A Study on Usability and Security Features of the Android Pattern Lock Screen

Author Details

Panagiotis Andriotis
Bristol Cryptography Group
University of Bristol
Merchant Venturers Building, Bristol, BS8 1UB
United Kingdom

George Oikonomou
Bristol Cryptography Group
University of Bristol
Merchant Venturers Building, Bristol, BS8 1UB
United Kingdom

Alexios Mylonas
Faculty of Computing, Engineering and Sciences
Staffordshire University
Beaconside, Stafford, ST18 0AD
United Kingdom

Theo Tryfonas
Bristol Cryptography Group
University of Bristol
Merchant Venturers Building, Bristol, BS8 1UB
United Kingdom

Corresponding author: Panagiotis Andriotis
Corresponding Author's Email: p.andriotis@ bristol.ac.uk

0 Please check this box if you do not wish your email address to be published

Acknowledgments (if applicable):
We would like to thank Mr Gareth Knowles for contributing his pattern dataset. The authors would like to express their appreciation to the anonymous reviewers for their valuable comments and suggestions.

Biographical Details (if applicable):

Panagiotis Andriotis is a PhD student in Computer Science in Bristol, U.K.. He holds an MSc with Distinction in Computer Science from the University of Bristol, U.K. and a BSc in Mathematics from the University of Athens, Greece. His main research area is Digital Forensics with a focus on smartphones and other mobile devices running the Android Operating System. He is also interested in Human Aspects of Security and Privacy and his work targets the Android graphical password authentication scheme in order to investigate its vulnerabilities and raise security awareness.

Dr George Oikonomou received the MSc and PhD degrees in computer science from the Athens University of Economics and Business, Athens, Greece, in 2002 and 2009 respectively. He is currently a Research Associate with the Faculty of Engineering at the University of Bristol and a member of the Cryptography research group. Previously, he

worked as a Research Associate at the Computer Science department, Loughborough University, UK. His current research focuses on wireless sensor networks and the Internet of things, with emphasis on security and IPv6 networking for low-power, severely constrained devices. Dr Oikonomou is an active developer of the Contiki open source embedded operating system for the internet of things.

Dr Alexios Mylonas is a Lecturer in the University of Staffordshire (UK) and an expert in Cybersecurity and Digital Forensics. In the past, he has worked as a security consultant focusing on managed PKI and IT security services. His current interests include network security, security and digital forensics in mobile devices and web security.

Dr Theo Tryfonas is a Senior Lecturer in the University of Bristol and an expert in Cybersecurity and Systems engineering with research work focused on assurance and resilience of critical infrastructures including transportation, utilities, healthcare and government. He worked in particular on systems for maritime safety and port security, public transport security, protection of UAVs, telecom revenue and system assurance, information security risk analysis as well as assisted in the investigation of computer crimes. His current interests extend to modelling cyber-capability with system dynamics and applications of game theory to the analysis of cyber attacks. He is a Chartered IT Professional member of the BCS and a Certified Information Systems Auditor.

Structured Abstract:

Purpose - The Android pattern lock screen (or graphical password) is a popular user authentication method that relies on the advantages provided by the visual representation of a password, which enhance its memorability. Graphical passwords are vulnerable to attacks (e.g. shoulder surfing), thus the need for more complex passwords becomes apparent. In this paper, we focus on the features that constitute a usable and secure pattern and investigate the existence of heuristic and physical rules that possibly dictate the formation of a pattern.

Design/methodology/approach – We conducted a survey to study the users' understanding of the security and usability of the pattern lock screen. We developed an Android application that collects graphical passwords, by simulating user authentication in a mobile device. This avoids any potential bias that is introduced when the survey participants are not interacting with a mobile device while forming graphical passwords (e.g. in web or hard-copy surveys).

Findings - Our findings verify and enrich previous knowledge for graphical passwords, namely that users mostly prefer usability than security. Using the survey results we demonstrate how biased input impairs security by shrinking the available password space.

Research limitations/implications – The sample’s demographics may affect our findings. Therefore, future work can focus on the replication of our work in a sample with different demographics.

Originality/value - We define metrics that measure the usability of a pattern (handedness, directionality, symmetry) and investigate their impact to its formation. We propose a security assessment scheme using features in a pattern (e.g. the existence of knight moves or overlapping nodes) to evaluate its security strengths.

Keywords:
Graphical password, pattern, vulnerability, user, authentication.

Article Classification: Research paper.

1 Introduction

Recently, the mobile device industry experienced a remarkable technological and economical bloom. Smartphones and tablets are now valuable multi-purpose tools assisting users to complete numerous tasks in their personal and professional lives. Innovative ideas take advantage of the capabilities that the new technology provides and focus on personalized user identification methods to protect sensitive data. One of the most recent approaches to the user identification problem is fingerprint detection. Flagship devices are now equipped with fingerprint identity sensors and algorithms that claim to be secure enough. At the same time, they provide a convenient and fast way to authenticate their users. However, at the moment, this technology is only available to expensive devices and it is already vulnerable to various attacks [1]. Therefore, it is important to further examine user authentication methods and expose aspects that make them vulnerable.

In general, the most common user authentication methods rely on text-based passwords (Personal Identification Numbers (PINs) or alphanumeric strings). It is quite common for a PIN to be a four-digit code, but an alphanumeric string can be longer and it can also include letters, digits and other characters and symbols. Despite their global use and acceptance, text-based passwords suffer from vulnerabilities that are closely related to the fact that they have to be memorable. These vulnerabilities can be exploited by popular attacks, such as dictionary attacks.

The security issues introduced by the usage of memorable text-based passwords and the need for more convenient authentication schemes led to the proposal of graphical passwords. This scheme employs images, pictures or various shapes to create novel and usable authentication methods. In the mobile devices' ecosystem, the Android *pattern lock screen* was introduced in the second version of the operating system (OS). It is a popular gesture-based authentication mechanism, which urges the user to draw a pattern within the limits of a 3×3 nodes grid in order to unlock the device. Users swipe their fingers connecting at least 4 nodes to form their graphical passwords. The fourth version of the Android OS introduced a new scheme called 'Face unlock'. It utilizes the device's camera to identify the face of its owner. However, the method is naive as it can be bypassed using a photograph of the owner. Hence, Android pattern lock screen is still a more reliable alternative authentication mechanism that provides usability and security.

The pattern lock screen is getting more popular, which increases the interest to examine its vulnerabilities. As smartphones contain a large amount of personal and business data, privacy and confidentiality can be breached if an adversary breaks the authentication method. Android developers claim that it is possible to bypass the authentication method if USB Debugging Mode is enabled [2]. However, the drawback of this attack is that USB Debugging Mode is not enabled by default. Also, the device must be restarted, thus, any temporary file stored in volatile memory will be lost.

