Short Paper – Pass-O: A Proposal to Improve the Security of Pattern Unlock Scheme

Harshal Tupsamudre Vijayanand Banahatti
Sachin Lodha Ketan Vyas
TCS Research, India
{firstname.lastname}@tcs.com

ABSTRACT

The graphical pattern unlock scheme which requires users to connect a minimum of 4 nodes on 3X3 grid is one of the most popular authentication mechanism on mobile devices. However prior research suggests that users' pattern choices are highly biased and hence vulnerable to guessing attacks. Moreover, 3X3 pattern choices are devoid of features such as longer stroke lengths, direction changes and intersections that are considered to be important in preventing shoulder-surfing attacks. We attribute these insecure practices to the geometry of the grid and its complicated drawing rules which prevent users from realising the full potential of graphical passwords.

In this paper, we propose and explore an alternate circular layout referred to as Pass-O which unlike grid layout allows connection between any two nodes, thus simplifying the pattern drawing rules. Consequently, Pass-O produces a theoretical search space of 9,85,824, almost 2.5 times greater than 3X3 grid layout. We compare the security of 3X3 and Pass-O patterns theoretically as well as empirically. Theoretically, Pass-O patterns are uniform and have greater visual complexity due to large number of intersections. To perform empirical analysis, we conduct a large-scale web-based user study and collect more than 1,23,000 patterns from 21,053 users. After examining user-chosen 3X3 and Pass-O patterns across different metrics such as pattern length, stroke length, start point, end point, repetitions, number of direction changes and intersections, we find that Pass-O patterns are much more secure than 3X3 patterns.

Keywords

Security; Graphical Passwords; Guessing; Shoulder-Surfing

1. INTRODUCTION

Today mobile devices are being used to perform a multitude of tasks including banking, mailing, social networking, shopping and browsing. Consequently, these portable devices are gateway to sensitive information such as credit card details, passwords and emails. To prevent unauthorised use of mobile devices several authentication mechanisms *e.g.*, textual passwords, numerical passwords (PINs), graphical passwords and biometrics are available. However, users perceive 3X3 patterns to be more usable as compared to textual passwords and PINs [15]. Further, biometric alternatives such as fingerprints are considered to be less secure than PINs, textual passwords and 3X3 patterns [2]. Hence, 3X3 patterns have received wide attention from the security community.

Although the grid-based pattern unlock scheme is considered as usable, the recent security studies [6, 13] show that human-generated graphical patterns are vulnerable to guessing attacks. In particular, users' pattern choices are highly biased and only a small fraction of the theoretical pattern space is actually used. Simple pattern shapes resembling English letters such as 'Z', 'S' , 'L', 'N', 'M' are quite popular among users. Since the 3X3 pattern space is already limited (3,89,112 combinations), the weak pattern choices of users make the problem much worse. Increasing the grid size to 4X4 does not solve this problem as 4X4 patterns are simply extended versions of popular 3X3 patterns [6].

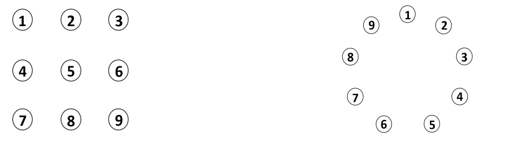
Yet another threat to the grid-based authentication scheme comes from shoulder-surfing attacks [10, 11]. These attacks are more likely to succeed since users choose simple patterns [6, 13] containing only horizontal (1 → 2) or vertical lines (1 → 4) which could be easily memorized by an observer. The features such as longer length, knight moves, direction changes and intersections which are necessary to counter shoulder-surfing attacks [4, 10, 11] are mostly absent in the user-chosen patterns. We attribute these insecure practices to the grid-based layout and its complex pattern drawing rules.

The rules are as follows, (a) the pattern should be drawn using straight lines and without lifting the hand, (b) the pattern should connect at least 4 nodes and a maximum of 9 nodes, (c) a node cannot be connected more than once, and (d) an unconnected node cannot be skipped if it lies along the path of a pattern.

The last rule (d) especially limits the space of 3X3 patterns as it does not allow connectivity between any two nodes unconditionally. For instance, users cannot connect 1 → 3 in the grid unless the node 2 is already connected (Figure 1a). In this paper, we develop an intuitive circular layout which unlike grid layout allows a direct connection between any two nodes, therefore yielding a theoretical space of 9,85,824 patterns, 2.5 times greater than 3X3 grid layout

ASIA CCS '17, April 02 - 06, 2017, Abu Dhabi, United Arab Emirates

ISBN 978-1-4503-4944-4/17/04. . . $15.00
DOI: http://dx.doi.org/10.1145/3052973.3053041



(a) Grid Layout (b) Circular Layout

Figure 1: 3X3 grid layout and Pass-O layout

(3,89,112). We refer to this circular layout as *Pass-O*.

Contributions. In this paper, we compare the security of 3X3 and Pass-O patterns against both guessing attacks and shoulder-surfing attacks. We study them analytically as well as empirically. Specifically, our contributions are:

- *Theoretical Analysis* - We perform theoretical analysis of all valid 3X3 patterns and Pass-O patterns. We show that Pass-O layout not only provides a large search space than grid-based layout but also patterns drawn on Pass-O are visually more complex in terms of intersections.
- *Largest ever Security Study* - To estimate the security of 3X3 and Pass-O patterns against guessing and shoulder-surfing attacks, we conduct a large-scale user study and collect 69,797 3X3 patterns and 53,393 Pass-O patterns from 21,053 users. To the best of our knowledge this is the largest patterns study reported till date.
- *Resistance to Shoulder-Surfing* - We compare the security of 3X3 and Pass-O datasets across different metrics such as repetitions, pattern length, stroke length, start point distribution, end point distribution, number of direction changes and intersections. The average length of Pass-O patterns is 7.46 while for 3x3 patterns it is 6.92. Further, the average number of intersections (3.47) in Pass-O patterns is significantly larger than that of 3X3 patterns (0.63). Thus, as compared to 3X3 patterns, Pass-O patterns are visually more complex and therefore more resistant to shoulder-surfing attacks.
- *Resistance to Guessing* - The large-scale data allow us to provide a more reliable estimate of guessing resistance of users' pattern choices. We find that the security of 3X3 patterns is much less than that reported in the literature [6,13]. Our Markov model based guessing algorithm cracked 18.55% of 3X3 patterns but only 11.51% of Pass-O patterns within first 20 guesses. Using the partial guessing entropy metric [8], we find that the security of the first 10% ($G_{0.1}$) of 3X3 patterns is just 5.80 bits (less than two random digits) while the security of Pass-O patterns is 7.06 bits (more than two random digits).
- *Top 500 patterns* - We also share a list of top 500 3X3 and Pass-O patterns with the research community [1].

