of multi-touch behaviours on Android unlock patterns

Weizhi Meng

Evaluating the effect of multi-touch behaviours on Android unlock patterns

Weizhi Meng
Department of Computer Science, City University of Hong Kong, Hong Kong and Infocomm Security Department, Institute for Infocomm Research, Singapore

Received 9 December 2014
Revised 7 March 2015
24 March 2015
Accepted 30 March 2015

Abstract

Purpose – This paper aims to evaluate the effect of multi-touch behaviours on creating Android unlock patterns (AUPs) by realising that users can perform more actions in touch-enabled mobile phones.

Design/methodology/approach – The author conducted two user studies with a total of 45 participates and performed two major experiments in the main user study.

Findings – The user study indicates that the multi-touch behaviours can have a positive impact on creating patterns; however, there are only nine touchable points for the original AUPs, which may reduce the usability when performing a multi-touch movement.

Research limitations/implications – An even larger user study could be conducted to further analyse the patterns generated by users, that is, to analyse the specific password space by integrating the behaviours of multi-touch and to involve more types of multi-touch behaviours in creating an AUP.

Practical implications – This work explores the effect of multi-touch movement on creating AUPs. The results should be of interest for software developers and security researchers for exploring the effect of multi-touch behaviours on the creation of graphical passwords on mobile phones.

Originality/value – The author conducts two user studies with a total of 45 participants to investigate the impact of multi-touch behaviours on creating AUPs. In addition, to address the issue of usability, the author proposes two ways: increasing the number of touchable points and improve the rules of pattern creation.

Keywords Graphical password, Android unlock patterns, Mobile security, User authentication

Paper type Research paper

1. Introduction

User authentication is an important topic regarding computer and network security. Currently, the most commonly used method for user authentication is called text-based password in which users are required to input their own user names and text passwords for authentication. But, previous research work (Yan *et al.*, 2004) has shown that text-based passwords suffered from both security and usability problems. For example, users are likely to choose short and simple strings for easy memorisation. SplashData's list of frequently used passwords shows that the worst password of 2013 is "123456" (SplashData, Inc, 2013).

I would like to thank all participants for their hard work in the user study and all anonymous reviewers for their helpful comments in improving this article.

Information & Computer Security
Vol. 24 No. 3, 2016
pp. 277-287
© Emerald Group Publishing Limited
2056-4961
DOI 10.1108/ICS-12-2014-0078

In order to address these issues of traditional text-based authentication, graphical passwords (GPs) have been developed as an alternative to text-based authentication. Some psychology studies such as Nelson *et al.* (1976) have already pointed out that human brain is better at remembering and recognizing images than text (e.g. digital strings). An important assumption here is that through reducing the memory burden, users are more likely to produce more secure passwords by means of images than text (i.e. GP-based scheme can offer a larger password space).

Currently, with the increasing popularity of mobile phones, users are likely to store a lot of sensitive information (e.g. credit card numbers and passwords) on their mobile phones (Karlson *et al.*, 2009) and to use their phones for security sensitive tasks (e.g. authorizing commercial transactions) because of their fast data connection and wireless connectivity (Dunphy *et al.*, 2010). Thus, it is very crucial to develop a powerful user authentication mechanism for mobile phones in authenticating legitimate users and detecting imposters.

1.1 Motivations

Several GP-based applications have been proposed on mobile phones, such as Android unlock patterns (AUPs), which is a revised version of Pass-Go (Tao and Adams, 2008) on the Android platform. It allows users to input correct unlock patterns to unlock their Android screen. In our previous work (Meng *et al.*, 2013), we identified that users could use more actions like multi-touch in creating GPs on a touch-enabled mobile phone than on a keyboard-based computer.

More specifically, our previous work (Meng *et al.*, 2013) conducted a specific case study on click-draw-based GP scheme (Meng, 2012), which aims to combine the existing input types of creating a GP. The experimental results with 60 participants indicated that the behaviour of multi-touch can improve the performance of creating a click-draw-based GP. As AUPs are very popular on Android phones, in this paper, the motivation is, therefore, to conduct further experiments and to explore the effect of multi-touch behaviours on creating AUPs.