In this paper we mount a survey and collect patterns that the users deem as usable and secure. With the analysis of the collected patterns, we study the usability and security of the Android pattern lock screen. The contributions of the paper can be summarized as follows:

- We developed an Android application to simulate password input on real devices and gather realistic results.
- We define metrics for pattern complexity. We use them to evaluate the complexity of the participants' patterns and thus their security strength.
- We examine if properties such as handedness, symmetry and native language writing style affect patterns' usability and security.
- Based on our results we demonstrate with a case study the dramatic shrinking of the graphical password space that biased input can cause.

Our findings, which come from a large and diverse sample, confirm common results that were based on web-surveys and hard-copy questionnaires (Aviv, et al., 2010), (Andriotis, et al., 2013), (Uellenbeck, et al., 2013). Our findings can be used to mount a dictionary attack

against a given pattern and/or in combination with other attacks (e.g. smudge attacks) increase the likelihood of recovering an Android pattern.

The rest of the paper is structured as follows. Section 2 discusses related work and Section 3 introduces our methodology for data collection and our definitions. Section 4 discusses our results and Section 5 demonstrates with a case study the security issues that can be caused by biased input. Finally, Section 6 includes our conclusions and future work.

2 Background

The choice of a text-based password must balance the memorability and convenience a usable alphanumeric string provides against the safety of a complex combination of symbols and letters (Sasse, et al., 2001). Unfortunately, users tend to prefer usability choosing memorable passwords that are easy to recall (Bonneau, 2012). Despite the various studies which propose schemes that enhance security without decreasing usability (Forget, et al., 2008), text-based passwords are still vulnerable to dictionary attacks (Ding and Horster, 1995).

With the proliferation of mobile devices, new authentication schemata that were based on graphical password input emerged (Biddle, et al., 2012). They rely on the efficiency of the human brain to accumulate visual information, making a graphical password easier to recall (Standing, et al., 1970). However, graphical passwords are also vulnerable to attacks; shoulder surfing (Tari, et al., 2006), (Zakaria, et al., 2011), brute force attacks (Botelho, et al., 2012) and smudge attacks (Aviv, et al., 2010) are among the most popular in the literature.

The principles that define the design of a graphical password vary. *Passfaces* for example [3] use a 3×3 grid containing photographs that the user clicks to form a password. The usability of such schemes was studied in (Brostoff and Sasse, 2000). However, schemes based on face selection often present security problems, as humans tend to choose faces that attract them (Davis, et al., 2004). Other popular graphical authentication algorithms prompt users to click on different spots on given images. Studies showed that despite their large 'password space', users tend to select specific regions on the images (Thorpe and van Oorschot, 2007). As a result, this biased input produces passwords with high predictability (van Oorschot and Thorpe, 2011). Additionally, the formation of a graphical password involves the human nature, thus, it might be influenced by behavioural heuristic rules, making a scheme vulnerable to image-based dictionary attacks (van Oorschot and Thorpe, 2008).

The Android pattern lock screen schema can be seen as a mutation of previous algorithms. A characteristic example is the *Draw a Secret* (DAS) method that was used to serve early mobile devices (Jermyn, et al., 1999). Users have to draw shapes on an $N\times N$ grid to authenticate. A variation of the scheme is the *Background Draw a Secret* (BDAS) (Dunphy and Yan, 2007), which adds a background image to the grid to improve its usability. Another user authentication method that could be seen as the closest to the Android pattern lock screen is the *Pass-Go* scheme (Tao and Adams, 2008). The method is based on the introduction of nodes (indicators) that help users to form edges and well-defined lines (very similar to the pattern lock). Recent proposals aim to enhance the security of graphical passwords facilitating haptic parameters such as pressure and velocity to the final authentication schema (Orozco, et al., 2006). Others try to distinguish different drawing styles based on the user's personality (Gao, et al., 2008).

The rules for the creation of an Android pattern are simple. The pattern must connect at least 4 nodes. Its length cannot exceed 9 nodes given that a node can be visited only once. In addition, the pattern will always connect the first node, which is along its path. This means that it is not feasible to 'jump' over a node. Finally, a pattern can cross an already visited node to connect a neighbour node.

Some vulnerabilities of the Android pattern lock screen were exposed in (Aviv, et al., 2010). With the use of a camera, smudge attacks were performed on smartphone screens to recover traces and oily residues left by their owners. The overall password space of the authentication scheme was also calculated (using brute force methods). The authors in (Andriotis, et al., 2013) replicated these experiments and were particularly interested in human factors that might affect the choice of a pattern. They investigated the occurrence of specific attributes such as sub-patterns and starting points and combined smudge attacks with their conclusions to reveal patterns drawn on smartphones. In a recent work, Uellenbeck et al. (2013), studied the actual user choices of patterns with a large-scale user study. They evaluated the strength of the patterns and argued that even a small change in the pattern layout can make the authentication more secure.

Our work is inspired by (Aviv, et al., 2010), (Andriotis, et al., 2013), (Uellenbeck, et al., 2013) and our goal is to further examine their validity by conducting a survey designed for actual Android devices. The basic differentiation from these works is that our collected data do not suffer from problems introduced when the participants do not interact directly with a device, by using pen-and-paper or online surveys.

3 Methodology

Our work aims to reveal behavioural heuristic rules that might affect the formation of patterns in Android devices. Our goal is to simulate the user authentication scheme and collect graphical passwords. This avoids the potential bias that is introduced when the survey participants are not interacting with a mobile device while forming their passwords (e.g. with a computer monitor using the mouse), which is a considerable limitation of previous studies (e.g. (Andriotis, et al., 2013)).

To this end, we developed an application (app), which was distributed through *Google Play*, i.e. Android's official app marketplace. Survey participants installed our app to their mobile devices and answered demographic questions, namely gender, age, educational level, their linguistic characteristics (their native written language) and their handedness. Then, they evaluated their understanding about computer security, they were asked if they used any lock screen security measure and clarified the reason for this choice. Then, similarly to (Andriotis, et al., 2013), they drew two patterns: (a) a usable pattern (easy to remember and use) and (b) a secure pattern (more complicated). The participants were allowed to draw the same pattern for the two categories. Finally, they selected the pattern they would prefer to use on their device (Appendix A includes the structure of the questionnaire).

The app was also communicated via social media and in a variety of university related groups (e.g. CSS- University of Bristol Computer Science Society), but the distribution of the app through the *Google Play* contributed to the diversity of our sample. Anonymity was assured and duplicate entries were discarded during analysis.

We start our analysis with basic statistic measures, i.e. average mean μ of sets of data using the standard arithmetic mean formula, and, the standard deviation σ of the set of values. Then, we continue our analysis by examining (a) pattern complexity and (b) pattern symmetry.

3.1 Pattern Complexity

Our analysis is based on the assumption that security involves complexity when we are dealing with passwords; the more complex a pattern is, the more secure it is considered to be. Based on previous literature (Sun et. al, 2014), we set four metrics to measure the complexity of a pattern (c.f. Figure 1a. for the positioning of nodes in the grid), namely:

- *Pattern length* is the number of the nodes that constitute a pattern.
- *Directional Changes* are encountered when three consecutive nodes do not form a straight line (for example (364) or (786)).
- *Overlapping nodes* are the nodes that are crossed more than once.
- *Knight moves* are the edges that connect distant nodes (for example 07 or 05).

