ISBN 978-981-11-7861-0
Proceedings of 2018 the 8th International Workshop on Computer Science and Engineering (WCSE 2018)
Bangkok, 28-30 June, 2018, pp. 610-617
doi: 10.18178/wcse.2018.06.102

A Study of Graphical Password Usability on Smartphones in a Week

Trust Ratchasan[1+], Rungrat Wiangsripanawan[1]

[1] Department of Computer Science, King Mongkut's Institute of Technology Ladkrabang, Bangkok, Thailand

Abstract. Smartphone technology nowadays is very progressive. With a powerful camera, high-speed connectivity, touchscreen interface, millions of different applications development and also a biometrics authentication system such as fingerprint scanner, iris scanner and even face scanner but whenever biometrics authentication system accidentally failed a smartphone still uses text passwords, PINs or Android's Unlock Pattern as a secondary authentication system but users typically create week text passwords since strong text passwords are difficult to recall and memorise. PINs and Android's Unlock Pattern are easier to recall and memorise but also having the guessablity problem. Graphical password system is one of the approach which propose of solving the memorability problem. In this paper we implemented and optimised the selected existing graphical password systems to smartphones and conducted an experiment to study and compare a usability of graphical password to the current secondary authentication system on smartphones in a week.

Keywords: user authentication, passwords, graphical passwords, usable security, human computer interaction.

1. Introduction

Biometrics authentication system on a smartphone became widespread and easily accessible. Even with high accuracy and easy for authentication but whenever biometrics authentication system is failed or unexpectedly unusable such as user's hands are too wet or the user wears personal protective equipments for example goggles, sunglasses or gloves a smartphone provides a secondary authentication system such as text password, PINs or Android's Unlock Pattern.

Text passwords are a common approach for authentication, but users normally create weak passwords and face a problem to memorise strong ones [1], [2]. Alternatively most of users prefer to use PINs and Android's Unlock Pattern as a secondary authentication system. On the other hand these authentication systems are even less secure than text passwords. Four digit PINs has only 16 bits of password space but also has very high usability for users. Android's Unlock Pattern is even easier to authenticate but has lower password space and higher guessability comparing to text passwords and PINs [3].

Graphical passwords have been proposed to solve the memorability problem based on the studies which indicated that humans are better at recognising and recalling images than texts of text passwords[4], [5], Some graphical passwords provide a high password space and against password guessing attacks that is equal to or greater than typical alphanumeric passwords, but also difficult to use such as low success rate and taking too long login time [6], there is a trade-off between usability and cryptographic strength.

In this paper we conducted an experiment to compare and evaluate usability of selected graphical password systems and PINs which is the most popular secondary authentication system in a smartphone with similar level of password strength (entropy), our study was conducted with 40 participants in a week. We developed and optimised an android application for studying participants use of selected graphical password

+ Corresponding author. Tel.: +66922733035; fax: +6623298412..
E-mail address: 58605087@kmitl.ac.th.

systems and PINs. Participants downloaded and installed the application from an email, Each user created their personal account and created one password for each graphical password scheme and used them daily in a week.

2. Graphical Password Systems

Graphical passwords are image-based passwords which are an authentication system that works by having the user select images or points of the image. They are an alternative way of solving the problem of using alphanumeric passwords [1], [2]. Graphical passwords are easier than text passwords for most people to remember [4], [5]. A study by Robert Biddle *et al*. [6] classifies and compares stereotype of graphical passwords which are Recall-based System, Recognition-based System and Cued-recall System.

2.1. Recall-based graphical password systems

Recall-based graphical password systems are also known as drawmetric systems which allows users to create passwords from drawing lines or points on empty spaces or a grid. This type of graphical password is the most difficult system to memorise since users must remember all lines without any memorisation aid. Examples of recall-based graphical password systems are Draw-a-Secret (DAS) [7], BDAS [8] and YAGP [9].

2.2. Recognition-based graphical password systems

Recognition-based graphical password systems are also known as cognometric systems or searchmetric systems. The system require users to select a set of images to create a password, then user must recognise their images from among decoys to log in, The images used are mostly people's faces, pictures, artwork and biographies. Examples of recognition-based graphical password systems are Use Your Illusion (UYI) [10] and Déjà vu [11].