1.2 Contributions

In this paper, based on our previous work (Meng *et al.*, 2013), I attempt to conduct a case study associated with AUPs to further investigate the effect of multi-touch behaviours on creating GPs. The contributions of this work can be summarized as follows:

- I begin by introducing the types of multi-touch behaviours on mobile phones and describing my target multi-touch action in the evaluation. I then analyse the potential impact of multi-touch behaviours on creating an AUP and compare different rules of multi-touch-enabled AUPs.
- To evaluate the effect, I mainly conduct two experiments with the same 45 participants. Through collecting and analysing the feedback, I identify that the multi-touch behaviour would make a positive effect on creating an AUP, but its usability may be restricted because of the lack of touchable points (i.e. only nine dots for AUPs).

The rest of this paper is organized as follows. Section 2 introduces the types of multi-touch behaviours on a touch-enabled mobile phone and presents the selected multi-touch action in the evaluation. Section 3 briefly analyses the potential impact of multi-touch on creating an AUP. Section 4 presents and analyses the user study with detailed implementation and received feedback. Section 5 reviews some related work. Finally, Section 6 concludes the paper and points out future directions.

2. Types of multi-touch

Nowadays, multi-touch is becoming a distinguished feature on touch-enabled mobile phones such as Android phones and iPhones in which users can touch the screen with multiple fingers at the same time, that is, enlarge web page or map site. Generally, touch behaviours on a mobile phone can be classified as single-touch, multi-touch and touch movement (Meng *et al.*, 2012):

- *Single-touch*: The input starts with a touch press down, followed by a touch press up without any movement in between.
- *Touch movement*: The input starts with a touch press down movement (also called drag), followed by a touch press up. In practical use, a touch movement can be included in either one-finger gestures or multi-touch gestures (e.g. scroll, pinch and rotate).
- *Multi-touch*: An input with two or more simultaneous distinct touch press down events at different coordinates of the touch screen (i.e. two fingers press down on the touch screen simultaneously) either with or without any movement before a touch press up event.

AUPs is an Android authentication application which requires users to unlock their phones by inputting the correct patterns. Figure 1 presents two specific cases of AUPs based on Berkeley Churchill (2013) and an Android simulator. It is visible that users can create an AUP by means of a touch movement on a 3 × 3 touch platform (with a total of nine touchable points). During the input, a touch movement should be completed without any touch press up. When finishing a touch movement, AUPs will compare the current input to its stored patterns.

To create a valid AUP, three major rules should be considered as below (Uellenbeck *et al.*, 2013):

(1) A valid pattern cannot use a dot more than once, as it is virtually removed after selection. For instance, on the left side of Figure 1, the touchable Dot 5 will not be counted during backward touch movement from Dot 6 to Dot 7.

(2) At least four dots must be chosen, and only straight lines are allowed for a valid pattern.

(3) It is not possible to create a line using three dots, without selecting the middle one, unless the latter has been previously visited.

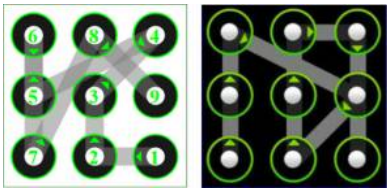


Figure 1.
Two cases of AUPs

2.1 Our targeted behaviour

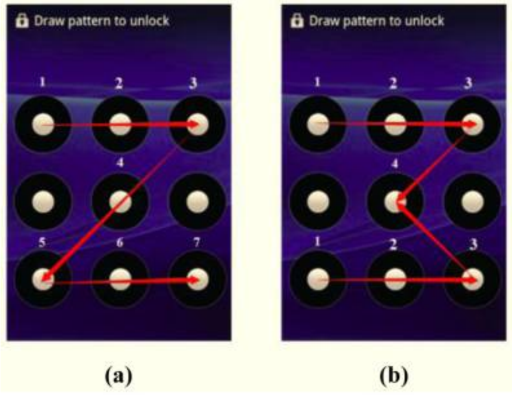
To evaluate the effect of multi-touch behaviours on creating an AUP, in this work, I mainly consider and allow completing a multi-touch movement with two fingers. Intuitively, by means of two fingers, AUPs can be generated in a different way. For example, two touchable points can be selected at the same time by using two fingers. In the next section, I will discuss the potential impact of using two fingers on creating AUPs.

