charPattern: Rethinking Android Lock Pattern to Adapt to Remote Authentication

Kemal Bicakci and Tashtanbek Satiev(✉)

Computer Engineering Department,
TOBB University of Economics and Technology, Ankara, Turkey
tsatiev@etu.edu.tr

Abstract. Android Lock Pattern is popular as a screen lock method on mobile devices but it cannot be used directly over the Internet for user authentication. In our work, we carefully adapt Android Lock Pattern to satisfy the requirements of remote authentication and introduce a new pattern based method called *charPattern*. Our new method allows dual-mode of input (typing a password and drawing a pattern) hence accommodate users who login alternately with a physical keyboard and a touchscreen device. It uses persuasive technology to create strong passwords which withstand attacks involving up to 10^6 guesses; an amount many experts believe sufficient against online attacks. We conduct a hybrid lab and web study to evaluate the usability of the new method and observe that logins with *charPattern* are significantly faster than the ones with text passwords on mobile devices.

1 Introduction

As being a viable alternative to traditional text based passwords, graphical passwords have gained significant attention in academic research in the last 15 years [1]. From practical point of view, maybe the most successful graphical password example is Android Lock Pattern (ALP) which comes pre-installed in most Android smartphones and is presumably the most widely deployed one. As its name implies, Android Lock Pattern (ALP) is mainly used to lock smartphones. Security and usability requirements for remote access (over the Internet) are very different than the ones presented in local operation while locking/unlocking a phone or tablet. We identify two main differences as follows:

1. ALP provides a theoretical password space of 18 or 19 bits [1,2]. Recent research estimates a partial guessing entropy of only 9.1 bits [2]. This may provide adequate level of security for its intended purposes especially with a policy enforcing maximum number of false trials. On the other hand, although there is not a consensus among security researchers for the minimum security requirements for web authentication, there is no doubt that ALP in its present form offers much less than required.
2. Even though touch screen devices are being widely deployed, use of a desktop or a laptop computer with an old-fashioned monitor is still common. Previous

S.F. Mjølsnes (Eds.): PASSWORD 2014, LNCS 9393, pp. 74–86, 2015.
DOI: 10.1007/978-3-319-24192-0_5

research suggested that an authentication scheme designed for touch screen devices such as ALP is likely not suitable for users alternating between desktops and touch screen devices, well [3].

In our work, we propose a new knowledge-based authentication method called charPattern targeting web applications by a careful adaptation of ALP method addressing the aforementioned differences and thus challenges. We also conduct a hybrid lab and web study to compare the usability of charPattern with text passwords and gridWordX [4]; a recent multiword password proposal answering the research challenge arising from the evolution of Internet access devices [3]. The results of user study show that while there is no significant difference between login times of charPattern and text passwords on desktop/laptop machines, login times on mobile devices are significantly lower with our new method, charPattern.

The rest of the paper is organized as follows: Sect. 2 overviews the related work. In Sect. 3, the proposed system is presented. The methodology of user study is discussed in Sect. 4 followed by presenting its results in Sect. 5. We discuss the results of user study in Sect. 6. Section 7 concludes the paper.

2 Related Work

Graphical Password. Schemes could be grouped based on how they are memorized: recall-based, cued-recall and recognition-based schemes.

Pass-Go, inspired by an old Chinese game, is a recall-based scheme where passwords are drawn by using grid intersection points [5]. Another grid-based system is Gridsure which specifically uses a 5×5 grid [6] as an alternative one-time PIN system. The grid is populated with different random digits, thus a user who memorizes her pattern could enter a different PIN occupied by the pattern in each login. PassPattern system [7] is a similar one-time password scheme.

Graphical passwords on mobile devices based on the recognition of photographs in the context of mobile devices were investigated by Dunphy et al. [8]. Schaub et al. explore the design space of graphical passwords on smart phones by implementing five different graphical password schemes on one smartphone platform [9]. They perform usability experiments and analyze shoulder surfing success rates. They consider two levels of theoretical password strength (14-bits and 42-bits).

