Complexity Metrics and User Strength Perceptions of the Pattern-Lock Graphical Authentication Method

Panagiotis Andriotis, Theo Tryfonas, and George Oikonomou

University of Bristol, Merchant Venturers Building, Bristol, BS8 1UB, U.K.
p.andriotis@bristol.ac.uk,
theo.tryfonas@bristol.ac.uk,
g.oikonomou@bristol.ac.uk

Abstract. One of the most popular contemporary graphical password approaches is the Pattern-Lock authentication mechanism that comes integrated with the Android mobile operating system. In this paper we investigate the impact of password strength meters on the selection of a perceivably secure pattern. We first define a suitable metric to measure pattern strength, taking into account the constraints imposed by the Pattern-Lock mechanism's design. We then implement an app via which we conduct a survey for Android users, retaining demographic information of responders and their perceptions on what constitutes a pattern complex enough to be secure. Subsequently, we display a pattern strength meter to the participant and investigate whether this additional prompt influences the user to change their pattern to a more effective and complex one. We also investigate potential correlations between our findings and results of a previous pilot study in order to detect any significant biases on setting a Pattern-Lock.

Keywords: Security, Android, password, bias, usability, feedback

1 Introduction

Innovation in the smartphone industry is now focused on novel user authentication methods. Apple recently launched their new flagship device with a built-in fingerprint identity sensor and the new trend has been set. Other smartphone manufacturers will include this feature to their products but there must exist devices that should be more affordable to the wide public. This is why traditional user authentication methods have to be enhanced with security precautions in order to make them solid against various types of attacks.

Mobile devices are playing a major role to the way we communicate with others. They are valuable assets to our personal and professional life because they integrate the most usable and popular applications. Despite the fact that a smartphone is a telephone device, it can also store sensitive information like text messages, electronic mail, notes and calendar events. It can record and play various multimedia files such as photos, audio and video. We can connect to the

Internet, browse web pages, navigate to our social media accounts and extend its internal capacity by using cloud storage services. All these capabilities imprint important personal information on their internal storage. Thus, user protection and authentication schemes should provide usability and security in a balanced mixture.

Traditional user authentication is achieved by utilizing text-based methods. These methods include Personal Identification Numbers (PIN) and text passwords. A PIN is usually (but not limited to) a four-digit code and a password is a sequence of characters. Over the years, alphanumeric and textual passwords have shown significant disadvantages because they are vulnerable to dictionary attacks. When it comes to the right proportion between usability and security people tend to prefer usability. Humans usually provide passwords that are easy to remember and add no complexity to their daily routine. This choice leads them to use poor and memorable passwords making the defense against intruders easy to break.

The problems textual passwords might cause to the protection of personal data stored in a mobile device were partially solved when graphical passwords were introduced. These types of security measures were also deployed by the need of commercial identification of Operating Systems against their competitors. Graphical passwords use pictures, images or patterns to create authentication schemes, which are easy to remember, fun to use and provide a sense of uniqueness, while at the same time aiming to be secure enough to prevent attackers from breaking them. The Android community introduced a popular graphical authentication method, which is called Android Pattern-Lock. The Android Pattern-Lock is a 3x3 grid of nodes. In order to unlock their phone, users swipe their fingers connecting nodes and formulate a memorable shape that acts as a password. Vision is also engaged in the particular process and this makes the password easier to remember.

Since the Android Pattern-Lock mechanism was introduced, numerous attempts were made by researchers to decode the way people responded to the new protection scheme. These studies tried to exploit psychological or physical biases that might occur when humans try to form a secure or a usable password. One of the problems we can identify to the graphical password authentication methods is the lack of interaction between the user and the device while the password is been generated. Thus, when setting a pattern users are not informed about its strength. On the other hand, our daily interaction with computers and web sites that require user identification, projects the importance of providing feedback to the users that the passwords they chose are not secure enough. A characteristic example of this concept is the coloured bars next to the password fields when we create a new account for a web site or when we update our details.

In this paper we investigate whether such feedback prompts actually have any impact on user perception about the security of an Android pattern. To this end, we developed an application and collected data from 120 Android users who participated in a survey about their understanding of Android Pattern-Lock security. We therefore confirm previous results highlighting that there exist spe-

cific heuristic rules that define pattern formation. Finally, we propose a password strength assessment methodology for the Android Pattern-Lock and evaluate its impact on survey participant responses.