Notations. For convenience, all nodes in 3X3 grid and Pass-O are labelled from 1 to 9 (Figure 1). Specifically, nodes in 3X3 grid are labelled in row-major order, the upper-left node is labelled as 1 and the bottom-right node is labelled as 9. Nodes in Pass-O are labelled in clockwise ascending order starting from the top-most node which is labelled as 1. A pattern can therefore be represented as an ordered sequence of nodes, *e.g.,12369*. We refer to the number of nodes connected in a pattern as pattern length or simply length. Thus, the pattern length of *12369* is 5. Patterns can also be viewed as a sequence of line segments. For instance, the pattern *12369* is composed of 4 line segments, $1 \rightarrow 2$, $2 \rightarrow 3$, $3 \rightarrow 6$ and $6 \rightarrow 9$. The number of line segments in a l length pattern is simply $l - 1$. We use symbols μ for average, σ for standard deviation and $\tilde{x}$ for median.

2. THREAT MODEL

We consider the threat posed to pattern unlock scheme by guessing as well as shoulder-surfing attacks. For more information about the related work on these attacks, we refer the reader to appendix A.

2.1 Guessing Attacks

In this threat model, we assume that an attacker is in possession of the user device (*e.g.*, by theft). Further, we assume that the attacker has no information about the device owner nor about the pattern lock. The only information that the attacker has an access to is the sorted list of most commonly used patterns. The attacker can make a maximum of 20 failed attempts before the device is deactivated and rendered useless [6]. Therefore, immediately after acquiring the device, the attacker draws the first 20 patterns from the sorted pattern list to authenticate.

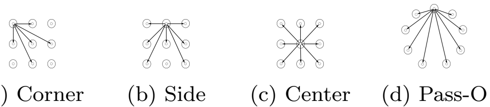
2.2 Shoulder-surfing Attacks

We quote the shoulder-surfing threat model as described in [14] verbatim. A user draws the pattern in a (semi-)public setting. The attacker, who has no previous knowledge about the characteristics (*e.g.*, length) of the drawn pattern, has perfect sight on the display. There are no occlusions and no distracting reflections. The attacker sees the whole authentication exactly once as there is no technical equipment involved (*e.g.*, video recording). Immediately after the attack, the observer gets in possession of the device (*e.g.*, by theft) and redraws the observed pattern to authenticate.

3. THEORETICAL ANALYSIS

To perform theoretical analysis, we wrote a recursive procedure that generates all valid 3X3 and Pass-O patterns. In addition, the procedure also calculates and stores the characteristics of all valid patterns. We focus on the characteristics such as node reachability, size of the search space, pattern length, stroke length and number of intersections.

Reachability. Figure 2 shows the reachability of nodes in both layouts. We classify all nodes in 3X3 grid into three categories, namely *corner nodes, center node and side nodes.* As the name suggests, a corner node is the one located at the corner of the grid {1,3,7,9}. The node 5 located at the center is a center node and the remaining nodes located along the boundary of the grid {2,4,6,8} are referred to as side nodes. A corner node can be connected to 5 other nodes unconditionally and to the remaining 3 nodes conditionally only if the intermediate node along the path is already visited. For instance, the line segment $1 \rightarrow 3$ is possible only if the node 2 is already visited. Similarly, a side node can be connected unconditionally to seven other nodes. The only node in this grid that can be connected to other eight nodes is the center node whereas in Pass-O any node can be connected to the remaining eight nodes.



(a) Corner (b) Side (c) Center (d) Pass-O

Figure 2: Reachability of 3X3 and Pass-O nodes

Total Space. Due to limited reachability of corner and side nodes, 3X3 grid offers only a limited space of 3,89,112 patterns. On the other hand, in Pass-O since every node can be connected to every other node, the total number of l length patterns can be easily computed using the formula ${}^{9}P_{l}$.

Theorem 1. *In a Pass-O with n nodes, the size of the theoretical space is* $\lfloor n! \cdot e - 1 \rfloor$.

If $n = 9$, the size of the theoretical space is $\lfloor 9! \cdot e - 1 \rfloor = \lfloor 9! \cdot 2.71828 - 1 \rfloor = 986,409$. This enumeration also includes patterns with length 1, 2 and 3, excluding these the size of the search space is 985,824.

Pattern length. The length of a pattern is simply the number of nodes connected to form that pattern. It is analogous to the length of a textual password and is one of the most important features in determining the pattern security.

Theorem 2. *In a Pass-O with n nodes, the average pattern length* μ_n *is* $n - 1$.

Thus, the average pattern length in the 9-node Pass-O is $9 - 1 = 8$. This also matches with the average $\mu_{node} = 8$ as computed by our program (Table 1). The length statisitcs of theoretical 3X3 and Pass-O patterns are quite similar.

Stroke Length. Not every line segment in a pattern has same length. For instance, in both grid and circular layouts, the line segment 1 → 6 is longer than the line segment 1 → 2. This distance notion is captured using the stroke length of a pattern, which is defined as the sum of Euclidean distances of all line segments that forms the given pattern. To compute the stroke length of 3X3 patterns, we label the upper-left node as (0,0) and the lower-right node as (2,2). Thus, the length of horizontal and vertical line segments connecting adjacent nodes is just 1 and the length of diagonal segments can be easily computed using the Pythagoras theorem.

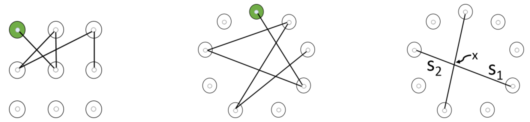
We categorize all line segments in 3X3 grid into five moves, straight move (horizontal or vertical) of length 1, short diagonal move of length $\sqrt{2} = 1.414$, long diagonal move of length $\sqrt{8} = 2.828$, knight move of length $\sqrt{5} = 2.236$ and overlapping move of length 2. A straight move connects a node to its adjacent neighbours, 1 → 2 and 1 → 4. A diagonal move connects a node to its diagonally adjacent neighbour 1 → 5 while a long diagonal move connects two diagonally opposite corners of the grid 1 → 9. A knight move connects non-adjacent nodes with a diagonal line 1 → 6 and 1 → 8, an overlapping move also connects two non-adjacent nodes but with a straight line 1 → 3 and 1 → 7. All five moves are possible (conditionally) only from the corner nodes {1,3,7,9}. The side nodes {2,4,6,8} allow all but long diagonal moves while the center node 5 allows only straight and short diagonal moves (Figure 2).