Android Lock Pattern(ALP). Could be considered as a variation of the Pass-Go scheme by using nine points arranged in a 3×3 grid [1,2]. By setting the minimum number of points that should be chosen as four, the number of possible patterns is 389.112 giving an approximate security of 19 bits. However, this is just a theoretical maximum value. Uelenbeck et al. shows that in practice only a partial guessing entropy of 9.1 bits is achieved which is around the same security level of 3-digits random PINs [2].

Given the popularity of ALP, it is of no surprise to see that the idea is ported to other platforms as well. For instance Eusing Maze Lock 3.1 is such a free product for Windows platforms [10].

Building **passwords from multiple words** is a long-standing idea promoted to increase memorability and security. Cheswick [11] (See also summary by Rik Farrow [12]), was the first who proposed user-chosen multi-word passwords for convenient entry on smartphones.

gridWordX, improved version of gridWord [3], is a hybrid multi-word password scheme which supports elements of text and graphical passwords [4]. With gridWordX, the user could choose from a grid of words to form a password without requiring character-by-character text entry. In Fig. 1(b), the words are arranged in a 8×13 (8 rows, 13 columns) 2D grid. Besides the grid, the interface also includes three combo boxes with autocomplete property for each words of the password to allow dual-mode of input (either by typing or touching on the grid). Here, three-word-length password provides around 20 bits of password security.

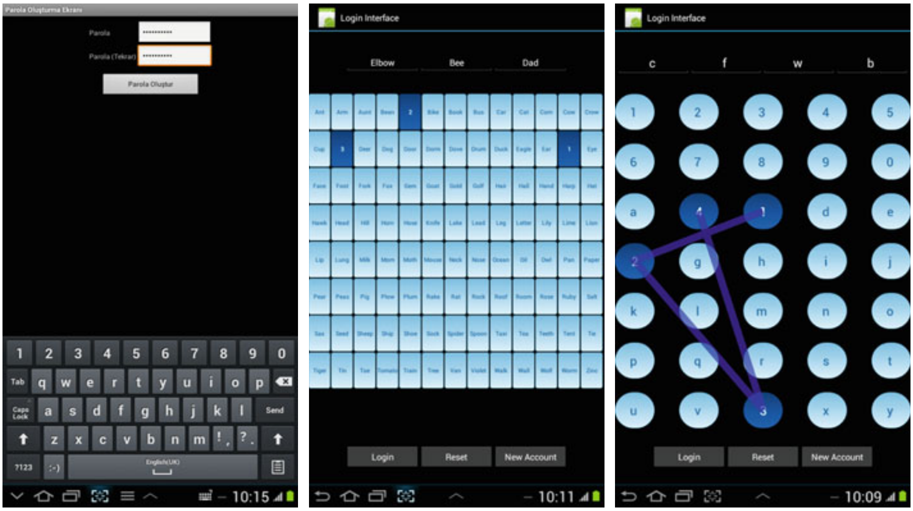
3 The Proposed System

The proposed system in this research, charPattern (see Fig. 1(c)), allows drawing a pattern over so called dot-characters to support entering a password by touching on the mobile device (dot-character is a dot corresponding to a unique character). Since patterns stimulate visual memory, charPattern is expected to leverage password memorability. Alternatively, the system also facilitates password entry by typing the dot-characters forming the pattern with a physical or a virtual keyboard.

3.1 Design Features

We identify the main differences between charPattern and Android Lock Pattern (ALP) as follows (see Table 1):

1. ALP has 9 dots organized in a 3×3 grid. On the other hand, charPattern has 35 dots organized in seven rows and five columns. With at least four dots forming a password, this gives a password space over one million. We note that if the passwords are chosen uniformly, a password space of one million could withstand against online attacks if lockout rules are in use [13,14].
2. Theoretical password space could not be reached in practice with user-chosen passwords since users are more likely to select a password among hotspots, a more popular subset. However, with persuasive technology proposed first with Persuasive Cued Click Points (PCCP) method [1], hotspots could be avoided. The basic idea is to suggest users a randomly generated password while they are creating their account. While users are allowed to ask for a new suggestion as much as they wanted, this significantly slow the password creation process. Hence a secure password selection becomes a path of “least resistance”. In a sense, use of persuasive technology could be regarded as balancing the tradeoff between system-generated passwords and user-chosen passwords regarding usability and security properties. In charPattern, we borrow this technique to suggest users a randomly generated pattern-password composed of four dot-characters.