In Sect. 2 we discuss the relevant research on the field of textual and graphical password security and mention some of the methods used in the past to exploit potential vulnerabilities present in these schemes. Section 3 provides a dissection of the experimental methodology we used and defines our metrics. Results and an evaluating discussion are been presented in Sect. 4. We draw our conclusions in Sect. 5 and propose future directions for further research.

2 Background and Related Work

Authenticating a user is among the most critical tasks in the area of computer security and especially when we are dealing with cases with high risk, including bank transactions, accessing personal information or logging into ad-hoc networks [2]. The common form of user authentication, when there is no need for sophisticated security measures, is a text-based password. Sometimes individuals have to balance between security and usability [13] and the outcome can be a choice of a weak password because a strong one is difficult to recall [5]. Numerous exploits of text-based passwords have been proposed including dictionary attacks. A well-known tool that performs such type of guessing is 'John The Ripper' [10].

As an alternative to the vulnerable textual passwords, other schemes have been proposed, known as graphical passwords [4], given the fact that the human brain reacts better when it has to deal with visual and graphical information [14] [17]. The variety of graphical passwords makes them distinct. Various processes like clicking points on an image or drawing a line can define their formation principles. An example of a graphical authentication is the PassFaces algorithm [9] that was studied and evaluated for its usability by [6]. However, human behavioural heuristic rules may affect the efficiency of a graphical password and make it vulnerable to image-based dictionary attacks [12]. Other types of graphical authentication include 'face selection' mechanisms or 'point harvesting' by clicking on specific areas of an image. Studies demonstrated that as users, we tend to pick faces that attract us [7] and we select distinct regions of interest on images [16], resulting to high levels of password predictability [11].

In the smartphone universe there exists a very popular and easy to use graphical password identification method called Android Pattern-Lock. This is a two-dimensional square grid of nine nodes that serves as a drawing canvas. The smartphone user has to form a shape that links between four and nine nodes, and this shape is the formal password that allows access to the phone. This is actually a specialized version of the Pass-Go [15] authentication system focused on the standardized size of mobile devices. Pass-Go could be considered as an algorithm that followed the concept of Draw-a-Secret (DaS) scheme [8]. In the Pass-Go paradigm we have a grid of nxn dots but the password does not need to be a cohesive line like the Android Pattern-Lock. The Pattern-Lock is a line

connecting nodes in a 3x3 grid. There are also some basic rules users must have in mind when they come up with their patterns: At least four nodes should be lit to form a password, a node cannot be used twice and jumps across unlit nodes are prohibited. These rules restrict the password space and allow only for 389,112 unique patterns to be drawn [3].

The special characteristics of the aforementioned password scheme make it an interesting topic for research. Aspects of its usability against security have been studied in [17]. In a relevant case study [3] researchers demonstrated the vulnerabilities of touchscreens and conducted attacks (known as smudge attacks) on graphical passwords using the residues that were left on the screen. This information, in conjunction with behavioural biases traced from a pilot web survey, was used in [1] to perform attacks on the Android Pattern-Lock providing promising results. Our intention here is to confirm those results and examine how the users would react if they had the ability to be informed by the smartphone about the strength of the graphical password they chose.

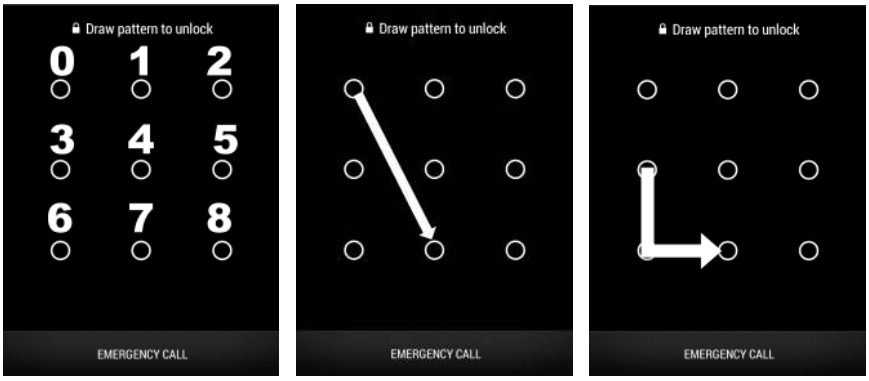
3 Experimental Setup and Definitions

In this section we will present the methodology we used to collect our data and evaluate them according to the objectives of this study. We want to measure the password strength of patterns the participants provide and also evaluate their responses to a feedback tool that informs them if they used a weak or a strong password.

