Do Bigger Grid Sizes Mean Better Passwords? 3x3 vs. 4x4 Grid Sizes for Android Unlock Patterns

Devon Budzitowski and Adam J. Aviv
dev@comcast.com aviv@usna.edu
United States Naval Academy

Ravi Kuber
rkuber@umbc.edu
University of Maryland, Baltimore County

ABSTRACT

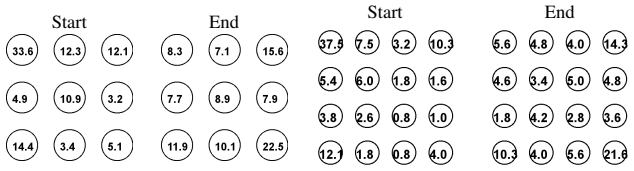
This poster-abstract presents the results of an IRB approved survey studying Android unlock pattern choices as compared between two grid sizes (3x3 and 4x4); the smaller grid size is the current standard. We recruited 80 participants who chose both patterns for themselves and guesses of others' patterns, collecting 491 3x3 and 504 4x4 patterns. Patterns were analyzed using several metrics including: repetition rates, pattern recall, pattern compromises, node length, stroke length, common pattern forms, and the start/end point frequency. Pattern recall and compromises varied between grid sizes; however, the variations in patterns between grid sizes, generally, are less pronounced with many 4x4 patterns simply being embedding of 3x3 patterns. Overall, 3x3 and 4x4 patterns chosen by humans have the same basic properties, and increasing the grid size to 4x4 would likely not change behavior despite significantly increasing the number of available patterns for 4x4 grid size from 389,112 to 4,350,069,823,024.

1. INTRODUCTION

Android graphical password patterns are perhaps the most common graphical password system to date, notably because it comes standard as an authentication choice on Android devices. The graphical pattern scheme requires users to recall a pre-selected shape and "draw" it on an on-screen grid of size 3x3. More unique patterns can be composed on a standard 3x3 grid, compared with a 5-digit PIN [5]. However, users do not fully utilize all available grid-based patterns [5, 4, 1], favoring to use a small subset of patterns on specific sections of grids. In this poster abstract, we question whether the user prefers to use simple patterns for purposes of authentication, or if they are somehow self-limiting the design of the pattern due to the constraints of the grid size.

To investigate this further, we recruited 80 participants at two institutions over the period of 6-weeks (10 sessions) in an IRB approved study. Participants ranged in age between 18 and 40 years old. Two-thirds of those recruited were male and one-third female. In total, 491 3x3 and 504 4x4 unlock patterns were collected using an in-lab, pen-and-paper methodology similar to that of [5] where participants first select sets of patterns as their own and then try to adversarial guess the patterns of others in their session.

We analyzed the collected patterns in several dimensions, including: repetitions and symmetries, embedding of 3x3 patterns in 4x4 patterns, pattern recall, pattern compromises, pattern lengths, common pattern forms, and start/end point frequency. We found that certain aspects of 4x4 grid patterns offer a superior alternative to 3x3 grid patterns; for example, participants tend to choose longer patterns for 4x4 than 3x3 (as measured by total number of contact points used), which are harder to compromise generally (see Figures 2 and 3). Other comparisons suggest that users would make



(a) 3x3 Patterns

(b) 4x4 Patterns

Figure 1: Frequency of Pattern Start and End Points (in percent)

similar pattern selections for 4x4 grids as they would for 3x3 grids; for example, the length of the lines within patterns, normalized for the grid size, follow similar distributions, suggesting that users choose similarly shaped patterns that repeat, as well as repeat the same patterns at the same frequency (see Figures 1, 4, and 5). Finally, nearly one-third of the 4x4 patterns are simply 3x3 patterns embedded within the 4x4 grid space (see Table 1).