3. Potential impact

In our previous work (Meng *et al.*, 2013), we identified that by integrating the multi-touch with only two fingers, the password space of click-draw-based GP can be further enlarged by K*i*!/2! times in the best cases, where K*i* means there are totally *i* clicks on a selected image. According to these observations, it is understandable that the action of multi-touch (a touch movement using two fingers) can offer a different way in creating anAUP.

In Figure 2, I show an example to illustrate the potential impact of multi-touch on creating AUPs. Figure 2(a) presents an AUP of "Z" with one finger, and the touch sequence can be represented as {1,2,3,4,5,6,7}. Note that each touchable point of the completed image "Z" is selected for one time. To draw this "Z" image with the same points, if we use a two-finger based touch movement, we can generate it with a sequence such as {multi-touch{(1,2,3), (1,2,3)}, {4}} as shown in Figure 2(b). That is, we can move two fingers to draw a sequence of {1,2,3} at one time and both back to {4}. Note that it is definitely different to generate AUPs by using one finger and two fingers, so we should consider that the patterns are similar if the same points are selected for constructing a secret. Thus, the drawing in Figure 2(b) does not look like "Z", but we consider these patterns are similar because of the same selected points. This simple example shows that to complete a similar pattern, multi-touch by means of two fingers can offer more chooses than using only one finger.

Overall, we can imagine that by using two fingers, more types of patterns could be generated. For a certain pattern, there would be different ways to generate. In other words, multi-touch behaviours can be used to improve the password space of original AUPs. However, because of different rules of generating a valid pattern, the specific calculation of



(a)

(b)

Figure 2.
Example: the potential impact on creating AUPs by means of two fingers

Notes: (a) "Z" shape drawn by one finger;
(b) "M" like shape drawn by two fingers

password space would be different. For instance, let us consider two sets of rules (named Rule sets A and B), which are modified based on the original AUPs' rules as follows.

(1) *Rule set A*:
   - A valid pattern cannot use a dot more than once, but one dot can be selected by a multi-touch movement at the same time.
   - At least four dots must be chosen, and only straight lines are allowed for a valid pattern.
   - It is not possible to create a line using three dots, without selecting the middle one, unless the latter has been previously visited.

(2) *Rule set B*:
   - A valid pattern can use a dot more than once, that is, it will not be virtually removed after selection.
   - At least four dots must be chosen, and only straight lines are allowed for a valid pattern.
   - It is not possible to create a line using three dots, without selecting the middle one, unless the latter has been previously visited.

3.1 Discussions

The major difference between Rule sets A and B is whether a dot can be selected more than once. It is easily understandable that the password space of Rule set B is greatly larger than that of Rule set A, as a dot can be reselected many times. In this case, the Rule set B would result in a longer and more complex pattern. Then, the password space can be ranked as: AUP (Rule set B) > AUP (Rule set A) > AUP (origin). Because of its complexity, I leave the concrete calculation of password space as our future work.

4. User study

In this section, I describe the implementation details, present two user studies with the same 45 participants and analyse the received feedback.

4.1 Implementation

Based on our previous work (Meng *et al.*, 2013), I utilise a Google/HTC Nexus One Android phone with a multi-touch capacitive touch screen (resolution 480 × 800 px) to collect raw data of touch movements.

The major advantage of using this particular phone is that its stock Android operating system (OS) can be replaced with a self-modified customized Android OS version. Specially, I updated the phone with a modified Android OS version 2.2 based on CyanogenMod. The modification consists of changes to the application framework layer to record raw input data from the touch screen, such as the timing of touch inputs, the coordinates x and y, the types of the input (e.g. press down and press up) and the touch pressure. In addition, I installed a separate application that enables to easily extract the recorded data from the phone[1].

