Twice as Nice? A Preliminary Evaluation of Double Android Unlock Patterns

Timothy J. Forman
United States Naval Academy
Annapolis, MD 21402, USA
m201902@usna.edu

Daniel S. Roche
United States Naval Academy
Annapolis, MD 21402, USA
roche@usna.edu

Adam J. Aviv
The George Washington University
Washington, DC 20052, USA
aaviv@gwu.edu

CHI '20 Extended Abstracts, April 25–30, 2020, Honolulu, HI, USA.

ACM ISBN 978-1-4503-6819-3/20/04.
DOI: https://doi.org/10.1145/3334480.3382922

Abstract

Android unlock patterns are a widely used form of graphical passwords, and like all password schemes, numerous studies have shown that users select a relatively guessable and non-diverse set of passwords. While proposals have been put forth for hardening patterns, such as increasing the number of or changing the location of contact points, none of these proposals has been implemented in the decade-plus since the interface's launch. We propose a new approach; instead of increasing the individual complexity, users select two sequential Android patterns, so called Double Patterns, that are visually super imposed on one another. This allows more complexity without dramatically changing the interface. We report on our preliminary findings of a large user study ($n = 634$) of Double Patterns, finding strong evidence that the scheme is highly usable and increases the complexity of user choice.

Author Keywords

Android Patterns; Mobile Authentication; Security; Usability.

CCS Concepts

•**Security and privacy → Graphical / visual passwords;**
•**Human-centered computing → Human computer interaction (HCI); Usability testing;**

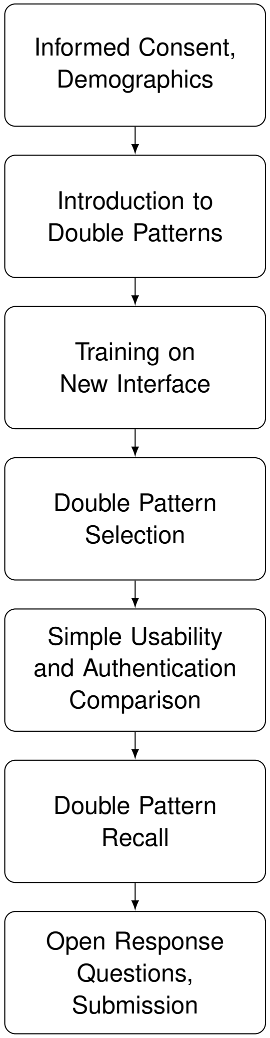

Informed Consent, Demographics
Introduction to Double Patterns
Training on New Interface
Double Pattern Selection
Simple Usability and Authentication Comparison
Double Pattern Recall
Open Response Questions, Submission

Figure 1: Survey structure

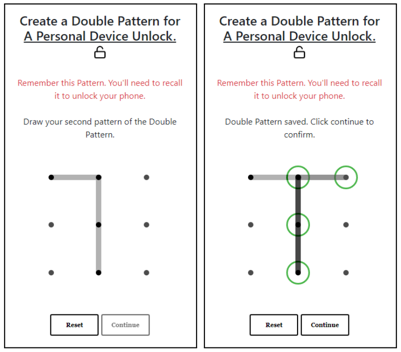
Introduction

Android unlock patterns are a widely recognized and utilized graphical password scheme is Android unlock patterns [4], whereby users recall a previously selected pattern drawn on a 3x3 grid of contact points to unlock their device. Despite there being multiple options to unlock their device, many users (as much as 26% in our study, for example) still rely on unlock patterns as their primary knowledge based authentication; the password used to unlock their device when biometrics are disabled, fail, are not-available, or the device initially boots.

The design and deployment of patterns has remained mostly static since its initial launch in 2008. As compared to other unlock authentication, such as PINs on iOS devices that have moved towards recommending 6-digits as opposed 4-digits, similar design updates for patterns are more allusive.

Although there are $389\,112$ possible patterns, users tend to select from a much smaller set of patterns in predictable ways [2]. It has been shown that user-generated patterns are roughly as random as selecting a 3-digit, numeric PIN [7]. There have been a number of proposals to improve the current state, such as providing user guided selection [3] or password-meters [5], however, these interfaces require add-on design principles that change the user-interface (UI) of Android unlock patterns. Further design changes, such as 4x4 patterns [1] or rings of contact points [7, 6], appear to have limited security benefits and also require substantial changes to the core Android pattern usage model.

We propose *Double Patterns*, whereby a user selects two patterns, entered in sequence and displayed super-imposed, as their unlock authentication. We seek to keep the same simple design of the 3x3 grid, but increase the natural complexity. From a security framework, Double Patterns should greatly increases the complexity of the password space.