3.2 Pattern Symmetry

We define two types of symmetry for the Android pattern lock screen:

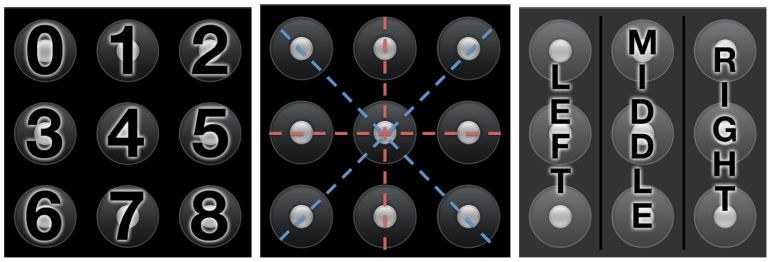
- *Line of Symmetry* is a straight line (defined by 3 consecutive nodes) that divides the pattern into two parts, which are mirror images to each other. Our definition initialises the lines (048) (147) (246) (345) as Lines of Symmetry for the Android pattern lock screen (Figure 1b).
- *Rotational Symmetry* happens when the pattern can be rotated by 180° and still looks the same without taking into consideration its directionality. Thus, node 4 will be considered as the centre point of the Rotational Symmetry (for example Figure 3(a) depicts a pattern with Rotational Symmetry).

We provide more examples of symmetric shapes: Figure 3(b) shows a symmetric pattern with Line of Symmetry (147), and Figures 3(e),(g) depict symmetric patterns with Line of Symmetry (246).

3.3 Usability Features

In this work we study how factors, such as handedness and linguistic style, affect (or not) the conception of a pattern as usable and effective. Thus, a major part of our analysis considers the handedness and the native written language of the respondents, particularly the direction of writing. The respondents had to choose their answers from a list, specifically: a) left-handed, b) right-handed, c) ambidextrous. Similarly, the list for native written language and style included: a) Left-To-Right Latin Alphabet (e.g. English, Spanish, German), b) Left-To-Right Cyrillic Script (e.g. Russian, Serbian, Ukrainian), c) Left-To-Right Abugida Style Script (e.g. Hindi, Bengali, Thai), d) Right-To-Left Abjad Style Script (e.g. Arabic, Hebrew, Farsi, Urdu), e) Top-To-Bottom Logographic Style (e.g. Chinese, Japanese, Korean).

We assume that users would be partially influenced by usability features such as their handedness and direction of writing, when they draw patterns. The way they are used to write would probably guide them to start their patterns from specific points using specific parts of their hands, such as their index fingers or thumbs. Also, to easily recall their passwords, they would not add a lot of security attributes in their patterns, making them easier to break.



(a) (b) (c)

Figure 1: a) Node Arrangement, b) Lines of Symmetry, c) Node Allocation

4 Survey Results and Discussion

Out of 388 unique participants 68.6% were male and 25% were female, whereas 6.4% chose not to disclosure their gender. 35.8% of the respondents were between 25 to 39 years old, 30.7% were 16 - 24 years old, 21.6% were under 16, 9.8% were 40 - 64 years old, and the rest 2.1% were over 65. Thus, our results are biased towards younger ages, but as these users constitute the early adopters of technology, we consider that our analysis provides considerable insight to the creation of graphical patterns by Android users. Moreover, as Android is the most popular OS for mobile devices, we regard that our results provide insights about the creation of graphical patterns in other OSes.

The education level of our sample is also diverse. 21.1% of them were postgraduates, 18.3% were graduates, 19.6% were on high-school educational level, 11.9% placed themselves in higher levels of education (doctorate) and 29.1% replied using the choice 'None'. Considering the respondents' computer security literacy, 36.6% replied that they had 'Little or None' knowledge of security, 34.5% had 'Fair Good' understanding, 15.5% knew the fundamentals and 13.4% considered themselves as experienced.

Regarding the use of lock screen mechanisms, 23.5% of the participants use the pattern lock scheme, which was the most popular lock screen mechanism in our sample. Among the rest of the participants, 19.7% use a password, 13.8% prefer the numeric PIN authentication and 12.5% use 'Other methods'. Finally, 30.5% did not use any authentication mechanism, which means that one out of three of the participants do not lock their devices, verifying previous studies (Mylonas et al., 2013).

Furthermore, w.r.t the reason their device gets locked our results suggest that: 31.7% protect their personal data, 28.6% prevent people fiddling with their phone, 11.2% prevent friends and family making calls or sending texts, 10.1% avoid device theft, and 18.4% named other reasons. Our study examines the effect of handedness and directionality of the participants' written native language and the respective demographics were: 62.4% right-handed, 24.2% left-handed, 7.2% ambidextrous, and 6.2% chose not to reveal their

handedness ('Unknown'). The majority of the respondents (65.7%) chose 'Left-To-Right' Latin writing style as their native language and 8.5% used the 'Right-To-Left' reply, 'Left-To-Right Abugida' and 'Top-To-Bottom Logographic' were chosen by 5.7% respectively, and 4.3% chose the 'Left-To-Right' Cyrillic option.

Our analysis revealed that only 29% of the participants entered two different patterns - most of them preferred to provide the same patterns for both categories (simple and complex). While the reasons for this outcome fall outside the scope of the current work, this might suggest that they do not understand pattern complexity or do not know how to create a complex pattern. The results suggest that the majority of participants (60.8%) preferred the simple pattern, 12.6% preferred the complicated one, and 26.5% replied that they would use something between the simple and the complicated pattern. This is a first and clear indication that most of the survey participants prefer usability against security when creating a graphical password for their mobile device. This trend led us to focus our analysis on simple patterns, to investigate the characteristics and attributes that make them usable.

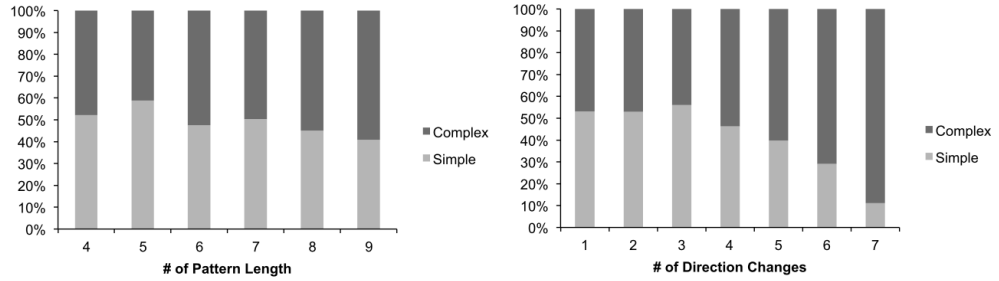
Table 1: Mean Length of the Simple (μ_1) and Complex Patterns (μ_2) for Each Gender Response

<Please insert here Table 1 >

Table 1 presents a dissection of the pattern's length, which is one of the basic characteristics that constitute the complexity of a pattern (Aviv and Fichter, 2014). The results indicate that if an individual is asked to input a simple and then a complicated pattern, it is more likely for the complicated pattern to have larger length. Despite the fact that only 29% of the participants entered two different patterns, there is still a strong indication that secure patterns tend to cover more nodes of the grid. The overall mean length of the simple patterns was 6.22 and the mean length of the complicated was 6.56. This is a notable increase if one considers the limitations of the *3×3* grid. The direction changes used for secure passwords are also an attribute that makes a pattern more complex. Figures 2a and 2b depict a comparison of lengths and directional changes that simple and complex patterns present. The results suggest that a complex shape is usually longer than a simple one. In addition, easy to use patterns present less directional changes than the more complicated ones.