2.3. Recognition-based graphical password systems

Cued-recall graphical password systems are also known as locimetric which require user choose positions or points of an image during password creation and authentication, subjects are given hints (cues) at the time of recall. The cues are supposed to help the subject recalls the memorised items. Examples of cued-recall graphical password systems are PassPoints [12] and Inkblot Authentication[13].

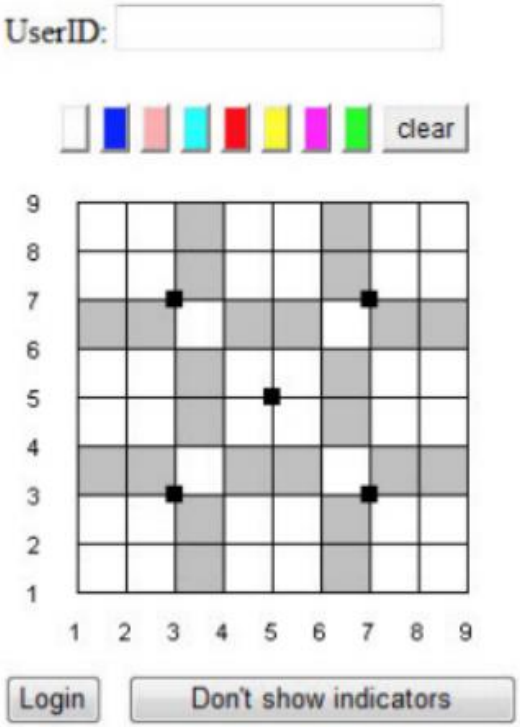


Fig. 1: User interface of PassGo

3. Related Work

3.1.PassGo

Pass-Go (Fig. 1) is a graphical password system proposed by Tao and Adams [14] which solves the Draw-a-Secret (DAS) [7] scheme issue: the difficulty of accurately duplicating sketches whose lines cross near grid lines or grid line intersections. It is named by the ancient board game Go, Pass-Go displays a grid of 9 x 9 dots and users draw their lines or points using grid intersection points. Each user's movements are snapped to gridlines and intersections, avoiding the effect of small variations in the trace. The theoretical password space of Pass-Go is larger than for DAS and PINs due to a finer grid (more squares); allowing diagonal movements (DAS encodes only horizontal and vertical movements); both resulting in greater password complexity than in DAS.

3.2.PassFaces

PassFaces is a graphical password system proposed by S.Brostoff, and M. A. Sasse [15]. The basic idea is as follows. The user will be asked to choose four images of human faces from a face database as their future password. In the authentication stage, the user sees a grid of nine faces, consisting of one face previously chosen by the user and eight decoy faces. The user recognises and clicks anywhere on the known face. This procedure is repeated for several rounds. The user is authenticated if he/she correctly identifies the four faces. The technique is based on the assumption that people can recall human faces easier than other pictures. The previous studies [16], [17] have shown that PassFaces are very memorable over long period.

3.3.PassPoints

PassPoints is a cued-recall graphical password systems which proposed by S. Wiedenbeck, J. Waters, J. Birget, A. Brodskiy, and N. Memon [12]. A password is a sequence of any n = 5 user selected click points (pixels) on a system-assigned image. The user selects points by clicking on them using a mouse. During login, re-entry of the click-points must be in the correct order, and accurate within a system-specified tolerance. The image acts as a memory cue to the location of the originally chosen click-points.