2. METHODOLOGY

Participants were asked to draw authentication patterns on paper rather than on a mobile device. While using a real mobile device may alter the results, we found the selected patterns for 3x3 grids were consistent with prior studies [5], and in fact, the methodology was modeled on the same prior work.

The basic protocol is that participants are incentivized by the promise of an edible treat (candy or chocolate) for both correctly remembering their own selected patterns and also correctly guessing passwords selected by other participants in their session. The survey consistent of four parts: (1) participants were asked to select three patterns that would be their own, which they considered to be perceivably secure and memorable; (2) participants were asked to make up to 10 guesses of patterns selected by others in their session; (3) participants were asked to fill out a short questionnaire evaluating their experience; (4) participants were finally ask to recall their three initially-selected patterns from (1).

The survey was conducted across multiple sessions ranging from 7-22 participants per session. Five sessions were undertaken to capture 3x3 patterns, and five sessions focused on 4x4 patterns. Participants only attended one session each, meaning that they would either produce patterns for either 3x3 or 4x4 grids. The visual and oral instructions and questionnaires were the same across sessions. The only difference was the grid size. Due to space limitations, we do not discuss results from the questionnaire herein.

3. RESULTS

The metrics we use in our analysis (as well as studies who have used the same metrics [3, 2, 5]) are as follows:

- **Common start- and end-points**: Referring to Figures 1a and 1b, and one can see that even with the additional contact

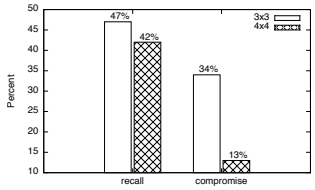


Figure 2: Recall and Compromise Rates

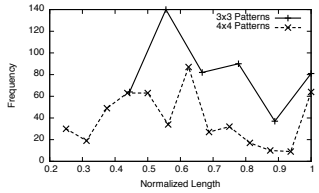


Figure 3: Node Length

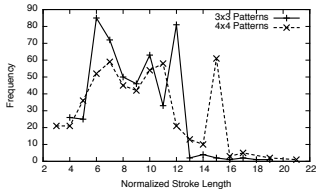


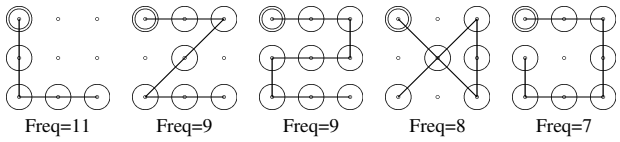
Figure 4: Stroke Length

	Size	Repetitions	Symmetries	Embedding
3x3 Patterns	491	245 (49.9%)	398 (81.1%)	n/a
4x4 Patterns	501	179 (35.7%)	204 (40.7%)	166 (33.1%)

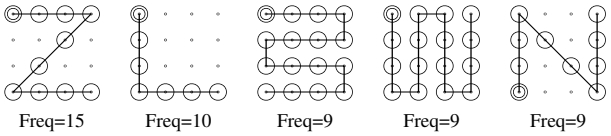
Table 1: The Fraction of Repetitions, Symmetries, and Embedding of 3x3 patterns in 4x4 patterns

points in 4x4 grids, patterns created for both 3x3 and 4x4 have similar start and end points. Patterns typically begin in the upper left and end in the lower right; similar observations were made by [5, 1].