4.2 The minor user study

This study was conducted before our main user study, attempting to obtain feedback for the two rule sets and offer participants more practice trials to get familiar with the phone and the multi-touch-enabled AUPs.

I implement both Rule sets A and B into multi-touch-based AUPs and allow all participants to have five practice trials for each rule set. After that, I require each participant to give their preference. The preference results are shown in Table I. It is visible that 37 out of 45 participants prefer Rule set B, whereas only 8 participants would like to apply Rule set A. I informally interviewed all participants and found that most participants consider Rule set B is more convenient, as they can reuse dot in creating a valid pattern. The benefit of reselecting a dot is the capability to create a more complicated pattern, which is harder to be compromised. In contrast, the pattern would be relatively simpler if applying Rule set A.

According to the feedback results above, in the main user study, I decide to apply Rule set B by providing better usability in which users can reselect a dot more than once.

4.3 The main user study

In the evaluation, I conducted an in-lab user study, which consisted of two major experiments with totally 45 participants. All participants are volunteers in the study with diverse backgrounds including students, engineers, businessmen and senior people. All participants are regular mobile phone users and in age range from 18 to 50 years. The detailed information of participants is shown in Table II.

4.3.1 Multi-touch-enabled AUPs. This condition allows users to create a valid pattern by means of two-finger-based movements. The touch movement should be completed without touch press up.

In the user study, I introduced the objectives of the user study and gave a detailed description of how the system logs its inputs. Every participant can additionally complete two practice trials for each scheme to get familiar with the platforms before he/she starts to complete his/her real trails. The detailed steps of these two experiments are described as follows:

(1) *Experiment 1:* Each participant can create five patterns using one finger on the original version of AUPs.
   - Step 1: AUP creation;
   - Step 2: AUP confirmation; and
   - Step 3: feedback.

Table I. The preference of rule set by participants

Rule set A	Rule set B
8	37

Table II. Participants' information

Age range (years)	Male	Female
18-30	12	13
30-40	9	6
40-50	3	2

All participants are required to complete a feedback form about the password creation and confirmation.

(2) *Experiment 2:* Each participant can freely create five patterns using two fingers based on the multi-touch-enabled AUPs.

- Step 1: AUP creation;
- Step 2: AUP confirmation; and
- Step 3: feedback.

All participants are required to complete a feedback form about the password creation and confirmation.

4.3.2 Feedback analysis. Ten-point Likert scales were used in each question, where score of 1 indicates strong disagreement and 10 indicates strong agreement. Several collected questions and scores are shown in Table III.

Based on the first two questions, it is noticeable that participants can create an AUP easily using both one finger and two fingers. It is noted that the score of using one finger is a bit better than the score of using two fingers. Some participants argue that they may be more familiar to create an AUP using one finger than two fingers.

In contrast, regarding the third and fourth questions, the score of the latter (8.8) is much higher than that of the former (7.6). Most participants feel that they can create a more secure AUP by means of multi-touch behaviours. Regarding the last two questions, most participants indicate that they prefer to use multi-touch in creating AUPs, whereas the score of the opposition is only 3.2.

Although most participants prefer the multi-touch, several participants point out that the number of touchable points in AUPs is not enough; they could not perform the touch movement freely by means of two fingers. By contrast, participants did not encounter this issue in our previous work on the click-draw-based GPs (Meng *et al.*, 2013). This is a reason why the score of the second question is lower than the first one. Through comparing these observations, I conclude that the effect of multi-touch behaviours will be affected by specific GP schemes.

4.3.3 Preliminary pattern analysis. After collecting the patterns during the experiments, I compute the average number of selected touchable points under these two experiments:

(1) *Experiment 1*: Using one finger.

(2) *Experiment 2*: Using two fingers (multi-touch).

The results are presented in Table IV. It is worth noting that under the second situation, a dot can be selected more than once as long as a touch movement touches it.