Our results verify the findings presented in (Andriotis, et al., 2013) about the complexity of patterns, regarding their lengths and directional changes. Andriotis et al. (2013) showed that the mean length of an 'easy' pattern was 6.19, whereas the mean length of a 'secure' pattern was 6.64. Also, the average number of directional changes was 2.74 for the 'easy' and 3.57 for the 'secure' patterns. The contribution of the current work can be stressed by the fact that in this study we had a larger number of participants. Furthermore, the respondents used their own devices to form the passwords, thus the user authentication simulation was highly realistic.

The rest of the discussion focuses on the analysis of the usability features of the 'easy' patterns set. Thus, the fact that only 29% of the participants provided a different 'secure' pattern does not affect the merits of our work, as we focus on the 'simple' patterns, which were provided by all respondents.



(a) (b)

Figure 2: Comparison between Simple and Complex Patterns Considering their a) Lengths and b) Directional Changes

4.1 Most Popular Patterns

Despite the relatively wide password space the Android pattern lock screen mechanism provides, some specific shapes were more popular in our survey. These shapes resemble letters (or numbers) of the Latin alphabet, such as Z, M, N, L. Figure 3 presents the most popular patterns that were used by approximately 30% of the participants of our survey. The pattern in Figure 3(a) was chosen by 9% of the respondents and it seems to be the most common shape we could expect to see.

Table 2: Symmetric Shapes in Our Set

<Please insert here Table 2 >

Moreover, Figures 3(a),(c),(f),(j) present patterns with Rotational Symmetry and Figures 3(b),(e),(g) are also symmetric - with Line of Symmetry, as discussed in Section 3.2. Overall, 70% of the top patterns are symmetric and this can be an explanation for their popularity - excluding the fact that these shapes reconstruct well-known symbols. In terms of complexity, the top patterns are fairly simple. The top eight have less than three directional changes (five of them present just 1 or 2 directional changes). However, most of these top patterns have a fairly large length, with six out of ten using seven or more nodes. Thus, our results prove that a lengthy pattern is not always a secure pattern. A secure pattern must contain more characteristics to be less predictable. Finally, the aforementioned finding can be used to create graphical dictionary attacks for pattern lock screens.

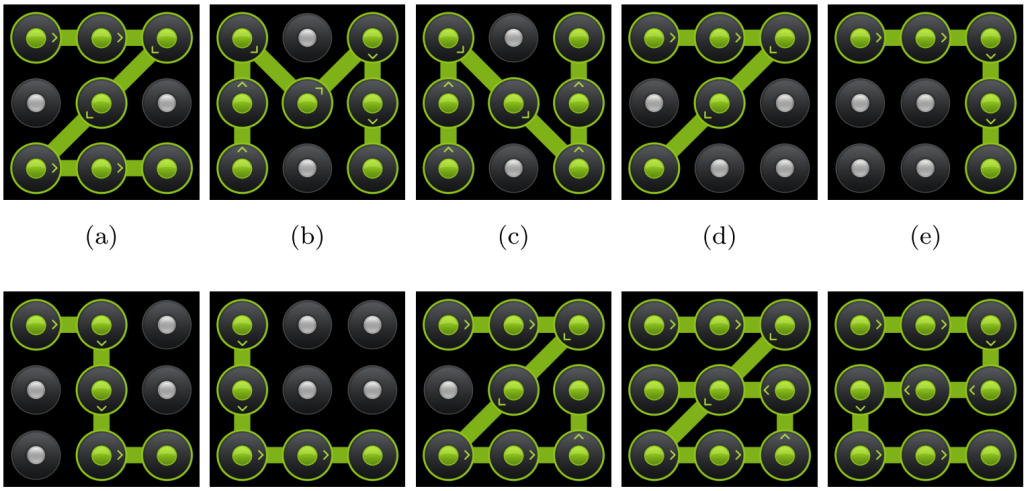


Figure 3: Most Popular Patterns

4.2 Symmetric Patterns

The presence of symmetry in the most popular patterns urged us to examine if any particular heuristic rule exists behind the pattern formation, which makes symmetry a fundamental feature for its construction. Therefore, we investigated the symmetric attributes (definitions in Section 3.2) of all patterns that were collected (simple and complex). Our results show that only 28.54% of the patterns in our set were symmetric. Among them, 20.85% included Rotational Symmetry and 7.69% had a kind of linear symmetry. Table 2 illustrates that line (147) is the most common Line of Symmetry.

Table 2 also indicates that patterns with Rotational Symmetry are the most common symmetric shapes (73.05%). This is reasonable if one considers the proliferation of such graphical passwords in the pattern set. Patterns such as (6304258), (0364852), (0367852) are quite common and symbolize letters (M, W, U), having the line (147) as Line of Symmetry.

In general, our results indicate that symmetry is a valuable attribute that participates as a behavioural and visual asset to our understanding of a graphical password. However, more complex patterns do not present a form of symmetry. Thus, the usability of a pattern can be enhanced by symmetric concepts we preserve in our minds. This bias results in very predictable patterns that are also quite common in our set (c.f. Section 4.1).

4.3 Usability Study

Previous studies investigated various features that can be extracted from a pattern (such as the starting positions or common bigrams and trigrams) and presented results disclosing the existence of certain biases during the formation of the graphical passwords (Andriotis, et al., 2013), (Uellenbeck, et al., 2013). This work not only validates these results, but it offers additional information about the features that make a pattern to appear as usable. For this reason, we also studied the effects of handedness and linguistic style, making the assumption that individuals holding the device with a specific hand (left or right), might behave differently when entering patterns. Additionally, the way the participants write might affect the way they form graphical passwords for their mobile devices. Since the survey participants prefer to use simple patterns, which is an indication that simple patterns are considered as more usable, the rest of this sub-section discusses our findings for the set of simple patterns.

Table 3: Handedness Effect on Starting Position Choice

<Please insert here Table 3 >

Table 4: Native Writing Language Effect on Starting Position Choice

<Please insert here Table 4 >

4.3.1 Starting Position

Previous studies revealed that users tend to start their patterns from the top left corner. Also, other popular starting points in (Andriotis, et al., 2013) were nodes 2 and 6. Table 3 summarizes the effect of the participants' handedness on the start of the simple pattern. Position 0 was the most popular starting position (54.4% of respondents). Moreover, it was more likely to be chosen by left-handed than right-handed respondents (with 62.8% and 50.8%, respectively). Regarding the second most popular start of simple patterns the respondents tended to prefer position 6.