To compute the stroke length of Pass-O patterns, we assume that the Pass-O circle is inscribed in 3X3 grid. If the grid fits on a mobile screen then, the inscribed circle also fits on the same screen. Thus, the radius of the nine nodes Pass-O inscribed in 3X3 grid is 1. We observe that every line segment in a Pass-O pattern is a chord in the unit circle and its length can be calculated using the formula, $r \cdot \theta$, where θ is the angle formed between two radii connecting the two ends of the chord. Therefore, from a given node x, there are 2 nodes {x+1, x-1} at a distance of 0.684 , 2 nodes {x+2, x-2} at 1.286, 2 nodes {x+3, x-3} at 1.732 and 2 nodes {x+4, x-4} at 1.970. Note that, we have penalized the stroke lengths in Pass-O by assuming its radius to be of unit length. Thus, the average stroke length of 3X3 patterns (11.02) is longer than Pass-O patterns (9.93).

Intersections. Intersection occurs when two line segments in the pattern cross each other. For instance, the 3X3 pattern *152436* depicted in Figure 3a has 3 intersections, the first between 1 → 5 and 2 → 4, the second between 1 → 5 and 4 → 3, and the third between 5 → 2 and 4 → 3. Similarly, the Pass-O pattern *148263* has 5 intersections.

Table 1: Statistics of 3X3 and Pass-O patterns

Measure	3X3			PassO		
	μ	$\tilde{x}$	σ	μ	$\tilde{x}$	σ
Pattern Length	7.97	8	1.02	8	8	0.99
Stroke Length	11.02	0.40	11.13	9.93	10.05	0.21
Intersection	2.22	2	1.96	5.16	5	3.13



(a) 3 intersections (b) 5 intersections (c) intersection x

Figure 3: Intersections in 3X3 and Pass-O pattern

Theorem 3. *In a Pass-O with n nodes, the average number of intersections is* $\frac{n^2-7n+13}{6}$.

The proof is given in appendix B. The average number of intersections in the 9-node Pass-O is thus $\frac{9^2-7\cdot9+13}{6} = 5.167$. This also matches with $\mu = 5.16$ as computed by our code (Table 1). Note that 3X3 patterns have only 2.22 intersections on an average.

Remark 1. *Theoretically, Pass-O not only provides a large search space but also the patterns drawn on Pass-O are uniform and visually more complex in terms of intersections.*

4. USER STUDY

The primary objective of our study was to quantify the security of human-generated 3X3 and Pass-O patterns against both guessing and shoulder-surfing attacks. To provide a reliable estimate of the pattern security, we sought a large sample size. However, we note that collecting a large amount of graphical patterns from a diverse set of users is a challenging task. In case of textual passwords, the breach of large-scale websites is a common event which presents researchers with an unique opportunity to analyse millions of password strings [3]. In contrast, since graphical patterns are mostly used to protect personal mobile devices, survey methodology seems to be the only way to study them. This method limits the number of patterns that can be collected. In fact, prior survey studies [6, 13] performed security analysis on a small number of patterns gathered from not more than 100 participants per condition.

To be able to perform a large-scale analysis of 3X3 and Pass-O patterns, we conducted a *web-based* user study in our organization. Since the organization is large and spread across multiple locations around the globe, conventional methods *e.g., pen and paper survey* [6, 13] would have required tremendous amount of resources. On the other hand, using the web-based study we were able to gather more than 1,23,000 patterns from 21,053 participants within two weeks.

4.1 Methodology

We created a website specifically for the study and made it accessible to all employees through an internal portal. This portal is used for many purposes and employees already had the credentials to access it. On visiting the study link, participants were shown both conditions, 3X3 and Pass-O, but they were allowed to participate in only one of them. After choosing the condition, participants were redirected to an appropriate page containing instructions for drawing patterns on the chosen layout. The competition ran for two weeks and participants could participate only once.

To attract more participants, we designed an adversarial game as described in [6,13]. More specifically, participants were asked to draw at most 3 distinct secret patterns which they think are *easy for them to remember but difficult for others to guess*. These are called *defensive patterns*. Further, participants were asked to draw at most 3 distinct pattern guesses which they think are being used as secret (defensive) by other participants. These are called *offensive patterns*.

The purpose of the competition was two-fold, i) to learn the common pattern choices of participants, ii) to use these learnings in educating participants about insecure choices. After the competition, we published a list of top 500 popular 3X3 and Pass-O patterns [1] to make participants aware of the insecure patterns that should ideally never be used.

Since paying a large number of participants costs more money, we awarded top 3 participants in each condition with a cash reward of $300. Participants were assigned a score based on the guessability (strength) of their defensive patterns and the guessing efficiency of their offensive patterns (zero-sum game). At the end of the game, we displayed a dashboard wherein each participant can view their score and their position (rank) with respect to other participants. We believe that the adversarial nature of the game and a large cash reward provided enough incentive for participants to choose strong defensive patterns in both 3X3 and Pass-O conditions.

Our organization does not fall under the jurisdiction of an IRB, but we did abide by the privacy laws and did not collect any data about participants. However, for research purpose, we requested the cumulative demographic data of participants from the Chief Security Officer of our organization.

4.2 Participants

11,960 employees participated in 3X3 condition and 9,093 in Pass-O condition (total 21,053). Participants in 3X3 condition provided 34,548 defensive and 35,249 offensive patterns (total 69,797). While participants in Pass-O condition provided 26,469 defensive and 26,914 offensive patterns (total 53,383). We found no significant difference between gender, age, qualification and nationality of participants in 3X3 and Pass-O conditions (chi-square test). Most participants were young and were in the age group of 20-30 (Table 2). Qualification-wise participants were quite diverse. Further, participants belonged to 43 different nationalities, however, more than 93% of participants belonged to nationality N1.