- **Recall and Compromise**: Analyzing the percentage of patterns participants successfully recalled between part (1) and part (4) of the survey, after approx. 15 minutes, there is no significant difference between 3x3 and 4x4 patterns; however, for the percent of compromised patterns (those selected in (1) that were guessed in (2)), significantly more 3x3 patterns were compromised compared to 4x4 patterns.
- **Length Measures**: We analyzed the length of the patterns using two metrics: node-length, the number of contact points used, and stroke-length [3, 2], the length of the lines within the pattern. To get a fair comparison, in Figure 3, we normalize the results based on the total number of contact points available (9 vs. 16). In 4x4, more contact points are generally used compared with 3x3 patterns. With respect to contact points in the pattern, 4x4 patterns typically should be longer, but there are also more contact points to choose from. For stroke-length, again, the data is normalized based on the size of the grid space, and the results are presented in Figure 4. Both 3x3 and 4x4 patterns follow similar shapes for stroke length, and this suggests that, overall, typical patterns for 3x3 and 4x4 are similarly shaped. This is furthered by the next observation below.
- **Common Patterns:** The frequency of pattern shapes and repeats between 3x3 and 4x4 patterns are also relevant. The most common patterns are presented in Figure 5, and in Table 1 statistics about repetitions of patterns are presented. Interesting, in both data sets, large portions of the patterns repeat at least once, and an even larger portion are symmetrically pair, that is, a pattern that can be transformed into another through a series of rotations, flips, or reversals. Additionally, we find that many of the 4x4 patterns are just simple embedding of 3x3 patterns; one-third of the 4x4 pattern shapes can be found in the 3x3 data set. For example, the 'Z' and 'L' shape appear in both the 3x3 and 4x4 data sets, and this trend continues when analyzing the tri-gram forms. In Figure 6, one can see that much of the same shapes appear in both sets, and there is a tendency to use the outer points as compared to the interior ones. The lack of originality in the 4x4 patterns is particularly problematic for security when considering that there are many orders of magnitude ore 4x4 patterns than 3x3 patterns, 389,112 vs. 4,350,069,823,024.

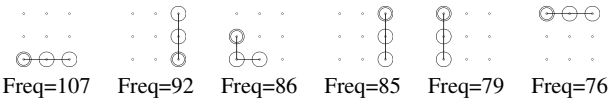


(a) 3x3 Patterns

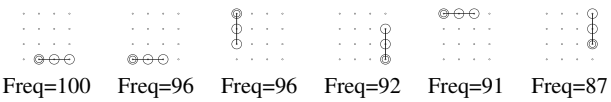


(b) 4x4 Patterns

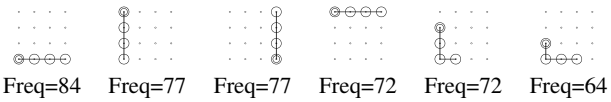
Figure 5: Top 5 Most Frequently Occurring Patterns



(a) 3x3 Pattern Tri-Grams



(b) 4x4 Pattern Tri-Grams



(c) 4x4 Pattern Quad-Grams

Figure 6: Top Ocuring Tri- and Quad-grams (4x4 only)

4. CONCLUSION

We studied how changing the grid size of Android's pattern unlock can affect user choice by conducting a large in-lab survey. We found that certain features of 4x4 patterns, such as node length and ease of guessing do improve, but overall, 3x3 and 4x4 patterns chosen by humans have the same basic properties with respect to stroke length, repetition, and basic shape. These results suggest while there may be benefits to increasing the grid size, overall, the general variations in patterns chosen by humans will likely stay the same despite the exponential increase in the overall number of available patterns by switching to a 4x4 grid size.

5. REFERENCES

[1] P. Andriotis, T. Tryfonas, G. Oikonomou, and C. Yildiz. A pilot study on the security of pattern screen-lock methods and soft side channel attacks. In *WiSec'13*, 2013.

[2] M. Arianezhad, D. Stebila, and B. Mozaffari. Usability and security of gaze-based graphical grid passwords. In *FC'13*. 2013.

[3] A. J. Aviv and D. Fichter. Understanding visual perceptions of usability and security of android's graphical password pattern. In *ACSAC'14*, 2014.

[4] A. J. Aviv, B. Sapp, M. Blaze, and J. M. Smith. Practicality of accelerometer side channels on smartphones. In *ACSAC'12*, 2012.

[5] S. Uellenbeck, M. Dürmuth, C. Wolf, and T. Holz. Quantifying the security of graphical passwords: The case of android unlock patterns. In *CCS'13*, 2013.