3.1 Methodology

We developed an application and distributed it through the official channel for Android apps (Play Store). We were aiming to get feedback by Android users who had the chance to draw their patterns on a real device, simulating the original user identification method of the phone. First, the participants had to answer some demographic questions. Then we asked them if they would change their password if their device gave them feedback that it was a weak one. Two more questions followed, asking their opinion if the pattern they were about to draw is usable and secure. The final stage prompted them to draw the actual pattern. After the pattern was formed, the device calculated and informed the users about its strength, subsequently asking if they would like to change it or keep it. They had the right either to change the chosen pattern and draw a new one or keep it and finish the survey by submitting the results.

The survey was fully anonymized and we also took precautions to avoid duplicates. We designed the application to be unambiguous and the participants should not spend more than a few minutes to complete it. The survey was publicized through the social media in various groups of interest.



(a) (b) (c)

Fig. 1. (a) The topography of the grid, (b) a knight move, (c) a direction change.

3.2 Definitions

The calculation of the password strength was one of the most critical parts of our study. We based our assumptions and definitions on our pilot study [1] which illustrated that there exist behavioural biases when humans create their graphical passwords. The basic heuristic rules we derived by the study are: (a) More than 50% of users start their patterns from the top left node, (b) a pattern that consists of less than 6 nodes is considered as not secure enough, (c) a secure password is the one that has more than 2 direction changes. Taking these observations into account, we also included two more features to our password strength assessment algorithm. The first is the presence of one or more knight moves and the other is the existence of overlapping nodes. (In Fig. 1 we demontrate the topology of nodes (a), we show an example of a knight move (b) and provide an example of a direction change (c).) We therefore provide the following definitions.

Let G be a set (representing the Android Pattern-Lock Grid) such that:
$G = \{n : n \in \mathbb{N}\ and\ 0 \leq n \leq 8\}$.
A pattern P is an ordered set:
$P \subseteq G : P = \{a_i : i \in \mathbb{N}\ and\ 0 \leq i < |P|,\ 4\ \leq\ |P|\ \leq\ 9\}$,
($|P|$ is the cardinallity of the set.)

A direction change (abbr. c) happens when there is an angle in the shape three consecutive nodes form or when we revisit an already visited node. For example, 367 or 364 constitute a direction change and 2435 define two direction changes.

A knight move (abbr. k) is an edge that connects two distant nodes, e.g. 07, 05, 16, 15, etc.

An overlapping node (abbr. o) is an already visited node. For instance, the pattern 0124357 has an overlapping node (the node 4), which gets visited for a second time when the user moves from node 5 towards node 3.

$\|\cdot\|$ defines the number of knight moves or overlapping nodes.

Let X be a 5x1 matrix: $X = \begin{bmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \\ x_5 \end{bmatrix}$ and N the 1x5 matrix $N = \begin{bmatrix} 1\ 1\ 1\ 1\ 1 \end{bmatrix}$

where

$$x_1 = \begin{cases} 1 & , \text{ if } a_0 \neq 0 \\ 0 & , \text{ else} \end{cases}$$

$$x_2 = \begin{cases} |P| - 5 & , \text{ if } |P| \geq 6 \\ 0 & , \text{ else} \end{cases}$$

$$x_3 = \begin{cases} 1 & , \text{ if } c \geq 2 \\ 0 & , \text{ else} \end{cases}$$

$$x_4 = \|k\| \text{ and } x_5 = \|o\|$$

x_1 evaluates if the starting point of the patten is 0, x_2 contributes to the score if the pattern consists of more than 6 nodes, x_3 is used to highlight if there are more than 2 direction changes and x_4, x_5 evaluate the presence of knight moves and overlapping nodes.

Thus, the pattern-lock strength Δ is defined as: $\Delta = N \cdot X$ (1)

The feedback Φ is given to the user in a form of textual information (Weak, Medium, Strong). There are three scales of security defined from the following equation.

$$\Phi = \begin{cases} \text{Weak} & , \text{ if } 0 \leq \Delta \leq 1 \\ \text{Medium} & , \text{ if } \Delta = 2 \\ \text{Strong} & , \text{ if } \Delta \geq 3 \end{cases} \quad (2)$$

4 Results and Discussion

Table 1 provides a generic presentation of the survey results. Most of the participants were male aged between 18-29 years old. As discussed previously, the survey was publicized through university related channels; hence the education level of the participants is quite high. The vast majority of the people that took the survey are smartphone owners, and they currently have devices running the Android OS. They prefer to use the Pattern-Lock mechanism to protect personal information, prevent others fiddling with the phone or protect data if someone steals their phone (Question 9). One of the most interesting questions for the current study is Question 10. We wanted to know if they would change their chosen password if they were informed by some kind of feedback, provided by the device, that their password is weak; 77.5% of them answered affirmatively. Finally, most of the replies suggest that the users believe that their chosen pattern is usable as well as secure.