Table 2: Participant demographics and Pattern Count

	3X3	Pass-O		3X3	Pass-O
Gender			**Nationality**		
Male	70.28%	70.50%	N1	93.89%	95.80%
Female	29.72%	29.50%	Others	6.11%	4.20%
Age			**Qualification**		
20-25	58.39%	40.16%	CS related	10.88%	12.49%
26-30	24.20%	33.35%	Engineer	60.72%	62.70%
31-35	9.93%	15.77%	Science	5.24%	4.60%
36-40	3.40%	6.37%	Commerce	7.69%	5.78%
≥ 41	4.08%	4.35%	Other	15.56%	14.43%
Pattern			**Total**		
#Defensive(Def)	34,548	26,469	#Def+#Off	69,797	53,383
#Offensive(Off)	35,249	26,914	#Participants	11,960	9,093

4.3 Limitations

Due to the web-based nature of the study, we were not in a position to verify whether participants stored their patterns for later use during the recall phase. Hence, we could not measure memorability in our study. Consequently, this experiment has to be treated as an initial security study of 3X3 and Pass-O patterns. Further, the generalizability of our study results is limited as the sample is not representative of a larger population. The population is younger and more technical than the overall population. However, the data analysis reveals striking similarity between the statistics of patterns from our study and pattern data reported in the past [5,6,13]. In fact, we found that the security of 3X3 patterns is less than that reported in these earlier studies.

5. DATA ANALYSIS

Now, we analyse the collected data and present empirical results. To determine the shoulder-surfing resistance, we use pattern characteristics such as pattern length, stroke length, direction changes and intersections [4,10,11] and to determine guessability we look at the common start and end points, popular patterns and repetitions [6,13]. Due to space constraints, we combine defensive and offensive patterns into a single list as done in [6,13] and compare the characteristics of all 69,797 3X3 patterns and 53,383 Pass-O patterns.

Pattern Length. Figure 4a shows the lengthwise distribution of user-chosen 3X3 and Pass-O patterns. 53.74% of the Pass-O patterns are connected using 9 nodes while only 26.30% of 3X3 patterns have 9 connected nodes. Surprisingly, the number of Pass-O patterns with length 7 and 8 is smaller. However, due to the preference for longer patterns, the average number of nodes connected in Pass-O patterns (7.46) is larger than that in 3X3 patterns (6.92).

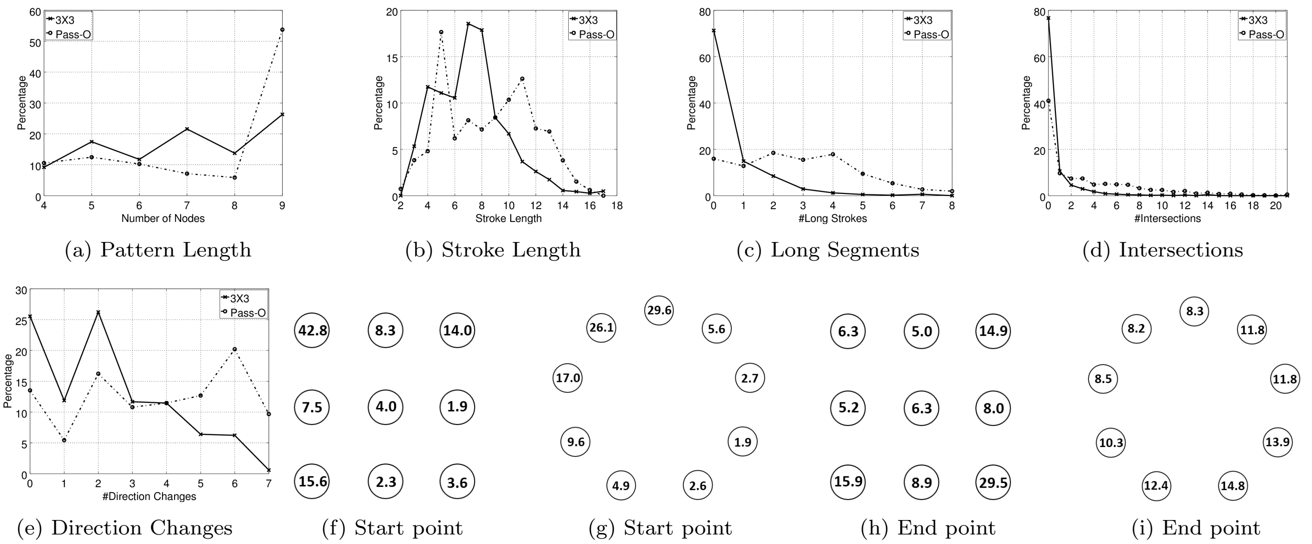
Stroke Length. Theoretically, the average stroke length of 3X3 patterns is larger than Pass-O patterns. However, the survey data reveals that not only 3X3 patterns are connected with fewer nodes, the line segments used in connecting them are also short. Figure 4b presents the stroke length distribution of 3X3 and Pass-O patterns. More than 71% of 3X3 patterns are composed using straight and short diagonal moves only. The line segments such as knight moves which resist shoulder-surfing attacks [4, 10, 11] are mostly absent in 3X3 patterns while more than 84% of Pass-O patterns are connected with longer line segments (Figure 4c). Consequently, the average stroke length of Pass-O patterns (8.57) is longer than 3X3 patterns (7.20).

Intersections. As shown in Figure 4d more than 76% of 3X3 patterns are simple and do not contain any intersections, a property which contributes towards the pattern complexity [4,10,11]. On the other hand, nearly 60% of Pass-O patterns have at least one intersection. 3X3 patterns contain only 0.63 intersections on an average while Pass-O patterns is drawn with 3.47 intersections (Table 3). Therefore, Pass-O patterns appear more complex than 3X3 patterns. We compare the shoulder-surfing resistance of 3X3 and Pass-O patterns in appendix C.