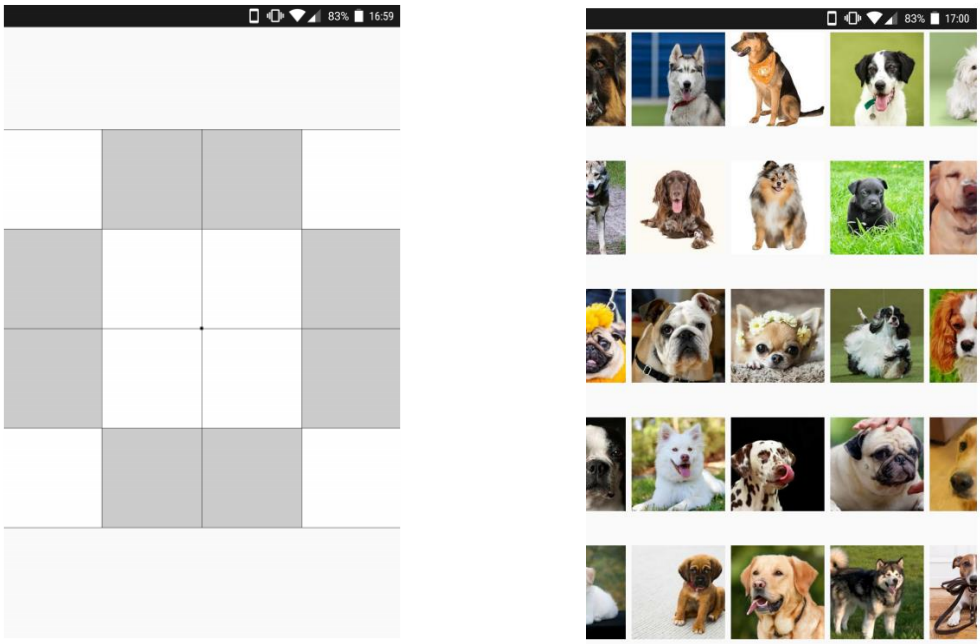
4. Experiment

4.1.Entropy Settings and Optimisations

We developed and optimised an android application as a prototype. In the following section we mentioned that we chose Pass-Go, PassFaces and PassPoints for the experiment. For PassGo it normally displays as 9 x 9 dots with multiple pen colours but for our optimisation to enhance the system more appropriate for a smartphone display size (typical smartphone display size is around 4.5" - 5.5") we scaled down a grid size to 5 x 5 (Fig. 2(a)) and remove an ability to select multiple pen colours, The theoretical password space of optimised Pass-Go is around 28 bits which is equivalent to six-character text password consisting of numbers, lowercase, and uppercase characters which is more secure than 6 digit PINs that has the theoretical password space around 20 bits.

PassFaces, The original PassFace settings had n = 4 rounds of P = 9 images per panel, with one image per panel from the set of images. The user portfolio contains exactly 4 faces, so all portfolio images are used during each login. The theoretical password space for PassFaces has cardinality P powered n, with P = 9, n = 4 yielding 6561, is around 13 bits. We optimised by increasing image per panel to 50, P = 50 and changed the number of rounds to 5, n = 5 (Fig. 2(b)) then the theoretical password space is increased to 28 bits which is equivalent to six-character text password consisting of numbers, lowercase, and uppercase characters and equivalent to optimised Pass-Go, We also did some optimisation to improve users recalling images and more user friendly by changing human faces to dog and puppy faces and for each image has its own uniqueness.

PassPoints, the original PassPoints uses click-based system and the theoretical password space was calculated by number of points(pixels) powered by a password is a sequence (n = 5) that is around 43 bits, but for a smartphone display which has smaller size than a computer display and it is also a touchscreen interface. Hence, we increased an area of tapping point on a smartphone display and the optimised theoretical password space is calculated by number of point which is 50, P = 50 and a sequence is 5, n = 5 then P powered by n is around 28 bits which is equivalent to six-character text password consisting of numbers, lowercase, and uppercase characters.



(a) (b)

Fig. 2: (a) User Interface of optimised Pass-Go (5 x 5 grid) on an android device. (b) User Interface of optimised PassFaces on an android device.

4.2.Experiment

We recruited 40 participants to involve the experiment, these participants (16 female and 24 male , age 23 - 35) are from the software development company where one of the researcher is currently working with. We assigned each participant to every optimised graphical password systems and 6 digits PINs. 83.33% of participants use pin as a secondary authentication system, 10% of participants use Android's Unlock Pattern as a secondary authentication system while the rest (6.66%) use text passwords as a secondary authentication system.