Table 1. Survey results

Number	Question	Category	Percentage
Q1	Gender	Male	60.0%
		Female	34.2%
		Didn't say	5.8%
Q2	Age	18 - 29 y.o.	60.8%
		30 - 39 y.o.	35.0%
		40+ y.o.	4.2%
Q3	Ethnicity	African-American	39.2%
		White	25.8%
		Asian	21.7%
		Hispanic/Latin	11.7%
		Others	1.6%
Q4	Education	Bachelor's	40.0%
		Master's	40.0%
		Doctorate	11.7%
		High School & Other	8.3%
Q5	Smartphone user	Yes	99.2%
		No	0.8%
Q6	Smartphone usage	6 - 12 months	45.1%
		1 - 6 years	30.1%
		less than 6 months	24.8%
		more than 6 years	1.7%
Q7	Smartphone OS	Android	82.5%
		iOS	30.1%
		Blackberry	4.2%
		Windows Phone OS	1.7%
Q8	Preferred password type	Pattern Lock	53.3%
		PIN	39.2%
		Others	7.5%
Q10	Password meter effect	Yes	77.5%
		No	22.5%
Q11	Usable pattern provided	Yes	81.7%
		No	18.3%
Q12	Secure pattern provided	Yes	86.7%
		No	13.3%

Table 2. Direction changes in the set of patterns

Changes	Number	Frequency
1	13	10.8%
2	26	21.7%
3	31	25.8%
4	33	27.5%
5	14	11.6%
6	2	1.6%
7	1	≈1%

4.1 Analysing Pattern Characteristics

The analysis of certain characteristics the patterns had (direction changes and pattern length, which is measured by the number of nodes that constitute the shape) provided the results we demonstrate in Tables 2 and 3. In Table 2 for example we can see that for the majority of patterns, their shape introduces 2 - 4 direction changes. Also, Table 3 shows that even if we use a feedback method to engage users to a better understanding of security, the outcome will still be patterns that basically consist of 5 - 7 nodes.

We believe that this is an observation that diversifies the users and keep the authentication method reliable from being predictable. If we force the user to provide stronger passwords that consist of 8 - 9 nodes (to be considered as stronger and safe) and loop around the nodes to produce a lot of direction changes, we eventually minimize the already limited password space of the Android Pattern-Lock method. Thus, a very strict feedback schema would probably have the opposite results than making the authentication method stronger and this is reflected in the definition of our strength criteria (Equation 2).

Table 3. Pattern length in the set of patterns

Length	Number	Frequency
4	17	14.2%
5	23	19.2%
6	25	20.8%
7	24	20.0%
8	13	10.8%
9	18	15.0%

4.2 Comparison with Previous Results

One of our objectives when we designed the experiment was to evaluate previous results we presented during a pilot study which examined (in a similar way) if there exist any heuristic rules that are responsible for specific biases in the provided patterns [1]. The experiments in this study were conducted using a web application, thus, the participants were not really interacting with a smartphone device but with the monitor of their computer. In addition, they were not using their fingers to form their passwords on the screen because it was an online survey and the interaction medium of the application and the user was the mouse. These characteristics and the fact that the whole procedure was a simulation of the original user authentication method, could force people to answer in a different way when they were interacting with a smartphone.