Table 3: Features comparison of 3X3 and Pass-O data

Measure	3X3			PassO		
	μ	$\tilde{x}$	σ	μ	$\tilde{x}$	σ
Pattern Length	6.92	7	1.68	7.46	9	1.88
Stroke Length	7.20	6.83	0.66	8.57	8.69	1.10
Long Strokes	0.53	0	0.75	2.81	3	1.50
Intersection	0.63	0	1.74	3.47	1	4.44
Direction	2.19	2	1.84	3.68	4	2.26

Start and End Points. As shown in Figure 4f, the upper-left corner of the grid is the most common choice for starting 3X3 patterns. The most popular beginning for Pass-O patterns is also the top-most node (Figure 4g), however the number of Pass-O patterns that begin at the top node (29.64%) is relatively smaller than 3X3 patterns (42.84%). While 3X3 patterns are most likely to begin with corner nodes, Pass-O patterns are most likely to begin with nodes



(a) Pattern Length (b) Stroke Length (c) Long Segments (d) Intersections

(e) Direction Changes (f) Start point (g) Start point (h) End point (i) End point

Figure 4: Feature distribution of 3X3 and Pass-O data

{1,9,8,7}. To gauge the amount of randomness in a given distribution, we use the Shannon entropy measure H.

$$Entropy\ H = \sum_{i=1}^{n} p_i \cdot log_2(1/p_i) \qquad (1)$$

The entropy due to starting point choices of 3X3 patterns is 2.51 bits while in case of Pass-O, the entropy is slightly higher 2.62 bits. Further, the end point choices of 3X3 participants are also highly biased with nearly 30% of 3X3 patterns terminating at the bottom-right node. Surprisingly, the termination choices of Pass-O patterns are relatively uniform. The entropy due to end point choices of 3X3 patterns is 2.89 bits while for Pass-O patterns it is 3.14 bits.

Repetitions. Of the 69,797 3X3 patterns, only 16,310 (less than 24%) patterns are distinct, whereas of the 53,383 Pass-O patterns, 27,497 (more than 50%) patterns are distinct. The most popular 3X3 pattern is the 'Z' shape and it constitutes 3.10% of all 3X3 patterns (Figure 5). Other popular 3X3 patterns also resemble the letters of an English alphabet such as 'S', 'L', 'N', and 'M'. The most popular Pass-O pattern constitutes 1.64% of all patterns and is drawn by connecting all nodes in an anti-clockwise fashion beginning from node 1. Other popular choices include patterns with alternating nodes and those resembling English letters such as 'Z' and 'C'. A list of top 500 patterns can be found at [1].

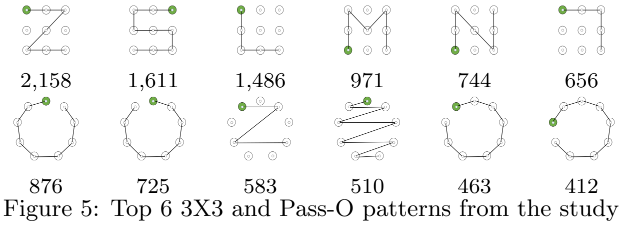


Figure 5: Top 6 3X3 and Pass-O patterns from the study

Remark 2. *The user-chosen Pass-O patterns are not only visually more complex but also less repetitive and have uniform beginning and ending as compared to 3X3 patterns. The data strongly suggests that the space utilized by Pass-O patterns is much better than that of 3X3 patterns.*

6. GUESSABILITY

In this section, we measure the relative strength of 3X3 and Pass-O patterns against guessing attacks. First, we use the pattern data to develop a Markov model based guessing algorithm [13] and then, we use it to estimate the partial guessing entropy [8] of 3X3 and Pass-O patterns.

6.1 Guessing Entropy

The attack technique we use is quite similar to that described in [13]. The objective is to recover as many patterns as possible using as few guesses as possible. To gain maximum benefit, pattern guesses should be generated in decreasing order of probabilities. To estimate pattern probabilities, we employ ngram-Markov model which exploits the fact that subsequent choices in a human-generated sequence are largely dependent on the current choices. For instance, the letter 'e' is more likely to follow 'th' than the letter 'z'. In case of 3X3 patterns the adjacent nodes are more likely to be chosen than the non-adjacent nodes. Based on this observation, the ngram-Markov model predicts the next letter in a sequence using the prefix of length $n-1$. The probability of a sequence of letters $s_1, \ldots, s_l$ can be modelled as

$$P(s_1, \ldots, s_l) = P(s_1, \ldots, s_{n-1}) \cdot \prod_{i=n}^{l} P(s_i | s_{i-n+1}, \ldots, s_{i-1}) \qquad (2)$$

Parameters. We choose the value of n to be 3. The suitability of the choice of trigrams is evident from Figure 8 given in appendix D. More than $1/6^{th}$ of 3X3 patterns are composed using the trigram *789*, while $1/13^{th}$ of Pass-O patterns are made up of trigram *234*. Further, we found that increasing the size of n to 4 does not improve the pattern guessability. We estimate the probabilities of trigrams that do not appear in the dataset using the Laplace smoothing technique.

Implementation. We use K-fold cross-validation technique and split our dataset randomly into $K = 5$ disjoint equal sized subsets. Then, we perform K iterations. In each iteration, we select a previously unvisited subset from $K = 5$ subsets, mark it as visited and use it as test set. The remaining 4 sets are combined and used as training set. The size of 3X3 test set is around 13,959 while the size of Pass-O test set is about 10,676. After fixing the training set and test set, we do the following computations.

- We assign highest probabilities to the frequent patterns (*count* $\geq$ 10) appearing in the training set, so that they are used upfront while performing guessing.

- We compute trigram probabilities using the training set and employ Markov model to estimate the probabilities of the remaining patterns.
- We sort all patterns in decreasing order of probability.
- We use these as guesses to crack the test set patterns.

We repeat the entire process 50 times and report the mean.