Question	Average score
1. I could easily create an AUP in Experiment 1	9.0
2. I could easily create an AUP in Experiment 2	8.5
3. I believe that my AUPs are different from others in Experiment 1	7.6
4. I believe that my AUPs are different from others in Experiment 2	8.8
5. I prefer to use multi-touch	8.6
6. I do not prefer to use multi-touch	3.2

Table III. Several questions and relevant scores

In Table IV, I compared the results of the average number of selected touchable points between Experiment 1 and Experiment 2. It is visible that users can generally choose more points in Experiment 2 than Experiment 1 (the difference is nearly two times in average). Intuitively, the bigger number of touchable points can increase the security of GPs, where attackers have to spend more time in cracking it. Actually, users can also create a valid pattern using fewer points, for example, the "Z" pattern as shown in Figure 2 that includes seven dots. Therefore, the preliminary pattern analysis validates that the multi-touch behaviour can have a positive impact on the creation of AUPs, as participants generally create patterns using more points.

4.3.4 Discussions. On the whole, based on the user studies, I identify that the multi-touch can have a positive effect on creating AUPs; however, the number of touchable points is not enough for the original AUPs. For example, fingers may tend to work in unison, and it is not easy to move freely (i.e. sharing the same start or end dot). Therefore, we consider that AUPs lack enough dots for multi-touch behaviours.

Moreover, I figure out that most participants in our studies have no problems in generating AUPs with two fingers. In this work, a multi-touch movement is valid as long as two fingers touch the screen at the same time, which means that one finger can move first, followed by another finger. I plan to conduct an even larger study to investigate this issue in future. The impacts can be summarized as follows:

- The multi-touch can increase the security of AUPs in that users would create more complicated patterns. Thus, attackers should spend much more time on cracking. For example, users may reselect some dots more than once, so it is very hard for attackers to decide the number of selected dots before cracking.
- From the feedback, I identify that the usability is an issue when using multi-touch movement on AUPs because there are only nine touchable points. Most participants feel it may reduce the usability of multi-touch-enabled AUPs. To address this issue, it is a promising way to increase the dots in AUPs or change its rules.

Actually, I improved the rules on AUPs by implementing Rule set B. If we use Rule set A (similar to simply apply multi-touch to original AUPs), the usability issue will be worse. Overall, the user studies provide useful and interesting views about the effect of multi-touch behaviours on the creation of AUPs. To further validate the results, more experiments should be conducted.

5. Related work

In general, GP schemes can be divided into three categories based on the input types: click-based, choice-based and draw-based GPs.

Regarding the click-based GPs, Blonder (1996) first designed a GP scheme in which that users could click on several pre-defined locations on an image. Wiedenbeck *et al.* (2005a) extended the above idea and proposed a PassPoints system in which users could click on any place on an image to create their passwords. They also analysed the effect

Table IV.
The average number of selected touchable points

Experiment 1: one finger	Experiment 2: two fingers (multi-touch)
6.7	11.8

of pixel tolerance [i.e. determining the minimum size of tolerance square; Wiedenbeck *et al.* (2005b)]. Chiasson *et al.* (2007) later proposed a scheme of Cued Click Points (CCP), where users could click on one point per image for a sequence of images. In the scheme of CCP, the next image was based on previous click point. Their analysis showed that CCP was more secure than PassPoints by increasing the number of images.

For the choice-based scheme, Passfaces (2013) was developed based on recognizing human faces, users select a number of images during the password creation phase, and identify pre-selected images from several decoys in the login phase. Then, Davis *et al.* (2004) implemented the above idea and proposed a story scheme in which users could choose everyday images instead of human faces in a correct order for authentication. For this scheme, users were encouraged to create their passwords like a story in helping them remember the order and the images.

For the draw-based scheme, Jermyn *et al.* (1999) proposed a draw-a-secret (DAS) scheme that allowed users to draw their own passwords on a two-dimensional grid. For authentication, users should redraw their pictures in the same sequence. Then, Lin *et al.* (2007) further proposed a qualitative DAS by using a directional change when the pen passes over a cell boundary.