We also examined the starting point position in relation to the direction of the native text, as shown in Table 4. One would assume that Left-To-Right writers would be more inclined to start on the left side of the pattern space. The results shown at Table 4 depict this trend and position 0 is still the most popular starting position. Right-To-Left writers selected position 0 less than others (45.5% of all Right-To-Left users). Node 2 (the top-right position) was chosen by the 18.2% of Right-To-Left respondents, over twice the rate of Left-To-Right respondents (8.5%). Top-To-Bottom writers also tend to pick the top row of positions as a starting point. Thus, these results confirm the hypothesis that the direction of writing affects the pattern construction, particularly the selection of the pattern's starting point. Our results also verify the findings in (Andriotis, et al., 2013), (Uellenbeck, et al., 2013) considering the pattern's starting point. Another interesting finding is that node 5 is rarely selected as the starting point (only 1.1% of the sample). Table 4 also demonstrates that number 6 is a popular starting node.

4.3.2 Monograms

We define as monograms the distinct nodes in a pattern. Each position can occur at most once and we are interested in their frequencies. Our analysis reveals that node 4 is the most popular monogram (appearing in 86% of the patterns). In addition, we collected the frequency of each monogram in relation to the direction of native writing and the handedness of the participants (c.f. Table 5). Table 5 does not provide any distinctive habits or biases. However, the results suggest that nodes 2 and 8 (located at the right hand side) were the most visited nodes from the Right-To-Left participants, excluding the 'popular' node 0 and the central node 4.

Table 5: Frequency of Monograms Based on Direction of Native Writing

<Please insert here Table 5 >

4.3.3 Bigrams

A bigram is a sub-pattern that consists of two connected nodes. The ten most popular bigrams in our survey are presented in Figure 4. Our results suggest that horizontal directionality is more likely to occur, as the four most frequent bigrams are the (01), (12), (67) and (78). We also examined any possible association of the bigram frequencies between bigrams, native writing direction and handedness (c.f. Tables 6-7).

Table 6 reveals a high occurrence of the bigrams (67) and (78) at Top-To-Bottom native language respondents. This may stem from the popularity of the L shaped pattern, which was the 6th most popular pattern. The L shaped pattern is noticeably the only pattern that starts with a downward direction in the top 10 patterns. However, there is no obvious difference between Left-To-Right and Right-To-Left respondents. Table 7 reveals a higher rate of right-handed respondents using bigrams on the right hand side, such as (25) and (58), while left-handed participants are more likely to use left side bigrams, such as (63). The difference of frequency between left-handed and right-handed respondents (namely 7%) could be considered a fair indication given that the average response rate of these bigrams is around 20%.

Table 6: Frequency of Bigrams Based on Direction of Native Writing

<Please insert here Table 6 >

Table 7: Frequency of Bigrams Based on Handedness of Respondent

<Please insert here Table 7 >

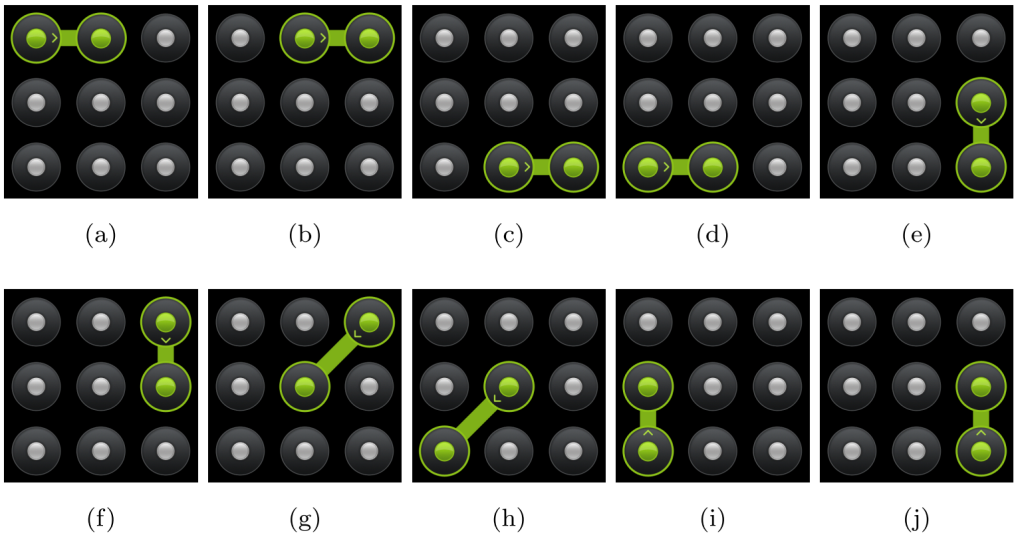


Figure 4: Most Popular Bigrams

4.3.4 Trigrams

The most popular trigrams are presented in Figure 5. Apparently, many of these trigrams contain a combination of two bigrams from section 4.3.3. The first observation is that (012) is the most frequent trigram, appearing in almost one third of the patterns. Our results might indicate a possible association of the pattern formation with native writing directionality and handedness, as shown in Table 8 and Table 9, respectively. The results do not suggest a considerable alteration of the behavior between Left-To-Right and Right-to-Left participants. However, Table 8 indicates that Top-To-Bottom writers did not produce trigrams such as (630) and rarely used other trigrams such as (785). The directionality of such sub-patterns implies a Bottom-To-Top notion of writing and the participants with a Top-To-Bottom writing style did not use them. Additionally, right-handed respondents tend to use trigrams located at the right hand-side, such as (258), more frequently than the left-handed (c.f. Table 9).

These findings enhance our initial assumptions that the usability of graphical password scheme depends on the handedness and the native writing of the user. Our analysis demonstrated the most common and popular patterns and sub-patterns and indicated that the way participants write influences the formation of pattern.