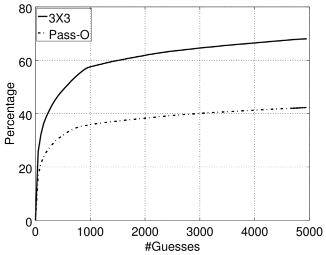


Figure 6: Guessing resistance of 3X3 and Pass-O patterns

Results. Figure 6 demonstrates the success rate of guessing algorithm against all (defensive + offensive) patterns. *Within 5000 guesses, the attacker can recover 70% of 3X3 patterns but only 40% of Pass-O patterns. Even within the first 20 guesses, the attacker can crack 18.55% of 3X3 patterns but only 11.51% of Pass-O patterns. Therefore, Pass-O patterns are more resistant to guessing attacks.*

Table 4 compares the percentage of patterns cracked on different layouts within the first 20 guesses. *Our guessing algorithm cracked 18.55% of 3X3 patterns, 11% more than that reported in [6]. Also, Pass-O patterns are much stronger as compared to 3X3 and 4X4 patterns [6], since within 20 guesses the attacker can crack 18.55% of 3X3 and 19.90% of 4X4 patterns but only 11.51% of Pass-O patterns.*

6.2 Partial Guessing Entropy

Now, we compare the partial guessing entropy [8] (for definition refer to appendix E) of 3X3 and Pass-O patterns. We define the probability p_i as the fraction of patterns cracked by i^{th} guess of our Markov-based algorithm. We found that the effort required to crack the first 10% ($G_{0.1}$) of 3X3 patterns is just 5.80 bits while for Pass-O the effort is 7.06 bits (Table 4). Note that the guessing resistance ($G_{0.1}$) of 3X3 patterns (5.80 bits) is less than reported (6.59 bits) in the earlier study [6]. The difference in security is much higher for cracking larger proportion of patterns, *e.g.*, the security of first 50% of 3X3 patterns is 9.86 bits (less than three random digits) while the security offered by Pass-O patterns is 15.28 bits (more than four random digits).

Table 4: Partial Guessing Entropy Comparison

Distribution	$\alpha = 0.1$	$\alpha = 0.2$	$\alpha = 0.5$	20 guess
3X3 All	5.80	6.95	9.86	18.55%
Pass-O All	**7.06**	**8.50**	**15.28**	**11.51%**
Aviv *et.al.* 3X3 All [6]	6.59	6.99	8.93	16.70%
Aviv *et.al.* 4X4 All [6]	6.23	6.64	11.61	19.90%
3X3 Def	8.61	9.50	13.02	6.65%
Pass-O Def	**10.01**	**14.07**	**18.49**	**4.45%**
Aviv *et.al.* 3X3 Def [6]	9.43	9.79	10.98	4.00%
Aviv *et.al.* 4X4 Def [6]	6.23	6.64	11.61	3.20%
Uellenbeck *et.al.* 3X3 Def [13]	8.72	9.10	10.90	
Uellenbeck *et.al.* Circle Def [13]	9.76	10.81	12.69	
3X3 Off	4.54	5.18	7.51	30.57%
Pass-O Off	5.62	6.82	11.66	18.97%
Aviv *et.al.* 3X3 Off [6]	6.98	7.69	9.31	12.50%
Aviv *et.al.* 4X4 Off [6]	6.46	7.57	10.40	16.70%
Uellenbeck *et.al.* 3X3 Off [13]	7.56	7.74	8.19	

As shown in Table 4, Pass-O defensive patterns are much stronger than 3X3 defensive patterns. The effort required to crack the first 20% of Pass-O patterns is $2^{14.07-9.50} = 2^{4.57} \approx 23.75$ times greater than that of 3X3 defensive patterns (Table 4). *Moreover, Pass-O defensive patterns are also stronger by an order of magnitude than the defensive patterns drawn on 4X4 grid [6] and Circle [13].*

7. CONCLUSION

In this paper, we proposed an alternate circular layout Pass-O which not only simplifies the pattern drawing rules but also improves the theoretical space and allows visually complex patterns. We conducted a large-scale user study and compared the security of 3X3 and Pass-O patterns. We found that users do take advantage of circular layout and create patterns with longer strokes and relatively large number of direction changes and intersections. Consequently, a significant fraction of the Pass-O patterns is classified as strong by existing strength meters. Further, the search space utilized by Pass-O patterns is much better than 3X3 patterns. Consequently, the guessing resistance of Pass-O patterns is also much higher.

Future Work. We found that Pass-O provides clear security improvements over 3X3 grid. However, due to the web-based nature of the study, we could not compare the usability of Pass-O and 3X3 patterns reliably. In future, we intend to perform a focused usability study to determine any resulting usability-security tradeoff due to the use of Pass-O.

8. REFERENCES

[1] Top 500 Popular Patterns. https://docs.google.com/spreadsheets/d/1o-EWLuKQXtuQ7rhXQpQzWvmzplRyh7EGk5nbw2bU2O0/.

[2] Fingerprint security on Nexus devices. https://support.google.com/nexus/answer/6300638?hl=en, accessed on 14 Feb 2016.

[3] World's Biggest Data Breaches. http://www.informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks/, accessed on 14 Feb 2016.

[4] P. Andriotis et al. Complexity metrics and user strength perceptions of the pattern-lock graphical authentication method. In *Human Aspects of Information Security, Privacy, and Trust*, pages 115–126. Springer, 2014.

[5] P. Andriotis et al. A pilot study on the security of pattern screen-lock methods and soft side channel attacks. In *WiSec '13*, pages 1–6. ACM.

[6] A. J. Aviv et al. Is bigger better? comparing user-generated passwords on 3x3 vs. 4x4 grid sizes for android's pattern unlock. In *ACSAC '14*, pages 301–310. ACM.

[7] R. Biddle, et al. Graphical passwords: Learning from the first twelve years. *ACM Comput. Surv.*, 44(4):19:1–19:41, 2012.

[8] J. Bonneau. The science of guessing: Analyzing an anonymized corpus of 70 million passwords. In *SP '12*, pages 538–552. IEEE Computer Society.

[9] A. Paivio. Mind and Its Evolution: A Dual Coding Theoretical Approach. Lawrence Erlbaum: Mahwah, In *N.J.,* 2006.

[10] Y. Song et al. On the effectiveness of pattern lock strength meters: Measuring the strength of real world pattern locks. In *CHI '15*, pages 2343–2352. ACM.

[11] C. Sun et al. Dissecting pattern unlock: The effect of pattern strength meter on pattern selection. *Journal of Information Security and Applications*, 19(4):308–320, 2014.

[12] H. Tao et al. Pass-go: A proposal to improve the usability of graphical passwords. *I. J. Network Security*, 7(2):273–292, 2008.

[13] S. Uellenbeck et al. Quantifying the security of graphical passwords: The case of android unlock patterns. In *CCS '13*, pages 161–172. ACM.

[14] E. von Zezschwitz et al. Easy to draw, but hard to trace?: On the observability of grid-based (un)lock patterns. In *CHI '15*, pages 2339–2342. ACM.