Figures 2 and 3 demonstrate that user reactions are quite similar in both experiments. We must underline here that the participants in both experiments

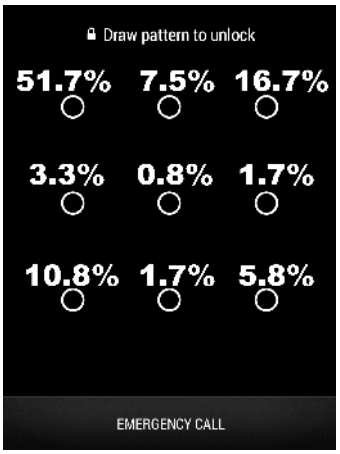
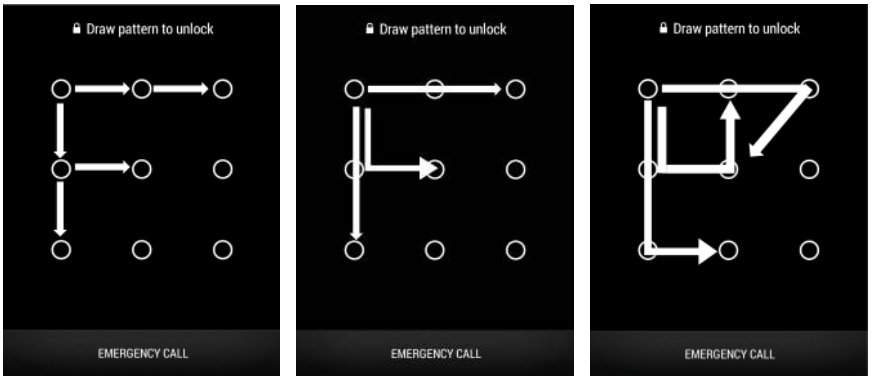


Fig. 2. Frequency of starting points.

were different and the second study took place two years after the first. In Fig. 2 we can see that more than 50% chose to start their patterns from node 0. Nodes 2 and 6 are also popular starting points and we can conclude that participants preferred to begin their drawings from the corners of the grid. Figure 3 illustrates the most common bigrams, trigrams and fourgrams. These are sub-patterns that exist in the password and provide information about the most common edges that were formed during the drawing of the pattern. A comparison with [1] shows that indeed the upper nodes are heavily utilized during password formation.



(a) (b) (c)

Fig. 3. The most common: (a) Bigrams, (b) trigrams, (c) fourgrams.

4.3 Evaluating the Feedback Responses

Table 4 concatenates the results of our research describing user perceptions about the security of the Android Pattern-Lock method and their responses to our feedback prompt. The findings we highlight in Table 4 evaluate the responses after the feedback prompt was shown to the participants. Hence, these are the final choices the users of our proposed scheme made. The password strength of the resulting patterns is almost equally distributed among the three scales. As expected, the 'Weak' passwords were fewer after the feedback was propounded. One observation we can make is that the majority of male users came up with stronger passwords in contrast to the patterns females chose.

In addition, 23.3% of the participants changed their choice of pattern when they were informed about the valence of their password. This means that almost one out of five users changed their pattern to make it stronger when the feedback underlined the lack of security of their initial choice. Another interesting finding that strengthens the importance of such a feedback mechanism is the fact that 10.7% of the people that finally changed their graphical password had said before (in Question 10) that they would not take into account any evaluation of their password strength from the device. Thus, one out of nine people paid attention to the feedback mechanism and changed the pattern they chose even though they had said (seconds before) that they would not do that.

Table 4. Password strength assesment

Scale	Number	Percentage	Gender	Number	Percentage
Weak	32	26.6%	Male	15	46.9%
			Female	12	37.5%
			Didn't say	5	15.6%
Medium	44	36.7%	Male	28	63.6%
			Female	16	36.4%
Strong	44	36.7%	Male	29	66.0%
			Female	13	29.5%
			Didn't say	2	4.5%
Remarks				Number	Percentage
Changed Pattern				28/120	23.3%
Changed despite their 'No' at Q10				3/28	10.7%
Didn't Change 'Weak' despite their 'Yes'				26/120	21.7%
Changed from 'Weak' to 'Weak'				2/28	7.1%

On the contrary 21.7%, meaning one out of five users, did not change their 'Weak' passwords although they had answered that they would consider a feedback from the device. Perhaps a more aggressive design strategy and a more exhorting message would be sufficient to change this feature. Finally, one out of fourteen participants that changed their patterns, they chose 'Weak' passwords again. An explanation to this observation might be that there is a small part

of users that prefer a very usable pattern ignoring the security a more complex drawing provides.

5 Conclusion and Future Work

In this study we compared our results with previous knowledge justifying that there are specific behavioural biases that define the formation of graphical patterns. We proposed a scheme, which measures the strength of Android Pattern-Lock instances and reported the effects a feedback prompt would have to users. We demonstrated that the majority of people that participated in our experiments were positively affected by the suggestions about security our proposed algorithm produced. They finally changed their passwords and this outcome resulted to stronger user authentication paradigms.