The experiment conducted at the company after working hour everyday during a week, initially at the first day users were introduced and well trained how to use the optimised graphical password systems. The participants were required to create the passwords at the first day. Afterwards, users were required to login with the initial passwords in each day. In the first day and the last day we also did the Lewis' Post-Study System Usability Questionnaire (PSSUQ) to participants [18] In the section 4.1 we set up and optimised password entropy and the selected graphical password systems have the similar theoretical password space which is 28 bits which make us easily compare and evaluate the data to 6 digits PINs.

We evaluate ease of graphical password systems access using four complimentary measures: (1) error rate of clicking incorrect points, (2) number of attempts required for successful authentication and (3) the login time required in a successful authentication.

5. Results

5.1.Error Rate

Error rate is the average rate of clicking incorrect points by all participants. Table 1 displays the distributions of error rate of each graphical password system and 6 digits PINs. Unsurprisingly, PINs has the lowest error rate between first day and last day (first day = 3.224 and last day = 0%, P = 0.0051) following by PassFaces (first day =18.98% and last day = 3.686%, P < 0.0001) then Pass-Go (first day = 24.444% and last day = 6.104%, P = 0.002) and PassPoints (first day =28.28% and last day = 13.855%, P = 0.006). The error rate is noticeably better comparing between the first day and the last day.

Table 1: Error rate result (percent)

	Day	Mean	t-test	S.d.	Min	Max
PINs	First day	3.224	t = 2.901 P = 0.0051	6.069	0	14.28
	Last day	0		0	0	0
Pass-Go	First day	24.444	t = 4.01 P = 0.002	23.428	0	70
	Last day	6.105		8.852	0	25
PassPoints	First day	28.28	t = 2.852 P = 0.006	23.93	0	73.33
	Last day	13.855		13.952	0	42.85
PassFaces	First day	18.98	t = 4.387 P < 0.0001	17.741	0	55.26
	Last day	3.686		7.708	0	20

5.2.Login Attempts

Table 2. displays the number of attempts required for successful authentication of each graphical password system. PINs has the lowest number of attempts (first day = 1.161 tries and last day = 1 try, P = 0.0425). PassGo has the most significant difference between the first day and the last day related to P value in t-test (first day = 2.355 tries and last day = 1.355 tries, P = 0.0013) following by PassFaces (first day = 1.709 tries and last day = 1.194 try, P = 0.0014) and PassPoints (first day = 1.935 tries and last day = 1.387 ties, P = 0.0075).

Table :. Login attempts result (tries)

	Day	Mean	t-test	S.d.	Min	Max
PINs	First day	1.161	t = 2.073 P = 0.0425	0.374	1	2
	Last day	1		0	1	1
Pass-Go	First day	2.355	t = 3.392 P = 0.0013	1.539	1	6
	Last day	1.355		0.486	1	2
PassPoints	First day	1.935	t = 2.772 P = 0.0075	0.964	1	5
	Last day	1.387		0.495	1	3
PassFaces	First day	1.709	t = 3.361 P = 0.0014	0.74	1	4
	Last day	1.194		0.401	1	2

5.3.Login Time

Table 3 displays the average login time required in a successful authentication of each graphical password system and 6 digits PINs in second time unit. PINs has the fastest login time (first day = 4.67 and last day = 4.344 sec, P = 0.5) and following by Pass-Go (first day = 19.305 sec and last day = 4.296 sec, P < 0.0001) then PassPoints (first day = 10.916 and last day = 4.389 sec, P < 0.0001) and PassFaces (first day = 28.755 and last day; μ = 15.088 sec, P < 0.0001). Login time on the selected graphical password systems after one week is also improved. Pass-Go and PassPoints login time in last day are similar to PINs.

5.4.Usability Results

We conducted user satisfaction experiment by using he Lewis' Post-Study System Usability Questionnaire (PSSUQ) which contains 19 usability questionnaire items and likert scale from 1 to 7. 1 means strongly disagree and 7 means strongly agree from Fig. 3 displays an average value for each graphical password system and 6 digits PINs comparing between the first day and the last day. The scores of PINs are slightly different between the first day and the last day but for the graphical password systems, the scores are significantly different and all of them are about the similar level. At the first day most of participants had negative comments for the graphical password systems for example some of them said that "why do I have to change from the current easy authentication system", "Graphical passwords are too complex" but at the last day 66.67% of participants said that they are willing to use the graphical password systems instead of 6

PINs, while 20% of participants said that they probably use the graphical password systems instead of 6 digits PINs and 13.33% of participants preferred to use 6 digits PINs than the graphical password systems.