[15] E. von Zezschwitz et al. Patterns in the wild: A field study of the usability of pattern and pin-based authentication on mobile devices. In *MobileHCI '13*, pages 261–270. ACM.

APPENDIX

A. BACKGROUND AND RELATED WORK

Graphical passwords are considered as usable alternatives to textual passwords as they exploit the superior ability of human brain to remember visual information. According to dual-coding theory [9], verbal (word-based) and non-verbal (image-based) memory are processed and represented differently in the brain. The storage of graphical information is a one-step process while the storage of textual information is a two-step process and thus requires more effort. Therefore, graphical passwords are a promising avenue to explore.

Depending on the memory task involved in remembering and entering password, graphical schemes are broadly classified into three categories, namely, recognition-based, cued recall-based and recall-based [7]. Pass-Go [12] is an example of recall-based scheme in which user selects one or more strokes on a $n \times n$ grid. The 3X3 pattern unlock scheme is an instance of Pass-Go, especially tailored for the hand-held mobile devices. (The name Pass-O for our circular layout is partly inspired from Pass-Go. Dropping the letter 'G' for Grid from Pass-Go yields Pass-O.)

A.1 Attacks on Pattern Unlock Scheme

Although pattern-based graphical schemes are usable, they are susceptible to a wide variety of attacks including guessing attacks and shoulder-surfing attacks. In this section, we give a brief overview of these attacks and differentiate our work from the prior studies.

Guessing Attacks. In 2013, Uellenbeck *et al.* [13] collected approximately 2,900 patterns from 584 participants on 5 different layouts and demonstrated that the security of 3X3 patterns is less than a 3-digit random PIN. The authors found that most users use only horizontal and vertical lines to create their 3X3 patterns and that 43% of participants begin their patterns with an upper-left node. To eliminate these biases, authors also tested four alternate layouts, of which the circular layout improved security.

Their circular layout citeUellenbeck:guessing consisted of 9 nodes of which 8 nodes were placed along the circumference of a circle while the remaining ninth node was placed in the center. Due to this arrangement, two nodes at diagonal ends could not be connected directly without passing through the center node. This arrangement allows a total space of 645,504 patterns, 1.6 times more than 3,89,112 patterns possible on 3X3 grid layout. *In Pass-O, we arrange all 9 nodes along the circumference of a circle, so that any node can be connected to any other node, which gives a full space of 9,85,824, about 2.5 times more than that of 3X3 grid layout and 1.5 times more than the circular layout of [13].*

Recently, Aviv *et al.* [6] studied the security of patterns drawn on 4X4 grid and found that most of the 4X4 patterns are just extended versions of 3X3 patterns. These results were based on 494 patterns collected from 80 participants.

In this paper, we report the largest pattern study conducted till date. We collect 69,797 3X3 patterns and 53,383 Pass-O patterns from 21,053 participants. We find that the guessing resistance of 3X3 patterns is much less than that reported in the literature [6, 13]. In addition to providing a reliable security estimate of 3X3 patterns, we also test the security of a new layout (Pass-O). Further, we share a list of 500 most popular 3X3 and Pass-O patterns from our dataset [1].

Shoulder-surfing Attacks. The graphical patterns are prone to shoulder-surfing attacks and to thwart them several pattern strength meters have been proposed [4, 10, 11]. The objective of the strength meters is to nudge users to create visually complex patterns. The more complex the pattern appears, the harder for the observer to memorize it.

The strength meter proposed by Androitis *et al.* [4] relies on 5 different features to determine the pattern complexity, namely starting point, length, direction changes, knight moves and overlapping nodes. Sun *et al.* [11] determined the pattern strength based on length, stroke length, number of intersections and number of overlaps. Later, Song *et al.* [10] also attributed the pattern complexity to length, number of intersections and number of non-repeated segments.

In this paper, we characterize the visual complexity of 3X3 and Pass-O patterns using features such as pattern length, stroke length, number of intersections and direction changes. We first adapt and implement the 3X3 pattern strength meters [4, 10, 11] for Pass-O and then compare the security of 3X3 and Pass-O patterns against shoulder-surfing attacks.

B. INTERSECTION PROOF

PROOF. First, we count the number of paths that contain an intersection x between the given two line segments s_1 and s_2 on n-node Pass-O (Figure 4c). To construct a path of length $n - j$ containing the intersecting line segments s_1 and s_2, we drop j nodes from the remaining $n - 4$ nodes. This can be done in ${}^{n-4}C_j$ ways. For counting purpose, we coalesce two nodes of line segment s_1 into one node and two nodes of line segment s_2 into another. After coalescing, we are left with $n - 2$ nodes. As there are $(n - j - 2)!$ different paths of length $n - j$ and the nodes connecting each of the line segments s_1 and s_2 can be visited in 2! ways, we have

$$\#paths\ with\ intersection\ x = \sum_{j=0}^{n-4} {}^{n-4}C_j \cdot (n-2-j)! \cdot 2!2!$$

After simplification we get

$$\begin{aligned}
&= 4(n-4)! \cdot \sum_{j=0}^{n-4} \frac{(n-2-j)(n-3-j)}{j!} \\
&= 4(n-4)! \cdot \Big(\sum_{j=0}^{n-4} \frac{(n-2)(n-3)}{j!} - \sum_{j=1}^{n-4} \frac{2n-5-j}{(j-1)!} \Big) \\
&\approx 4(n-4)! \cdot e \cdot ((n-2)(n-3) - (2n-5) + 2) \\
&= 4(n-4)! \cdot e \cdot (n^2 - 7n + 13)
\end{aligned}$$

This gives the number of paths containing a particular intersection x. Now, any 4 points in a n-node Pass-O define one unique intersection. Hence, there are ${}^{n}C_4$ intersections. Also by *Theorem 1* there are $n! \cdot e$ different paths. Therefore, the average number of intersections is given by

$$\mu_{intersection} = {}^{n}C_4 \cdot \frac{4(n-4)! \cdot e \cdot (n^2 - 7n + 13)}{n! \cdot e}$$

$$\mu_{intersection} = \frac{n^2 - 7n + 13}{6} \qquad (3)$$

□

C. SHOULDER-SURFING

In section 5, we found that features such as longer length, longer strokes and intersections are pre-dominantly present in Pass-O patterns. These features add to the visual complexity of patterns and therefore provide better security against shoulder-surfing attacks [4, 10, 11]. The intuition is that humans can store very few items in the short term memory. Therefore, if a pattern is longer and visually complex it is difficult for a human observer to memorize the pattern in just one observation. To determine the visual complexity of 3X3 patterns, few strength meters have been proposed in the literature [4, 10, 11]. We adapt these algorithms for Pass-O and measure the shoulder-surfing resistance of 3X3 and Pass-O patterns. Due to space constraints, we report on the combined list of defensive and offensive patterns.