Further work should include the investigation of the impact other features might have at the calculation of the password strength. The password valence assessment criteria could include ending points, bigrams, trigrams and dexterity; the algorithm could also assign different weights to the final evaluation criteria of the password strength. Another issue we should take into consideration is how aggressive and persuasive a feedback prompt could be in order to provide to the user a better understanding of security without decreasing the password space of the Android Pattern-Lock method.

Acknowledgements

This work has been supported by the European Union's Prevention of and Fight against Crime Programme "Illegal Use of Internet" - ISEC 2010 Action Grants, grant ref. HOME/2010/ISEC/AG/INT-002 and the Systems Centre of the University of Bristol. We are grateful to Etelaowoni Queeneth Ogbeche for her contribution to data collection.

References

1. P. Andriotis, T. Tryfonas, G. Oikonomou, and C. Yildiz.: A pilot study on the security of pattern screen-lock methods and soft side channel attacks. In: 6th ACM conference on Security and privacy in wireless and mobile networks, WiSec13, pp. 1 - 6. ACM, (2013)
2. I. G. Askoxylakis, D. D. Kastanis, and A. Traganitis.: Elliptic curve and password based dynamic key agreement in wireless ad-hoc networks. In: Communication, Network, and Information Security, pp. 50 - 60, (2006)
3. A. J. Aviv, K. Gibson, E. Mossop, M. Blaze, and J. M. Smith.: Smudge attacks on smartphone touch screens. In: 4th USENIX conference on Offensive technologies, pp. 1 7, USENIX Association, (2010)
4. R. Biddle, S. Chiasson, and P. C. Van Oorschot.: Graphical passwords: Learning from the first twelve years. ACM Computing Surveys, 44 (4) : 141, (2012)

5. J. Bonneau.: The science of guessing: analyzing an anonymized corpus of 70 million passwords. In: Security and Privacy (SP), 2012 IEEE Symposium, pp. 538 - 552, IEEE, (2012)
6. S. Brostoff and A. Sasse.: Are Passfaces More Usable Than Passwords? A Field Trial Investigation. In: People and Computers XIVUsability or Else!, pp. 405 - 424, Springer London, (2000)
7. D. Davis, F. Monrose, and M. Reiter.: On user choice in graphical password schemes. In: USENIX Assosiation Proceedings of the 13th USENIX Security Symposium, pp. 151 163, USENIX Association, (2004)
8. I. Jermyn, A. Mayer, F. Monrose, M. K. Reiter, and A. D. Rubin.: The Design and Analysis of Graphical Passwords. In: 8th USENIX Security Symposium, pp. 1 - 14, (1999)
9. Passfaces Corporation.: The Science Behind Passfaces. White paper, available at http://www.passfaces.com/enterprise/resources/white_papers.htm.
10. Solar Designer. John the Ripper. Online at http://www.openwall.com/john/.
11. P. C. van Oorschot and J. Thorpe.: Exploiting Predictability in Click-based Graphical Passwords. Journal of Computer Security, 19 (4) : 669702, (2011)
12. P. C. van Oorschot and J. Thorpe.: On predictive models and user-drawn graphical passwords. ACM Trans. Inf. Syst. Secur., 10 (4) : 5:15:33, (2008).
13. M. A. Sasse, S. Brostoff, and D. Weirich.: Transforming the 'weakest link' - a human/computer interaction approach to usable and effective security. BT Technology Journal, 19 (3) : 122131 (2001)
14. L. Standing, J. Conezio, and R. N. Haber.: Perception and Memory for Pictures: Single-trial Learning of 2500 Visual Stimuli. Psychonomic Science, 19 (2) : 7374, (1970)
15. H. Tao and C. Adams.: Pass-Go: A Proposal to Improve the Usability of Graphical Passwords. International Journal of Network Security, 7 (2) : 273292, (2008)
16. J. Thorpe and P. C. van Oorschot.: Human-seeded attacks and exploiting hot-spots in graphical passwords. In: USENIX Assosiation Proceedings of the 16th USENIX Security Symposium, pp. 103 118, USENIX Association, (2007)
17. S. Uellenbeck, M. Dürmuth, C. Wolf, and T. Holz.: Quantifying the security of graphical passwords: the case of android unlock patterns. In: 2013 ACM SIGSAC conference on Computer & communications security, pp. 161 - 172, ACM, (2013)