Table :. Login time result (seconds)

	Day	Mean	t-test	S.d.	Min	Max
PINs	First day	4.67	t = 0.659 P = 0.5	1.911	1.78	9.93
	Last day	4.344		1.923	1.37	8.39
Pass-Go	First day	19.305	t = 6.612 P < 0.0001	12.258	5.14	48.51
	Last day	4.296		2.076	1.8	10.21
PassPoints	First day	10.916	t = 6.256 P < 0.0001	5.261	2.28	20.39
	Last day	4.389		2.0165	1.3	8.71
PassFaces	First day	28.755	t = 4.547 P < 0.0001	15.661	12.07	71.37
	Last day	15.088		5.074	7.51	25.74

6. Discussion and Limitations

The results from section 5 shows that after users used the graphical password systems in one week as a daily usage, error rate, login attempts, login time and usability are significantly improved and some of them are almost equivalent to 6 digits PINs with the higher theoretical password space and less guessability issue, Although the participants were well trained at the fist day but the error rate of graphical password systems are still very high.

Our findings regarding error rate and login attempts show that users could take just one week to improve. Once participants are familiar to the graphical password systems, the error rate for the selected graphical password systems PassGo and PassFaces are significantly improved. Error rate result in the last day are also comparable to 6 digits PINs. The error rate of PassPoints was slightly improved because users found that tapping at the same position on a smartphone display is a difficult task even though we already enlarged the tapping area.

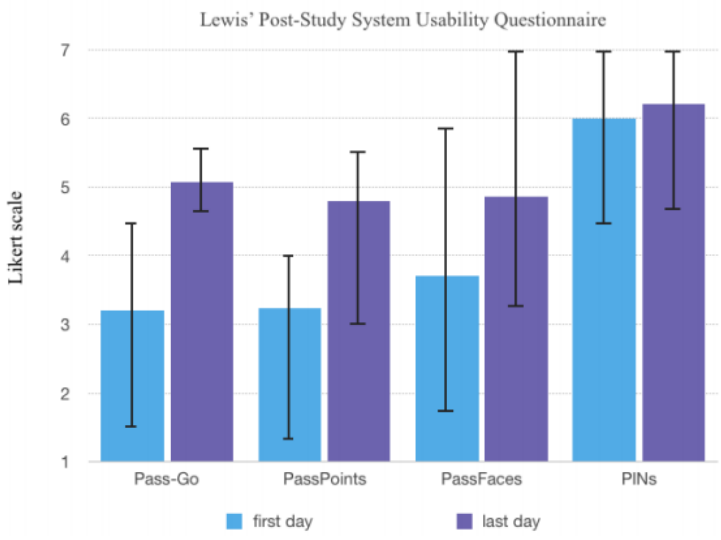


Fig. 3: PSSUQ result

Our findings regarding login time show that for each graphical password system were noticeably improved especially for PassGo. The results of Pass-Go and PassPoints at the last day are comparable to 6 digits PINs. Login time of PassFaces were about 50% improved but still taking long time compare to the others (PassFaces 14.927 sec, 6 digits PINs 4.606) because participants found that it was tough to find a password image on total 50 images per one panel.

In addition of usability, Each graphical password system has about the same likert score as we mentioned in section 5.4 most of participants are more satisfied comparing between the first day and the last

day and most of them are willing to change their secondary authentication system on a smartphone instead of 6 digits PINs.

From the experiment, although the result could show that error rate, login attempts, login time and usability were improved in a week but one of the main issue of graphical password system is shoulder surfing attack is still need to be prevented and improved, some of our selected may or may not have an ability to resist the attack.