(a) Text password.

(b) gridWordX.

(c) charPattern.

Fig. 1. Login interfaces of authentication methods investigated in our work on a mobile device.

3. In charPattern, each of the dots is mapped to a unique alphanumeric character. We choose 10 numeric digits and 25 lowercase letters (all letters in English alphabet except the letter "z") to have 35 characters in total. This gives the opportunity to map each pattern to a text password composed of 4 characters. Users are free to enter their passwords either by drawing the pattern or by typing the text password. For instance, the pattern seen in Fig. 1(c) could also be entered by typing the password "cfwb".
4. To be able to draw a pattern with any of four dots (not only the consecutive dots), we require pausing for minimum of 150 ms on a dot to select it as part of the pattern. In other words, unlike ALP method, with charPattern it is possible to skip dots if we draw a pattern without pausing over them.

3.2 Implementation

The proposed system is implemented for both mobile devices and as a web application for desktop/laptop computers. On the mobile device, charPattern is implemented as a standalone full-screen Android application (see Fig. 1).

We also develop charPattern as a web application for desktop computers using PHP, HTML and Javascript version 5 (not shown as a figure). Both the mobile and the web application are developed by the same programmer to achieve a comparable look and feel.

Table 1. ALP vs. charPattern

Comparison criteria	ALP	charPattern
Number of dots	9	35
Dot-matrix size	3×3	5×7
Dot interface	Only dots	Each dot mapped to a unique character
Password-length	[4,9] dots	4 dots
# of possible passwords	389112	1256640
Max. password entropy (bits)	17	20
Compatibility with entry using physical keyboards	NO	YES
Creating a password	User-selected	Use persuasive technology
Dot selection method	Every dot in a path	150 ms pausing on a dot to select

4 User Study

We conduct a user study to compare the usability of traditional text passwords, gridWordX and charPattern on mobile devices and in a traditional desktop/laptop environment. Before the study, we formed our hypotheses as follows:

1. Login with charPattern takes shorter time than with text-based authentication on mobile devices.
2. Login with charPattern takes shorter time than with gridWordX on mobile devices.
3. Login with charPattern takes comparable time with login using text passwords on computers having physical keyboard.
4. Login with charPattern takes comparable time with login using gridWordX on computers having physical keyboard.

In the user study, 25 undergraduate and graduate students of TOBB University of Economics and Technology (17 males and 8 females) participated. The ages of participants are ranged between 19 and 28. We note that every participant is already familiar with using desktop computers and mobile devices for Internet access.

4.1 Sessions of the Study

The user study has a within-subjects design and consists of four sessions. The interval between each session is minimum of four days and maximum seven days. In the first session, each participant is invited to the lab and asked to create an account by entering a username and creating a password on a mobile device. A password is created for all three systems; text password authentication, gridWordX and charPattern hence each participant has three passwords in total. The participant also performs a login on the mobile device after solving a mental rotation test (MRT) test. MRT is used to remove users' short term memory. We employ counterbalancing between password methods to handle order effects.

In the second and third sessions, the participants perform logins on their own laptop/desktop computers remotely by their username-password pairs created in the first session (with all three systems).

In the fourth (last session) session, the participants are re-invited to the lab and asked to perform a second login on the mobile device with their username-passwords (again with all three systems).

4.2 Pre-experimental Instructions

Before the first session, a brief presentation about the user study was provided which includes general oral instruction and a short demo on three password methods. The oral instruction covers the following points:

- We emphasize that our aim is to evaluate the authentication methods, not the participants themselves.
- We ask participants to create a text password which consists of at least eight characters.
- We ask them not to use a password they use in real life as the text password they create for the study.
- The participants should not take a note of their passwords in any form (writing down, taking a photo, etc.).
- The participants are asked to treat their passwords as a real passwords rather than just experimental as they have to use them in future sessions, again.

We do not mention which authentication method is designed by us in order to avoid any bias among the participants with respect to usability of the methods.

4.3 Lab Study

In the lab study, all participants used the same mobile device (Sumsung Tab2 7 inch tablet with Android SDK API 17 which has 600×1024 resolution and 170 ppi pixel density) so that they are tested under same conditions. The participants filled out a post-task questionnaire after the second login performed in their second visit to the lab.