Table 8: Frequency of Trigrams Based on Direction of Native Writing

<Please insert here Table 8 >

Table 9: Frequency of Trigrams Based on Handedness of Respondent

<Please insert here Table 9 >

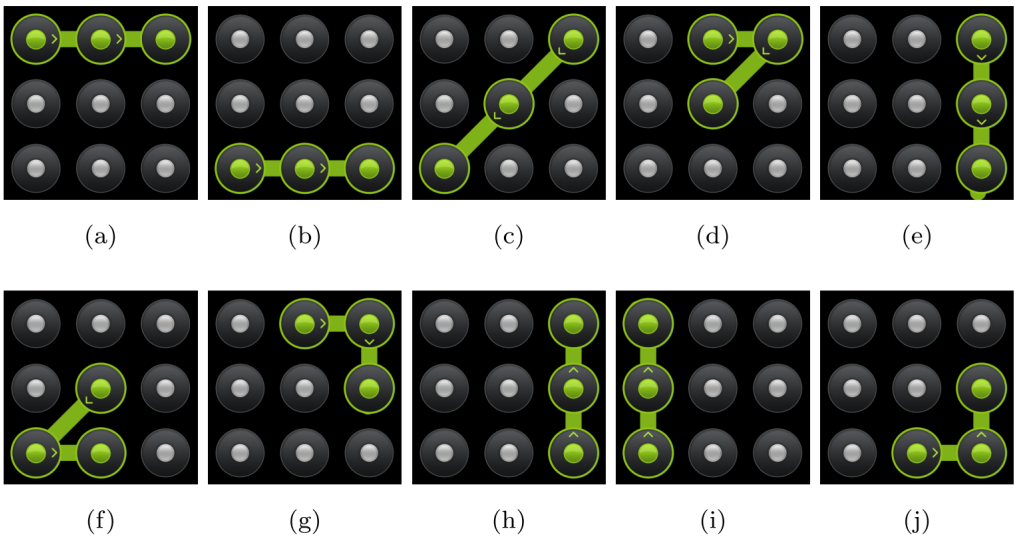


Figure 5: Most Popular Trigrams

4.4 Security Study

As already mentioned in Section 4, approximately 29% of the respondents provided two different patterns; a simple and a more complex. The complexity of a pattern is closely related to its security. This work provided details about the length and the directional changes (Section 4) and concatenated them in Table 1. A comparison between our findings and the results presented in (Andriotis, et al., 2013) showed that the conception of a pattern's complexity is closely related to its length and its directional changes. In addition, this work examined other attributes that could project different aspects of complexity, i.e. overlapping nodes and knight moves (c.f. Section 3.1).

Focusing on the participants who created two different patterns, the overlapping nodes and the knight moves within the set of secure patterns were examined. Table 10 shows the occurrence of the features; the second column presents their percentage inside the whole set

with the secure patterns and the third column shows the number of overlapping nodes or knight moves that occurred among the complex patterns with the specific characteristics. For instance, among the patterns that contained at least one overlapping node (18.83% of the total 'secure' patterns), only 6.9% were shapes that had 3 overlapping nodes. Table 10 illustrates that among the secure patterns only 18.83% had at least one overlapping node and 9.09% contained at least one knight move. The patterns that had one overlapping node were the 93.1% of the aforementioned set. The results show that even though participants aim to create a secure pattern, they do not form passwords with overlapping nodes. When they do so, they just overlap the shape once.

The same observations can be made for knight moves. It is somewhat hard to include a knight move in the pattern, not only because one might not think or know the existence of such an option, but also because the grid is very narrow and thus it is physically hard to reach two distant nodes. Table 10 confirms the assumption. Only 9.09% of the secure patterns contained at least one knight move. Among them, the majority (64.29%) contained one knight move, 14.29% contained two and 21.42% included seven knight moves. The latter patterns were representations of asteroid shapes and each edge was a knight move. Finally, only 2.6% of the secure patterns contained both overlapping nodes and knight moves.

As a conclusion, even though overlapping nodes and knight moves increase the complexity of a pattern, our results show that it is less likely for users to include them in their (secure) patterns. This might stem from the lack of sufficient guidance from the OS, when users enter for the first time a pattern to lock the screen. Thus, our results suggest that users who create patterns needed more training regarding the creation of secure patterns.

Table 10: Overlapping Nodes and Knight Moves within the Secure Patterns Set

<Please insert here Table 10 >

5 Case Study

The results regarding the usability and security features of Android's pattern lock screen will be used herein to demonstrate vulnerabilities that might occur by the predictability of the users' behaviour. To serve this purpose we developed a brute force program that produces all available patterns (namely 389,112 unique patterns).

We will study the case where a usable (simple) pattern is entered as a password in an Android device. Our survey suggests that more that 50% of the users will start their patterns from the top left corner and over 85% of the provided patterns will cross node 4. Hence, by filtering the patterns with shapes that include these characteristics we can reduce the password space (c.f. Table 11). According to the results of our survey, these candidates are almost the half of the population who use the pattern lock screen and prefer a convenient password.

The impact of biased input on user authentication can be realized by focusing on the set of patterns with the most popular length, i.e. 6 nodes. The overall number of such patterns according to our results from the brute force method is 26,016. However, the available password space for the users who start from node 0 and cross node 4, shrinks significantly (approximately 90%, c.f. Table 11).

Our results suggest that participants did not use knight moves, even when they were creating a secure pattern. In the usable pattern set, 9.18% of the respondents used overlapping nodes and only 3.78% used knight moves. Therefore, a usable pattern is less likely to contain a knight move. If we focus again on usable patterns of the previous set, which start from node 0, cross node 4 and also omit knight moves, then the password space for patterns of length 4, 5 and 6 shrinks even more (c.f. Table 12). Finally, the password space can be further decreased by including more findings from the user study. For instance, one of the most popular trigrams in our survey was (012). The addition of this parameter to the case study reduces the number of patterns with length six to 20, passwords of length five to 6 and there is only one pattern with length four (0124) (c.f. Table 12).

This case study demonstrates that the results of our survey can significantly reduce the password space of the Android pattern lock screen. Our findings can be combined with data from the physical device, directly from its screen (e.g. traces or residues originated by the use of the phone), to increase the likelihood of recovering the graphical password. Such traces could be some nodes or edges (in other words bigrams and trigrams) of the pattern.

Table 11: Number of Possible Patterns for the 9-node Pattern Authentication Scheme with Specific Attributes

<Please insert here Table 11>

Table 12: Decreasing the Password Space Using More Attributes from the Survey

<Please insert here Table 12>

6 Conclusions and Future Work

Creating a graphical password is a process that involves visual stimuli, understanding of security and subconscious biases driven by the way we are used to act in our daily lives. In this paper, we developed an Android application to conduct a survey that would collect sets of usable and secure patterns. We analyzed the collected patterns to study the existence of heuristic rules that may affect the formation of such a graphical password. Subsequently, we used our findings in a case study to stress the importance of the balance between usability and security. In our case study, we were able to reduce the password space of patterns with length 6 by 99.92% (20 choices out of 26,016).

Our work regarding the creation of patterns validates common results presented in previous studies, which used pen-and-paper or online surveys for data collection. Contrarily, in this work we simulated the creation of patterns on real Android devices, which avoids potential bias that is introduced when the survey participants are not interacting with a mobile device while forming their passwords. This work attempts to justify biases such as the trend to start the pattern from the top left node and the inclusion of node 4 to the vast majority of patterns. Also, the survey showed that participants prefer to use a simple pattern rather than a more complex one. We examined the effect that handedness, symmetry and native writing style have on the perception of a usable pattern and we further illustrated the preference to popular shapes that resemble Latin letters. We also defined metrics for pattern complexity (pattern length, directional changes, overlapping nodes and knight moves). We examined their existence in the collected patterns to evaluate the complexity of the participants' patterns and, thus, their security strength.