Create a Double Pattern for A Personal Device Unlock.

Remember this Pattern. You'll need to recall it to unlock your phone.

Draw your second pattern of the Double Pattern.

Create a Double Pattern for A Personal Device Unlock.

Remember this Pattern. You'll need to recall it to unlock your phone.

Double Pattern saved. Click continue to confirm.

Figure 2: Double Pattern creation process

There are $389\,112$ possible patterns, and thus, there are $(389\,112)^2$ possible Double Patterns, or roughly 151×10^9 (which is still far less than 4.3×10^{12} possible 4x4 patterns).

While there have been a number of proposals to improve the current state, such as providing user guided selection [3] or password-meters [5], these interfaces require add-on design principles that potentially significantly change the user-interface (UI) of Android unlock patterns. The simplicity of the Android UI is one of the distinguishing features that made them popular in the first place. From a usability framework, given the wide usage of Android patterns, we hypothesized that users would find the new interface natural and straightforward, even with the slight time increase in entry. A similar usability trade-off is already present given that users have adopted 6-digit PINs without much conflict.

We have conducted a series of studies to assess the potential usability and security of Double Patterns. We first performed a preliminary study with $n = 286$ participants, as a preliminary investigation, to hone our survey material and collect a sample set of Double Patterns. Following, we performed our main study ($n = 634$) to assess the feasibil-

	Control	BL First	BL Double	**Total**
18-24	17	26	19	62
25-29	52	61	55	168
30-34	45	41	57	143
35-39	47	35	35	117
40-44	14	21	17	52
45-49	17	11	14	42
50-54	6	7	9	22
55-59	5	5	3	13
60-64	2	1	2	5
65+	2	3	3	8
Prefer not to say	2	0	0	2
Male	112	123	135	370
Female	95	84	74	253
Non-binary	0	3	5	8
Prefer not to say	2	1	0	3
Total	**209**	**211**	**214**	**634**

Table 1: Demographic information of the participants, column names are shorthand for treatments

	Control	BL First	BL Double	**Total**
No Devices	0	1	0	1
1 Device	122	123	129	374
2 Devices	66	73	67	206
3 Devices	17	10	15	42
4 Devices	4	4	3	11
Iris Recognition	0	2	1	3
Finger Print	108	106	111	325
Facial Recognition	26	26	26	78
No Biometric	72	70	67	209
Other Form	3	7	6	16
Pattern	57	49	56	162
4-Digit PIN	96	89	98	283
6-Digit PIN	29	34	36	99
PIN of Other Length	8	8	7	23
Alpha-Numeric	6	12	9	27
Not Listed	11	16	7	34
Prefer not say	2	3	1	6
Total	**209**	**211**	**214**	**634**

Table 2: Participant device utilization, column names are shorthand for treatments

ity of the Double Pattern interface based on its security and usability, where participants selected Double Patterns on their own mobile device and answered questions about the usability and perceived security of the new interface.

The preliminary results indicate that users find the updated interface highly usable and show a favorable level of confidence about the security of Double Patterns relative to existing authentication methods. In our continuing work, we will assess the guessability of Double Patterns as they compare to previous studies on Android unlock patterns.

Methodology

We conducted a preliminary study and a main study. In the preliminary study, we asked participants to select Double Patterns in multiple application scenarios, such as banking, shopping, and mobile device unlocking, as well as answer feedback questions. We found that our design of the preliminary study led to unintended bias in user selected Double Patterns; namely, during the instructions, we offered a sample Double Pattern, which our users overly selected as their choice of Double Pattern for at least one of the scenarios. We corrected this bias in our main study by updating our survey content and implementing two types of blacklist treatments as a replacement for the application scenarios. Our blacklists were informed by a sub-sample of the 20 most frequently selected patterns in the preliminary study.

All studies were conducted on Amazon Mechanical Turk. We recruited $n = 286$ for the preliminary study (collecting 572 double patterns), and $n = 634$ (collecting 634 double patterns) for the main study. The demographics of our main studies are presented in Table 1, and we discuss the methods for the main study in the rest of this section.

Survey Structure. See Figure 1 for the main structure survey. After participants have agreed to our informed consent, we begin by surveying them of their current device usage and mobile authentication choices. Those response can be found Table 2. Following, we inform participants about Android unlock patterns using a description of the interface and visuals, and we then introduce the Double Pattern interface and the ruleset that governs it.