In literature, many studies have evaluated the performance of AUPs. For example, De Luca *et al.* (2012) presented an implicit approach to improve authentication on current mobile devices such as AUPs. In particular, they added an invisible layer to the system, which examined users not only by the shape they input but also by the way they perform the input. Then, Andriotis *et al.* (2013) presented a pilot study on user habits when creating an AUP and on their perceptions regarding what constitutes a secure pattern. By successfully attacking a pattern using various physical attacks, they concluded that currently using an optical camera or a microscope is the best way to perform physical attacks and produce quality results.

Later, Uellenbeck *et al.* (2013) explored the security of AUPs through performing a large-scale user study. They measured actual user choices of patterns and found that there is a high bias in the pattern selection process, for example, the upper left corner and three-point long straight lines are very typical selection strategies. They further concluded that the security offered by the scheme is less than the security of only three-digit randomly assigned personal identification numbers (PINs) for guessing 20 per cent of all passwords. These studies above demonstrate that the security mechanism of AUPs should be greatly improved.

6. Conclusion and future work

In this work, I mainly attempt to evaluate the effect of multi-touch behaviours on creating AUPs. More specifically, as compared to a traditional one-finger-based touch movement, I target on a two-finger-based touch movement in creating AUPs (named multi-touch-enabled AUPs). In the evaluation, I conduct two user studies with a total of 45 participants: a minor study and a main study. The former examines users' preference of different rules, whereas in the latter, I analyse the results by collecting the received feedback from two specific experiments. The results provide useful information and indicate that the use of multi-touch can have a positive impact on creating AUPs. However, there are only nine touchable points for the original AUPs, which may reduce the usability when performing the multi-touch movement. To address this issue, it is a promising way to increase the number of touchable points or improve the rules.

This work is at its early stage, so there are many future directions which could include analysing the specific password space by integrating the behaviours of multi-touch and involving more types of multi-touch behaviours in creating an AUP. In addition, future work could include changing the rule set (i.e. allowing a line without touching the middle dot) and analysing the patterns generated by users to validate the practical effect of multi-touch actions on creating GPs (i.e. whether two fingers tend to work in unison or not). Moreover, future work could also include evaluating multi-touch-enabled AUPs under several attacks such as brute force attacks and shoulder surfing attacks.

Note

1. The modified Android OS version is available at: http://sourceforge.net/projects/touchdynamicsauthentication/files/

References

Andriotis, P., Tryfonas, T., Oikonomou, G. and Yildiz, C. (2013), "A pilot study on the security of pattern screen-lock methods and soft side channel attacks", *Proceedings of the 6th ACM Conference on Security and Privacy in Wireless and Mobile Networks (Wisec)*, *New York, NY*, pp. 1-6.

Berkeley Churchill. (2013), "Unlock pattern generator", available at: www.berkeleychurchill.com/software/android-pwgen/pwgen.php

Blonder, G. (1996), "Graphical passwords", United States Paten 5559961, Lucent Tech.

Chiasson, S., Van Oorschot, P.C. and Biddle, R. (2007), "Graphical password authentication using cued click points", *Proceedings of ESORICS, LNCS*, Vol. 4734, pp. 359-374.

Davis, D., Monrose, F. and Reiter, M.K. (2004), "On user choice in graphical password schemes", *Proceedings of the 13th Conference on USENIX Security Symposium*, *Berkeley, CA*, pp. 151-164.

De Luca, A., Hang, A., Brudy, F., Lindner, C. and Hussmann, H. (2012), "Touch me once and I know it's You!: implicit authentication based on touch screen patterns", *Proceedings of the 2012 ACM Annual Conference on Human Factors in Computing Systems (CHI)*, *Austin, Texas*, pp. 987-996.

Dunphy, P., Heiner, A.P. and Asokan, N. (2010), "A closer look at recognition-based graphical passwords on mobile devices", *Proceedings of the Sixth Symposium on Usable Privacy and Security (SOUPS)*, *ACM*, *New York, NY*, pp. 1-12.