Our work suggests that users need more training regarding the creation of secure patterns. This holds true as in our survey users (a) opted for usability and not for security with regards to pattern creation and (b) created patterns that can be easily recovered. Currently, when Android users see the interface that enables them to create a pattern, they are presented with simplistic instructions on how to create a pattern that (a) do not explain the importance of the complexity of a pattern and (b) do not list all the available moves (e.g. knight moves). Training users to create more complex patterns by including knight moves, overlapping nodes and random starting points can avoid behavioural attacks as the ones presented in this work.

Entropy is a measure used to describe the uncertainty in a random variable. As future work we plan to compare our empirical results with entropic measures that are commonly used in information theory. Another direction of future research would be the creation of a password meter that warns users about the strength of a chosen graphical password.

Notes

1 'Spoofing fingerprints', https://srlabs.de/spoofing-fingerprints/ (Accessed June 2, 2015).

2 xda developers, '[Android][Guide]Hacking And Bypassing Android Password/Pattern/Face/PI', http://forum.xda-developers.com/showthread.php?t=2620456 (Accessed June 2, 2015).

3 'Science Behind Passfaces', http://www.passfaces.com/enterprise/resources/white_papers.htm, (Accessed June 2, 2015).

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, *in* 'Proceedings of the sixth ACM conference on Security and privacy in wireless and mobile networks', pp. 1--6.

Aviv, A.J., Fichter, D., 2014. Understanding Visual Perceptions of Usability and Security of Android's Graphical Password Pattern, in: Proceedings of the 30th Annual Computer Security Applications Conference, ACSAC '14. ACM, New York, NY, USA, pp. 286–295.

Aviv, A. J.; Gibson, K.; Mossop, E.; Blaze, M. and Smith, J. M. (2010), Smudge attacks on smartphone touch screens, *in* 'Proceedings of the 4th USENIX conference on Offensive technologies', pp. 1--7.

Biddle, R.; Chiasson, S. and Van Oorschot, P. C. (2012), 'Graphical passwords: Learning from the first twelve years', *ACM Computing Surveys (CSUR)* **44**(4), 19.

Bonneau, J. (2012), The science of guessing: analyzing an anonymized corpus of 70 million passwords, *in* 'Security and Privacy (SP), 2012 IEEE Symposium on', pp. 538--552.

Botelho, B. A. P.; Nakamura, E. T. and Uto, N. (2012), Implementation of tools for brute forcing touch inputted passwords, *in* 'Internet Technology And Secured Transactions, 2012 International Conferece For', pp. 807--808.

Brostoff, S. and Sasse, M. A. (2000), Are Passfaces more usable than passwords? A field trial investigation'People and Computers XIV - Usability or Else!', Springer, , pp. 405--424.

Davis, D.; Monrose, F. and Reiter, M. K. (2004), On User Choice in Graphical Password Schemes, *in* 'USENIX Security Symposium', pp. 151--164.

Ding, Y. and Horster, P. (1995), 'Undetectable on-line password guessing attacks', *ACM SIGOPS Operating Systems Review* **29**(4), 77--86.

Dunphy, P. and Yan, J. (2007), Do background images improve Draw a secret graphical passwords?, *in* 'Proceedings of the 14th ACM conference on Computer and communications security', pp. 36--47.

Forget, A.; Chiasson, S.; van Oorschot, P. C. and Biddle, R. (2008), Improving text passwords through persuasion, *in* 'Proceedings of the 4th symposium on Usable privacy and security', pp. 1--12.

Gao, H.; Guo, X.; Chen, X.; Wang, L. and Liu, X. (2008), Yagp: Yet another graphical password strategy, *in* 'Computer Security Applications Conference, 2008. ACSAC 2008. Annual', pp. 121--129.

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

Mylonas, A.; Kastania, A.; and Gritzalis, D. (2013), 'Delegate the smartphone user? Security awareness in smartphone platforms', *Computers & Security*, Vol 34, pp. 47-66.

van Oorschot, P. C. and Thorpe, J. (2011), 'Exploiting predictability in click-based graphical passwords', *Journal of Computer Security* **19**(4), 669--702.

van Oorschot, P. C. and Thorpe, J. (2008), 'On predictive models and user-drawn graphical passwords', *ACM Transactions on Information and system Security (TISSEC)* **10**(4), 5.

Orozco, M.; Malek, B.; Eid, M. and El Saddik, A. (2006), Haptic-based sensible graphical password, *in* 'Proceedings of Virtual Concept', pp. 1--4.

Sasse, M. A.; Brostoff, S. and Weirich, D. (2001), 'Transforming `the weakest link' - a human/computer interaction approach to usable and effective security', *BT technology journal* **19**(3), 122--131.

Standing, L.; Conezio, J. and Haber, R. N. (1970), 'Perception and memory for pictures: Single-trial learning of 2500 visual stimuli', *Psychonomic Science* **19**(2), 73--74.

Sun, C.; Wang, Y.; and Zheng, J. (2014), ‘Dissecting pattern unlock: The effect of pattern strength meter on pattern selection’, Journal of Information Security and Applications 19(4), 308--320.

Tao, H. and Adams, C. (2008), 'Pass-Go: A Proposal to Improve the Usability of Graphical Passwords.', *IJ Network Security* **7**(2), 273--292.

Tari, F.; Ozok, A. and Holden, S. H. (2006), A comparison of perceived and real shoulder-surfing risks between alphanumeric and graphical passwords, *in* 'Proceedings of the second symposium on Usable privacy and security', pp. 56--66.

Thorpe, J. and van Oorschot, P. C. (2007), Human-seeded attacks and exploiting hot-spots in graphical passwords, *in* '16th USENIX Security Symposium', pp. 103--118.

Uellenbeck, S.; Dürmuth, M.; Wolf, C. and Holz, T. (2013), Quantifying the security of graphical passwords: the case of android unlock patterns, *in* 'Proceedings of the 2013 ACM SIGSAC conference on Computer and communications security', pp. 161--172.

Zakaria, N. H.; Griffiths, D.; Brostoff, S. and Yan, J. (2011), Shoulder surfing defence for recall-based graphical passwords, *in* 'Proceedings of the Seventh Symposium on Usable Privacy and Security', pp. 1--12.

Appendix
A. Online Questionnaire

The following list includes the different options that were presented to the survey participants by the Android application we implemented.