Next, we give participants an opportunity to practice using the Double Pattern interface, with minimal direction or assistance, to avoid biasing selections, and after completing the practice, we prime the participants by informing them that they should create a Double Pattern that they would use to secure their own smartphone. The language used to prime users during pattern creation directly parallels language a user would encounter when initially creating a pattern on an Android device. The device we specifically referenced was a Samsung Galaxy S8.

Participants select their Double Pattern using the same interface they practiced on, and once they confirm their pattern it is saved, as is the case on Android devices. During selection, as we will discuss in the following section, some participants may encounter a blacklist of Double Patterns, forcing them to select a different choice.

After selection, participants are directed to answer a set of sentiment questions about their process for creating the pattern. The questions focus on their creation strategy, if they felt the pattern they created provides adequate security, and if it was difficult for them to create a pattern. We also field System Usability Scale questions to gauge user sentiment on the usability of our system.

Using the sentiment questions as a distractor task, participants recalled the Double Pattern selected earlier. After three attempts, they are presented with an option to indicate they cannot remember, and they are moved forward in the survey automatically after five attempts.

Authentication Comparison (Likert Scale)

1. Double Patterns are a secure way to unlock my personal device.
2. Double Patterns are more secure than 4-digit PIN codes for unlocking my personal device.
3. Double Patterns are more secure than 6-digit PIN codes for unlocking my personal device.
4. Double Patterns are more secure than alpha-numeric passwords for unlocking my personal device.
5. Double Patterns are more secure than the original Android Patterns for unlocking my personal device.

Real World Utilization

1. In a situation where your biometric fails or your mobile device reboots and you are utilizing a Double Pattern to unlock your personal mobile device, would you use the Double Pattern you selected in this survey, or would you select a different one?
2. You have indicated that you (would use|would not use|are unsure if you would use) the Double Pattern you created in this survey on your personal mobile device. Please expand on your choice here.

Figure 3: Questions fielded in our survey

At the end of the survey, we collect standard demographic information, as well as information that may influence usability aspects of our interface, such as dominant handedness and academic involvement in the information technology field. Participants are asked if they have completed the survey honestly, and given a final chance to submit any feedback based on the survey itself or the interface.

Blacklist Treatments. Using data from our preliminary study, we implemented three treatments, including two treatments with an enforcing blacklist implementation. Participants were unaware of the blacklist prior to their first encounter. The different treatments are (with shorthand):

- Control Treatment (**Control**)
- Blacklist First Component Pattern (**BL First**)
- Blacklist Double Pattern (**BL Double**)

These blacklists only affect users when they are creating a Double Pattern for the scenario of securing their mobile device, not during their practice in creating Double Patterns. We felt it was important to separate learning the interface from creating an appropriate Double Pattern.

In the *Control* treatment, users were free to create any Double Pattern. In the *Blacklist First Component Pattern* treatment, if a user draws their first component pattern and it is blacklisted, they are immediately presented with a warning message informing them, "The first pattern of your Double Pattern can be easily guessed" and forced to start the process from the beginning. In the *Blacklist Double Pattern* treatment, the user is able to draw an entire Double Pattern before being informed, "The Double Pattern you created can be easily guessed" and forced to select a different one.

Recruitment. We recruited our participants using Amazon Mechanical Turk. Our preliminary study was comprised of 286 participants, and we ensured that participants who conducted our preliminary study were not able to also take our main survey. For our main study, our goal was to collect at least 200 participants from each treatment, with 600 Double Patterns in total. The demographic breakdown of our participants can be found in Table 1. Participants were compensated $1.00 for their participation. The study was approved by our IRBs.

	Average Attempts [std] (med)	**Recall Rate**
Control	1.36 [0.86] (1.00)	97.1%
Blacklist First	1.47 [0.96] (1.00)	94.8%
Blacklist Both	1.30 [0.70] (1.00)	97.2%
Overall	**1.38 [0.85] (1.00)**	**96.4%**

Table 3: Participant recall rates

Limitations. One of the primary limitations of our study is the user base we are collecting our sample from; the participant group may not accurately represent a larger population. The majority of our users are right handed, males, 35 or under, live in a suburban environment, have an associates or higher level degree, and have no background working in the information technology field. However, this still composes a large user base of Android devices, and we would argue that they likely generalize or, at least, provide an important data point for usability and security as they relate to the modification of Double Patterns. The demographics are also inline with prior work on the topic.