7. Conclusions

We have presented the study of the graphical password usability on a smartphone can be significantly improved in a week with higher theoretical password space comparing to PINs and we found that there's possible to use graphical password systems as a secondary authentication system on a smartphone. In the future we would like to develop a better graphical password system on a smartphone which consists both acceptable usability and security.

8. Acknowledgement

We would like to thank F. Schaub, M. Walch, B. Könings, and M. Weber [19] for publishing an android open-source Pass-Go which can reduce huge of our application development time.

9. References

[1] B. Enso. How Consumers Remember Passwords. Forrester Research Report, June 2, 2004.

[2] D. Florencio and C. Herley. A large-scale study of web password habits. *proc. of the International Conference on World Wide Web (WWW 2007)*, pp. 657-666 (2007)

[3] S. Uellenbeck, M. Dürmuth, C. Wolf and T. Holz. Quantifying the security of graphical passwords: The case of android unlock patterns. *proc. of the 2013 ACM SIGSAC Conference on Computer & Communications Security (CCS '13),* pp.161-172. ACM, New York, NY, USA (2013)

[4] S. Chiasson, A. Forget, E. Stobert, P. Van Oorschot and R.Biddle. Multiple password interference in text passwords and click-based graphical passwords. *proc. of 16th ACM conference on Computer and communications security*, pp. 500–511, ACM (2009).

[5] D. Nelson, U. Reed and J. Walling. Picture superiority effect. *Journal of Experimental Psychology*, Human Learning and Memory (3), pp. 485–497 (1977).

[6] R. Biddle, S. Chiasson and P. van Oorschot. Graphical Passwords: Learning from the First Twelve Years, Carleton University - School of Computer Science, *Technical ReportTR-11-01*, January 4, 2011.

[7] I. Jermyn, A. Mayer, F. Monrose, M.K. Reiter and A.D. Rubin. The Design and Analysis of Graphical Passwords. *proc. of USENIX Security Symposium* (1999).

[8] P. Dunph and J. Yan. Do Background Images Improve "Draw a Secret" Graphical Passwords? *proc. of 14th ACM Conference on Computer and Communications Security*, Virginia, USA. pp. 36-47, ACM Press, New York, October 28-31, 2007.

[9] H. C. Gao, X. W. Guo, X. P. Chen, L. M. Wang and X. Y. Liu. YAGP: Yet another graphical password strategy. *proc. of 24th Annual Computer Security Applications Conference (ACSAC 2008)*, California, USA. pp.121-129, August 8-12, 2008.

[10] E. Hayashi, R. Dhamija, N. Christin and A. Perrig. Use Your Illusion: secure authentication usable anywhere. *proc. of SOUPS '08*, ACM (2008).

[11] R. Dhamija and A. Perrig. Deja Vu: A User Study Using Images for Authentication. *proc. of 9th USENIX Security Symposium*(2000).

[12] S Wiedenbeck, J Waters, J. Birget, A. Brodskiy and N. Memon. PassPoints: Design and longitudinal evaluation of a graphical password system, *International Journal of Human-Computer Studies*, pp.102–127 (2005).

[13] A. Stubblefield and D. R. Simon. Inkblot Authentication. Microsoft Technical Report MSR-TR-2004-85 (2004).

[14] Hai Tao. Pass-Go, a New Graphical Password Scheme, Master Thesis. University of Ottawa Canada, (June 2006).

[15] S. Brostoff and M. A. Sasse. Are PassfacesTM more usable than passwords? A field trial investigation. *proc. of Human Computer Interaction*. pp. 405-424 (2000).

[16] T. Valentine. An evaluation of the Passface personal authentication system, Technical Report. Goldsmiths College, University of London (1998).

[17] T. Valentine. Memory for Passfaces after a Long Delay, Technical Report, Goldsmiths College, University of London (1999).

[18] J.R. Lewis. IBM Computer Usability Satisfaction Questionnaires: Psychometric Evaluation and Instructions for Use, *International Journal of Human-Computer Interaction.* pp. 57–78 (1995).

[19] F. Schaub, M. Walch, B. Könings and M. Weber Exploring the design space of graphical passwords on smartphones. *proc. of SOUPS '13* (2013).