4.4 Web Study

Second and third sessions were conducted over the Internet hence we call it a web study. The web study was held to compare usability of charPattern with traditional text password and gridWordX on desktop/laptop computers. We asked participants not to use their touch-screen devices in the web study. But we did not ask anything particular regarding mouse use. The users were free to use a keyboard or a mouse (applicable only with gridWordX and charPattern) to enter their passwords. In the web study, users were allowed to ask for their passwords through email after three unsuccessful attempts if they decided they could not recall their passwords.

5 Results

The following data is collected in the user study:

- **Timing.** Creation & confirmation and login times.
- **Number of Attempts.** The number of attempts until the correct login.
- **Number of Shuffles.** How many times a user asks for a new password suggestion (applicable to gridWordX and charPattern).
- **Modes of Input.** In gridWordX and charPattern, users enter passwords either by typing or by drawing (touching). Mixing these two modes is also possible. As a result, there are three different modes of input.
- **Questionnaire.** User responses to survey questions.

5.1 Collected Data Analysis

Here, we provide the results of the collected data analysis. While applying statistical tests, a difference is considered statistically significant if the p value is less than 0.05.

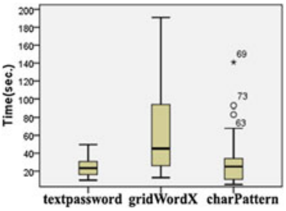


Fig. 2. Creation & confirmation times.

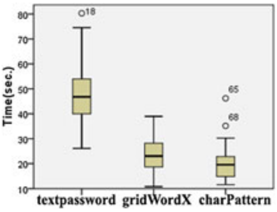


Fig. 3. Login times in lab study.

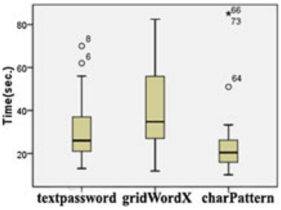


Fig. 4. Login times in web study.

The times to create and confirm passwords for each method are presented in Fig. 2.

Login times in the lab study and in the web study are presented in Figs. 3 and 4, respectively.

Regarding login times of three methods on the mobile device (lab study), we obtain highly significant difference between three datasets by applying non-parametric k-related sample-test Friedman to three datasets in each of two sessions separately as shown in Table 2.

Table 3 presents results of non-parametric k-related sample-test Friedman applied to login times of text passwords, gridWordX and charPattern in the Web

Table 2. Friedman test results for lab study.

Method name	Mean ranks			Test results	
	First login	Last login		First login	Second login
text password	2.93	2.84	Chi-Square	31.76	26.64
gridWordX	1.56	1.64	df	2	2
charPattern	1.52	1.52	Asymp.Sig	0.00000	0.00000

Table 3. Friedman test results for web study.

Method name	Mean ranks			Test results	
	First login	Last login		First login	Second login
text password	1.92	2.16	Chi-Square	4.16	2.96
gridWordX	2.32	2.12	df	2	2
charPattern	1.76	1.72	Asymp.Sig	0.125	0.228

study. Here, we find no significant difference although charPattern has shorter login times than text passwords and gridWordX.

Table 4 presents success rates of text passwords, gridWordX and charPattern with regard to creation & confirmation and login (a user is considered successful if he/she could complete it with no more than three attempts and if the password is not asked by email). We apply non-parametric k-related sample-test Friedman and obtain no significant difference between results.

Table 4. Login success rates

	Create & confirm	Login sessions			
		First	Second	Third	Fourth
text password	25/25	25/25	24/25	25/25	25/25
Success rates	100.00 %	100 %	96 %	100 %	100 %
gridWordX	23/25	25/25	17/25	23/25	25/25
Success rates	92 %	100 %	68 %	92 %	100 %
charPattern	25/25	24/25	16/25	24/25	25/25
Success rates	100 %	96 %	64 %	96 %	100 %

As presented in Table 5, shuffle count of charPattern is less than of gridWordX, but by applying the paired-sample Wilcoxon test, we obtain no significant difference between them.

The number of participants using more than 5 shuffles with gridWordX is 5, whereas with charPattern it equals to 1. In Table 6, we show how number of shuffles in gridWordX and charPattern influences success rates.