Jermyn, I., Mayer, A., Monrose, F., Reiter, M.K. and Rubin, A.D. (1999), "The design and analysis of graphical passwords", *Proceedings of the 8th Conference on USENIX Security Symposium*, *Washington, DC*, pp. 1-14.

Karlson, A.K., Brush, A.B. and Schechter, S. (2009), "Can I borrow your phone?: understanding concerns when sharing mobile phones", *Proceedings of the 27th International Conference on Human Factors in Computing Systems (CHI)*, *ACM*, *New York, NY*, pp. 1647-1650.

Lin, D., Dunphy, P., Olivier, P. and Yan, J. (2007), "Graphical Passwords and qualitative spatial relations", *Proceedings of the 3rd Symposium on Usable Privacy and Security (SOUPS)*, *Pittsburgh, PA*, pp. 161-162.

Meng, Y. (2012), "Designing click-draw based graphical password scheme for better authentication", *Proceedings of the 7th IEEE International Conference on Networking, Architecture, and Storage (IEEE NAS)*, *IEEE*, *Xiamen, Fujian*, pp. 39-48.

Meng, Y., Li, W. and Kwok, L.F. (2013), "Enhancing click-draw based graphical passwords using multi-touch on mobile phones", *Proceedings of the 28th IFIP TC 11 International Information Security and Privacy Conference (IFIP SEC)*, *Springer*, *Heidelberg*, pp. 55-68.

Meng, Y., Wong, D.S., Schlegel, R. and Kwok, L.F. (2012), "Touch gestures based biometric authentication scheme for touchscreen mobile phones", *Proceedings of the 8th China International Conference on Information Security and Cryptology (INSCRYPT)*, *Springer*, *Heidelberg*, pp. 331-350.

Nelson, D.L., Reed, V.S. and Walling, J.R. (1976), "Pictorial superiority effect", *Journal of Experimental Psychology: Human Learning and Memory*, Vol. 2 No. 5, pp. 523-528.

Passfaces (2013), available at: www.realuser.com/

SplashData, Inc (2013), "Password unseated by '123456' on SplashData's annual worst passwords list", available at: http://splashdata.com/press/worstpasswords2013.html

Tao, H. and Adams, C. (2008), "Pass-go: a proposal to improve the usability of graphical passwords", *International Journal of Network Security*, Vol. 7 No. 2, pp. 273-292.

Uellenbeck, S., Durmuth, M., Wolf, C. and Holz, T. (2013), "Quantifying the security of graphical passwords: the case of android unlock patterns", *Proceedings of the 2013 ACM Conference on Computer and Communications Security (CCS)*, *New York, NY*, pp. 161-172.

Wiedenbeck, S., Waters, J., Birget, J.C., Brodskiy, A. and Memon, N. (2005a), "Passpoints: design and longitudinal evaluation of a graphical password system", *International Journal of Human-Computer Studies*, Vol. 63 Nos 1/2, pp. 102-127.

Wiedenbeck, S., Waters, J., Birget, J.C., Brodskiy, A. and Memon, N. (2005b), "Authen-tication using graphical passwords: effects of tolerance and image choice", *Proceedings of the 2005 Symposium on Usable Privacy and Security (SOUPS*), *New York, NY*, pp. 1-12.

Yan, J., Blackwell, A., Anderson, R. and Grant, A. (2004), "Password memorability and security: empirical results", *IEEE Security and Privacy*, Vol. 2 No. 5, pp. 25-31.

About the author

Weizhi Meng received his B.Eng. degree in Computer Science from the Nanjing University of Posts and Communications in 2009 and obtained his PhD degree in Computer Science from the City University of Hong Kong in 2013. He was previously known as Yuxin Meng and is currently a Research Scientist in Infocomm Security (ICS) Department, Institute for Infocomm Research, Singapore. Prior to this, he was employed by the CS Department, City University of Hong Kong as a Senior Research Associate. His research interests are information security including intrusion detection, mobile authentication security, web security, malware analysis, cloud computing and intelligent security applications. He is a member of the IEEE and ACM. Weizhi Meng can be contacted at: yuxin.meng@my.cityu.edu.hk