- Gender
  - Male
  - Female
  - Undisclosed
- Age
  - Under 16
  - 16-24
  - 25-39
  - 40-64
  - Over 65
- Level of Education
  - None or Very Little
  - Second School / High School
  - Further Education
  - Graduate Level
  - Postgraduate Level
- Handedness
  - Left-Handed
  - Right-Handed
  - Ambidexterity
- Native Written Language
  - Left-To-Right Latin Alphabet (e.g. English, Spanish, German)
  - Left-To-Right Cyrillic Script (e.g. Russian, Serbian, Ukrainian)
  - Left-To-Right Abugida Script (e.g. Hindi, Bengali, Thai)
  - Right-To-Left Abjad Script (e.g. Arabic, Hebrew, Farsi, Urdu)
  - Top-To-Bottom Logographic (e.g. Chinese, Japanese, Korean)
- Understanding of Computer Security
  - Very little knowledge
  - Some fundamental knowledge
  - Fairly good understanding and knowledge
  - Expert and highly experienced
- Current usage of Lockscreen Security
  - Don't own a device
  - Don't use any Lockscreen Security
  - Use PIN Authentication
  - Use password Authentication
  - Use pattern Authentication
  - Use other form of Authentication
- What best describes the reason for current Lockscreen Security
  - Don't own a device or don't use any Lockscreen Security
  - To protect personal data
  - To protect sensitive business or organization data
  - To stop family and friends making calls, emails, texts, etc. on phone
  - To avoid device theft issues
  - To stop people fiddling with my phone
- Entry of a simple, easy to remember Lockscreen Pattern
- Entry of a more complicated, hard to remember Lockscreen Pattern
- Preference on which pattern to use
  - Simple but easier-to-remember pattern
  - Complicated but harder-to-remember pattern
  - Pattern somewhere between simple and complicated

A Study on Usability and Security Features of the Android Pattern Lock Screen

Table 1: Mean Length of the Simple (μ_1) and Complex Patterns (μ_2) for Each Gender Response

	Simple		Complex		$\lvert\mu_1 - \mu_2\rvert$
	μ_1	Σ	μ_2	σ	
Male	6.19	1.688	6.63	1.778	0.44
Female	6.29	1.708	6.46	1.750	0.18
Other	6.32	1.676	6.20	1.732	0.12
All	6.22	1.689	6.56	1.768	0.34

Table 2: Symmetric Shapes in Our Set

Symmetry Type	% in Total	% in Symmetric Set
Rotational	20.85	73.05
Line (147)	5.67	19.86
Line (246)	4.86	17.02
Line (345)	1.01	3.57
Line (048)	0.40	1.42

Table 3: Handedness Effect on Starting Position Choice

Handedness	Start Position of Simple Pattern								
	0	1	2	3	4	5	6	7	8
Ambidexterity	57.1%	0.0%	7.1%	7.1%	3.6%	0.0%	14.3%	0.0%	10.7%
Left-Handed	**62.8%**	4.3%	7.4%	3.2%	7.4%	0.0%	9.6%	2.1%	3.2%
Right-Handed	**50.8%**	5.8%	10.3%	6.2%	1.7%	0.8%	19.8%	2.1%	2.5%
All	54.4%	4.9%	**9.3**%	5.5%	3.3%	0.5%	**16.8%**	1.9%	3.3%

Table 4: Native Writing Language Effect on Starting Position Choice

Direction	Start Position of Simple Pattern								
	0	1	2	3	4	5	6	7	8
Left-To-Right	53.4%	4.1%	8.5%	6.1%	4.1%	1.4%	16.3%	2.4%	3.7%
Right-To-Left	45.5%	0.0%	**18.2%**	6.1%	3.0%	0.0%	21.2%	3.0%	3.0%
Top-To-Bottom	**63.6%**	**18.2%**	**9.1%**	0.0%	4.5%	0.0%	4.5%	0.0%	0.0%
All	53.3%	4.6%	9.5%	5.7%	4.0%	**1.1%**	16.0%	2.3%	3.4%

Table 5: Frequency of Monograms Based on Direction of Native Writing

Direction	Frequency of Monogram Contained in Patterns								
	4	0	2	8	6	7	1	5	3
Left-To-Right	84%	77%	69%	69%	66%	67%	65%	65%	64%
Right-To-Left	94%	73%	**91%**	**73%**	70%	61%	67%	70%	70%
Top-To-Bottom	91%	64%	64%	77%	73%	86%	64%	41%	45%
All	86%	75%	70%	70%	67%	67%	65%	64%	63%

Table 6: Frequency of Bigrams Based on Direction of Native Writing

Direction	Frequency of Bigrams Contained in Patterns									
	01	12	78	67	58	25	24	46	63	85
Left-To-Right	38%	32%	28%	24%	24%	23%	20%	19%	21%	21%
Right-To-Left	36%	39%	30%	27%	30%	36%	27%	18%	18%	18%
Top-To-Bottom	45%	32%	**55%**	**50%**	18%	14%	41%	45%	5%	9%
All	38%	32%	30%	26%	24%	24%	22%	21%	20%	20%

Table 7: Frequency of Bigrams Based on Handedness of Respondent

Handedness	Frequency of Bigrams Contained in Patterns									
	01	12	78	67	58	25	24	46	63	85
Ambidexterity	50%	50%	43%	46%	18%	21%	46%	39%	11%	18%
Left-Handed	46%	37%	28%	26%	21%	20%	26%	23%	**26%**	21%
Right-Handed	38%	30%	31%	26%	**26%**	**26%**	22%	20%	19%	19%
All	41%	34%	31%	27%	24%	24%	25%	23%	20%	20%

Table 8: Frequency of Trigrams Based on Direction of Native Writing

Direction	Frequency of Trigrams Contained in Patterns									
	012	678	246	124	258	467	125	852	630	785
Left-To-Right	28%	19%	17%	16%	18%	13%	13%	13%	12%	11%
Right-To-Left	33%	24%	18%	18%	21%	15%	18%	6%	18%	15%
Top-To-Bottom	27%	45%	36%	32%	14%	45%	0%	9%	**0%**	**5%**
All	28%	21%	18%	17%	18%	15%	13%	12%	11%	11%

Table 9: Frequency of Trigrams Based on Handedness of Respondent

Handedness	Frequency of Trigrams Contained in Patterns									
	012	678	246	124	258	467	125	852	630	785
Ambidexterity	46%	39%	39%	32%	14%	29%	14%	11%	7%	11%
Left-Handed	32%	18%	21%	21%	14%	15%	13%	13%	11%	11%
Right-Handed	27%	21%	17%	17%	**21%**	16%	12%	12%	13%	11%
All	30%	22%	20%	20%	18%	17%	12%	12%	12%	11%

Table 10: Overlapping Nodes and Knight Moves within the Secure Patterns Set

Features	Total	Denomination
Overlapping Nodes	18.83%	93.1% 1 node 6.9% 3 nodes
Knight Moves	9.09%	64.29% 1 move 14.29% 2 moves 21.42% 7 moves
Both	2.6%	1 node & 1 move

Table 11: Number of Possible Patterns for the 9-node Pattern Authentication Scheme with Specific Attributes

Attributes	Length	Unique Patterns
Starts at Node 0	4	154
	5	684
	6	2516
	7	7104
	8	13792
	9	13792
Starts at Node 0 and Crosses Node 4	4	82
	5	456
	6	1948
	7	6152
	8	12944
	9	13792

Table 12: Decreasing the Password Space Using More Attributes from the Survey

Length	Unique Patterns, No Knight Moves	Unique Patterns, No Knight Moves + (012)
4	44	1
5	160	6
6	442	20