Table 5. Shuffle results of gridWordX and charPattern

	N	Mean	Std. Dev	Min	Max
gridWordX	25	4.60	7.984	0	36
charPattern	25	1.56	1.981	0	7

Table 6. Effects of shuffles on success rates for gridWordX and charPattern

	# of shuffles	# of trials	Confirm and login success rates				
			Conf	1st	2nd	3rd	4th
gridWordX	Low: < 6	20 (80 %)	95 %	100 %	70 %	90 %	100 %
	High:> 5	5 (20 %)	80 %	100 %	60 %	100 %	100 %
charPattern	Low: < 6	24 (96 %)	100 %	95.8 %	62.5 %	96.8 %	100 %
	High: > 5	1 (4 %)	100 %	100 %	100 %	100 %	100 %

Table 7. Frequency of input modes in charPattern and gridWordX

		Create & confirm	Logins			
			wk 1	wk 2	wk 3	wk 4
gridWordX	clicking	25	24	23	23	25
	typing	0	0	1	0	0
	hybrid	0	1	1	2	0
charPattern	drawing	25	25	22	24	25
	typing	0	0	2	1	0
	hybrid	0	0	1	0	0

Input modes are typing, drawing (touching/clicking) and hybrid mode in charPattern and gridWordX. The distribution of participants regarding these three input modes is shown in Table 7.

In the questionnaire, we ask seven 10-point Likert-scale (1 is disagreement, 10 is strong agreement) questions. The results are given in Table 8.

6 Discussion

Before the user study, we conjectured that users would spend less time to login with charPattern on a mobile device because drawing a pattern is much natural than typing on a virtual keyboard (as in text passwords) or touching on cells in a grid (as in gridWordX). As seen in Table 2, charPattern is faster than text passwords and gridWordX with respect to login times on the mobile device which supports our first two hypothesis.

Regarding login times of text passwords, gridWordX and charPattern in the Web study, we find no significant difference (see Table 3). As a result, hypothesis

Table 8. The questionnaire results

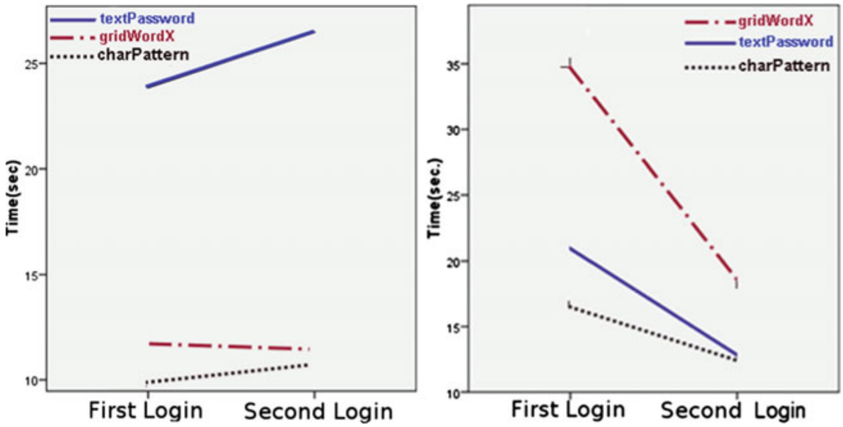
Question	Mean
1. Using pattern makes charPattern easily memorable	8.56
2. The increase in number of dots does not make drawing a pattern more difficult	6.76
3. I easily created a password in charPattern	8.68
4. Login using charPattern was easy on a desktop computer	9.48
5. Login using charPattern was easy on a mobile device	9.08
6. I liked charPattern as much as a text password	8.04
7. charPattern is at least as secure as a text password	7.72

3 and 4 are also supported. Before the user study, we conjectured that on a machine without a touchscreen the advantage of charPattern regarding login times is lost because drawing the pattern on the screen is no longer possible. But we thought charPattern still yields comparable login times with the other methods since users have the chance to try other modes of input *i.e.*, by typing. After the user study, we see that the expected result is observed due to a reason not we have foreseen. In the user study, users still prefer drawing the pattern over typing the password but this time with a mouse or a touchpad. Since drawing a pattern with a mouse or a touchpad is not as comfortable as drawing it on the screen, the login times turned out to be as expected; comparable to other two methods.