LNCS Strength Meter. Andriotis *et al.* [4] used 5 different features to determine the complexity of 3X3 patterns, namely starting point, number of nodes, direction changes, knight moves and overlapping nodes. The longer patterns that begin with any but upper-left node, that contains knight moves, overlaps (line segments with length > 1.414) and direction changes are assigned highest scores. A direction change in the pattern occurs when an angle is formed between two consecutive strokes. For instance, the consecutive line segments 1 → 2 and 2 → 5 on 3X3 grid constitute a direction change, while the line segments 1 → 2 and 2 → 3 constitute no direction change. This strength meter weighs every feature equally and classifies all patterns into three categories, weak, medium and strong.

We use the same 5 features to classify Pass-O patterns as well. The starting point (top-most node) and the number of nodes are trivial to find but we need an equivalent notion of knight and overlapping moves in the Pass-O context. Since knight moves in 3X3 grid are nothing but strokes of longer lengths, we consider the line segments of length 1.732 and 1.970 in Pass-O as knight moves. Overlap is a unique feature of the 3X3 grid and therefore we set the value of overlapping feature for Pass-O patterns as 0. Further, straight lines are not possible on circular layout as there is always an angle between every consecutive strokes (chords), hence most of the Pass-O patterns will be classified as strong. To prevent this, we slightly alter the definition of a direction change.

We say that a direction change in the pattern occurs if two consecutive strokes have different lengths. For instance, the consecutive line segments 1 → 2 and 2 → 3 on circular layout are of same length and therefore they do not constitute a direction change, but 1 → 2 and 2 → 7 are of different lengths and as per our definition they constitute a direction change. Therefore, simple 3X3 patterns such as 'L' and 'S' and Pass-O patterns of the form *123456789* which are composed entirely of similar line segments have zero direction changes. The average number of direction changes in Pass-O (3.68) is 1.7 times higher than that of 3X3 pattern (2.19). The distribution is shown in Figure 4e.

JISA Strength Meter. The strength meter proposed by Sun *et al.* [11] computes shoulder-surfing resistance using entropy like formula by employing 4 different features, namely stroke length, pattern length, number of intersections and overlaps. Again, while quantifying the complexity of Pass-O patterns, we set the overlap feature value to zero. Also, the authors used a 5 point interval scale (very weak to very strong) to measure the shoulder-surfing resistance of 3X3 patterns, however to be consistent with the scales of other two strength meters, we convert this 5 point scale into 3 point scale by merging patterns that belong to very weak and weak categories into a single class and patterns that belong to very strong and strong categories into another class.

CHI Strength Meter. Song *et al.* [10] used 3 different features, namely pattern length, number of non-repeated segments and intersections to determine the shoulder-surfing resistance of 3X3 patterns. The idea behind non-repeated segments is similar to that of direction change given by us. The authors performed shoulder-surfing experiments and learned relative weights of these 3 features. The weight of the pattern length was found to be 0.81 and that of intersections to be 0.15. The authors used chess board distance to compute the segment length *i.e.* the distance between two nodes (x_1,y_1) and (x_2,y_2) is simply $\max(|x_1 - x_2|,|y_1 - y_2|)$. Our pattern strength evaluation considers Euclidean distance as opposed to chess board distance metric.

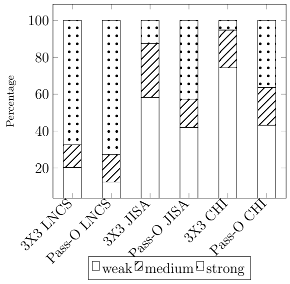


Figure 7: Shoulder-Surfing resistance of 3X3 and Pass-O data as computed using 3 distinct strength meters [4, 10, 11]

Figure 7 depicts the shoulder-surfing resistance of 3X3 and Pass-O patterns as evaluated by these 3 meters. LNCS meter classified most of 3X3 and Pass-O patterns as strong. JISA meter determined only 12.59% of 3X3 patterns as strong whereas it classified 43.09% of Pass-O patterns (3.4 times higher) as strong. Similarly, CHI meter classified only 5.25% of 3X3 patterns as strong while in case of Pass-O, the percentage is nearly 6.9 times higher (36.40%).

D. POPULAR NGRAMS

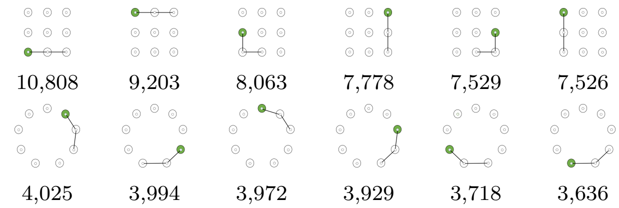


Figure 8: Top 6 3X3 and Pass-O trigrams

E. PARTIAL GUESSING METRIC

The partial guessing metric [8] models an adversary that terminates the guessing process after breaking a certain fraction α of passwords. If $\mu_\alpha = min\{i_0 | \sum_{i=1}^{i_0} p_i \geq \alpha\}$ represents the minimum number of guesses to recover at least a fraction α of passwords and $\lambda_\alpha = \sum_{i=1}^{\mu_\alpha} p_i \geq \alpha$ represents the actual fraction recovered then, the partial guessing entropy is computed using the formula,

$$G_\alpha(X) = (1 - \lambda_\alpha) \cdot \mu_\alpha + \sum_{i=1}^{\mu_\alpha} i \cdot p_i \tag{4}$$

The first part in the addition is contributed by those patterns that remained unguessable after μ_α attempts and the second part is due to those patterns that were guessed in μ_α attempts. To compute the partial entropy into bits, the formula can be expressed as follows,

$$\tilde{G}_\alpha(X) = log\left(\frac{2 \cdot G_\alpha(X)}{\lambda_\alpha} - 1\right) + log\left(\frac{1}{2 - \lambda_\alpha}\right) \tag{5}$$