Figure 5 demonstrates the change in login times in subsequent logins. The login time in the second login on a mobile device takes longer that the one in the first login for all three methods. This results suggest that although we applied a MRT test, users were more comfortable in entering their passwords just after they created it. On the other hand, in the web study second logins took much less time than the first login. This result is as expected because the first login was the first time the web interface was presented to the users. The important point here is that in the lab study the difference between login times of charPattern and text passwords holds for both logins (on the other hand, the difference between gridWordX and charPattern drops significantly).

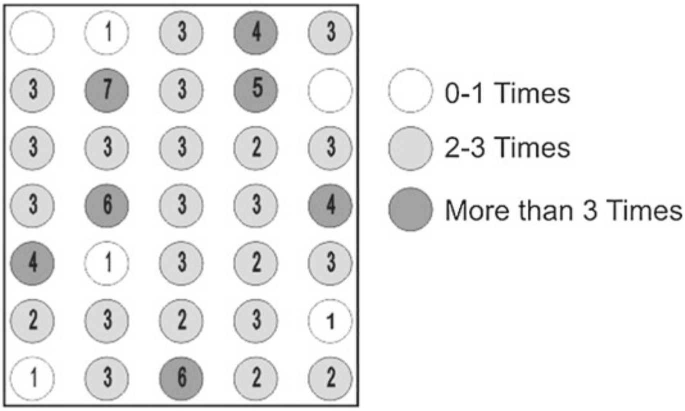
The survey results show that users find charPattern easy-to-use both on desktops and mobile devices. It is surprising to see that users find charPattern easier to use than text passwords more on desktop machines than mobile devices (although the difference is not significant).

Limitations. One obvious limitation is with regard to demographics and number of the participants. The participants were all university students which might not reflect the behavior of general public. Secondly, the number of participants was limited and not sufficient to make sharp conclusions. Finally, we conducted the study within a short time period. Studies in longer time frames would be better for analyzing memorability of charPattern.



(a) Login Times on Mobile Device. (b) Login Times on Desktop Computer.

Fig. 5. The change in login times in the first and second logins on Web and Lab Studies.



	1	3	4	3
3	7	3	5	
3	3	3	2	3
3	6	3	3	4
4	1	3	2	3
2	3	2	3	1
1	3	6	2	2

Fig. 6. Frequency of dots selected as part of a charPattern password.

Security Analysis. We mentioned that the password entropy of charPattern is 20 bits which can safeguard against online attacks with lockout rules. On the other hand, it is still of an issue whether some passwords are more likely to be chosen in this space. An attacker could exploit the nonuniform password distribution by giving priority to more likely passwords while guessing. In charPattern, we mitigate guessing attacks by disallowing user-chosen passwords and suggesting users randomly generated passwords. Hotspots could still be present in charPattern passwords if users ask for suggestions (hit the "Shuffle" button) until an easy-to-guess password is suggested.

Figure 6 presents the frequency of dots selected by the participants where 17.14 % were selected 0–1 times, 62.86 % were 2–3 times and 20 % of dots were selected more than 3 times. To understand whether this particular distribution is different than a random distribution, we generate simulated data consisting of 100 datasets each of which has 25 pairs of (x, y) elements where x ranges from 1 to 5 and y ranges from 1 to 7 corresponding to column and row sizes of the dot-matrix in charPattern, respectively. Then, we calculate rough estimate values of password entropy for the collected dataset together with random datasets using the formula H(X) defined in [15]. Our rough estimate password entropy of collected dataset is between maximum and minimum entropy values of simulated datasets. Since each random dataset represents a chance to include the observed data, with 99 % probability, the user study dataset is a dataset occurred by chance. This analysis gives an evidence that hotspots do not skew the password distribution for charPattern.

7 Conclusion

As Android Lock Pattern has successfully demonstrated, drawing a pattern-password is preferred over typing a password or a PIN by many users for locking/unlocking their touchscreen devices. However, lock patterns could not be used over the Internet directly for remote user authentication due to different security and usability requirements. In this paper, we introduce charPattern, a new pattern-based authentication method which increases password space to adequate levels (i) by increasing number of possible patterns by careful addition of more dots, (ii) by using persuasive technology to avoid hotspot passwords (more popular patterns). To accommodating users who alternately login from devices with and without full physical keyboards, the new scheme improves on the idea of Android Lock Pattern by introducing a second mode of input by enabling users to type the characters corresponding the dots forming their pattern-password.

Our user study, which involves lab and web sessions, shows that charPattern has significantly shorter login times than text passwords on a mobile device. In addition, most users prefer to enter charPattern passwords by drawing the pattern rather than by typing via keyboard even on desktop machines, which leads to login times comparable to those of text passwords on desktops. Based on user study findings, we conclude that charPattern is a promising alternative to text passwords for those who access same sites from both of mobile devices and desktops. In the future, we plan to compare recall of charPattern passwords with recall of text passwords in a long term user study.

References

1. Biddle, R., Chiasson, S., van Oorschot, P.C.: Graphical passwords: learning from the first twelve years. ACM Comput. Surv. **44**(4), 19:1–19:41 (2012)
2. Uellenbeck, S., Dürmuth, M., Wolf, C., Holz, T.: Quantifying the security of graphical passwords: the case of android unlock patterns. In: Proceedings of the 2013 ACM Conference on Computer and Communications Security, CCS 2013, pp. 161–172. ACM, New York (2013)

3. Bicakci, K., van Oorschot, P.C.: A multi-word password proposal (gridword) and exploring questions about science in security research and usable security evaluation. In: Proceedings of the 2011 Workshop on New Security Paradigms Workshop, NSPW 2011, pp. 25–36. ACM, New York (2011)
4. Cil, U., Bicakci, K.: gridwordx: Design, implementation, and usability evaluation of an authentication scheme supporting both desktops and mobile devices. In: Workshop on Mobile Security Technologies (MoST 2013) (2013)
5. Tao, H., Adams, C.: Pass-go: a proposal to improve the usability of graphical passwords. Int. J. Netw. Secur. **7**(2), 273–292 (2008)
6. Brostoff, S., Inglesant, P., Sasse, M.A: Evaluating the usability and security of a graphical one-time pin system. In: Proceedings of the 24th BCS Interaction Specialist Group Conference, BCS 2010, pp. 88–97. British Computer Society, Swinton (2010)
7. Kumar, T.R., Raghavan, S.V.: PassPattern System (PPS): a pattern-based user authentication scheme. In: Das, A., Pung, H.K., Lee, F.B.S., Wong, L.W.C. (eds.) NETWORKING 2008. LNCS, vol. 4982, pp. 162–169. Springer, Heidelberg (2008)
8. Dunphy, P., Heiner, A.P., Asokan, N.: A closer look at recognition-based graphical passwords on mobile devices. In: Proceedings of the Sixth Symposium on Usable Privacy and Security, SOUPS 2010, pp. 3:1–3:12. ACM, New York (2010)
9. Schaub, F., Walch, M., Könings, B., Weber, M.: Exploring the design space of graphical passwords on smartphones. In: Proceedings of the Ninth Symposium on Usable Privacy and Security, SOUPS 2013, pp. 11:1–11:14. ACM, New York (2013)
10. Eusing Maze Lock 3.1. (2014). http://www.bit.ly/maze203
11. Cheswick, W.: Rethinking passwords. Queue **10**(12), 50:50–50:56 (2012)
12. Farrow, R.: Login: USENIX Magazine, **36**(2) 68–69 (2011)
13. Florêncio, D., Herley, C., Coskun, B.: Do strong web passwords accomplish anything? In: Proceedings of the 2nd USENIX Workshop on Hot Topics in Security, HOTSEC 2007, pp. 10:1–10:6. USENIX Association, Berkeley (2007)
14. Florêncio, D., Herley, C., van Oorschot, P.C.: An administrator‘s guide to internet password research. In: 28th Large Installation System Administration Conference (LISA14), USENIX Association, Seattle (2014)
15. Bicakci, K., Atalay, N.B., Yuceel, M., van Oorschot, P.C.: Exploration and field study of a password manager using icon-based passwords. In: Danezis, G., Dietrich, S., Sako, K. (eds.) FC 2011 Workshops 2011. LNCS, vol. 7126, pp. 104–118. Springer, Heidelberg (2012)