Another limitation our study faces is the validity of patterns chosen in our survey. While we paralleled the selection process a user would encounter in a real world scenario, the subject is ultimately aware that we will see their pattern selection. We address this with our *Real World Utilization questions and the responses we observed from users.*

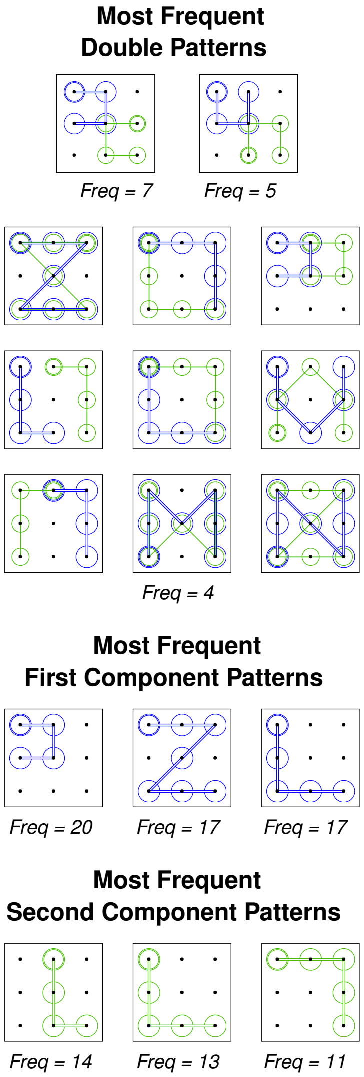


Figure 4: Frequent Double Pattern occurrences

Preliminary Results

The preliminary results from our analysis of Double Pattern data show an increase in pattern complexity with a low trade off in interface usability. We will discuss the frequency rate in which Double Patterns are selected, the effects that blacklisting had on Double Pattern and component pattern complexity, and the usability of our interface in the form of both simple usability scale results and the additional time required to utilize our new interface. Our continuing work will discuss updating our blacklists, performing guessing analysis, and the inclusion of further analysis of the qualitative and quantitative feedback.

Pattern Frequency. Only 8.0% of all Double Patterns were utilized twice or more; however, in the Blacklist First treatment no Double Pattern occurred more than twice, comprising a mere 3.8% of our Double Patterns collected in this set. In previous work on Android unlock patterns, Aviv et al. reviewed repetitions in a self-report and pen and paper study of 3x3 patterns [1]. Among the groups studied, the prevalence of repeated patterns was found to comprise over 40% of the patterns collected in several cases. As well, around 20% of the patterns in every data set were found to repeat at least 4 times.

The Effect of Blacklists. We measured the effects of blacklisting on the distinct features appearing in the Double Patterns. In our *Blacklist First Component Pattern* treatment, 70/211 (33.2%) users encountered a blacklist after drawing their initial component pattern. 19/214 (8.9%) users encountered a blacklist after drawing their initial Double Pattern in the *Blacklist Double Pattern* treatment.

We looked at the frequency with which the following features appeared in the overall Double Pattern, as well as each component pattern:

- pattern length, the number of contact points used;
- stroke length, the length of the strokes when the grid is mapped to a Cartesian plane;
- contact point utilization, the number of contact points used on the grid in the construction of the Double Pattern, ignoring repetition;
- turns, the number of turns, or direct changes, in the patterns;
- knight moves, the number of oblique, non 90-degree angle strokes, as a knight moves in chess;
- non-adjacencies, the number of times two contact points, non-adjacent, in the grid are connected.

We also examined the frequency with which the second component pattern was a palindrome of the first, and the frequency that users chose the same contact point to both end their first component pattern, and begin their second component pattern, a term we deemed "overlap".

Examining each feature, we used an Anderson-Darling Pairwise Test to determine if treatment populations had a normal distribution in regard to each individual feature. For the features that were not of a normal distribution, we then used a Kruskal-Wallis One-Way Analysis of Variance with Dunn post-hoc Analysis and Holm-Sidak correction to determine statistical differences among treatment populations.

As a result of the pairwise testing and subsequent post-hoc analysis, the Double Patterns within our *Blacklist First Component Pattern* treatment showed significant statistical differences from the other two treatment populations in overall amount of turns (H=21.5, p<0.001), amount of turns in the first component pattern (H=31.0, p<0.001), first pattern knight moves (H=7.2, p=0.026), first pattern non-adjacency moves (H=7.3, p=0.021), and total contact point utilization (H=7.0, p=0.025). We conjecture that the high rate of encounters with the blacklist within the *Blacklist First*

Treatment	Average [std](median)
Control	3.83 [2.40] (3.15)
Blacklist First	4.02 [2.09] (3.29)
Blacklist Both	3.62 [2.04] (3.12)
All Patterns	3.82 [2.18] (3.17)

Table 4: Time to recall Double Pattern

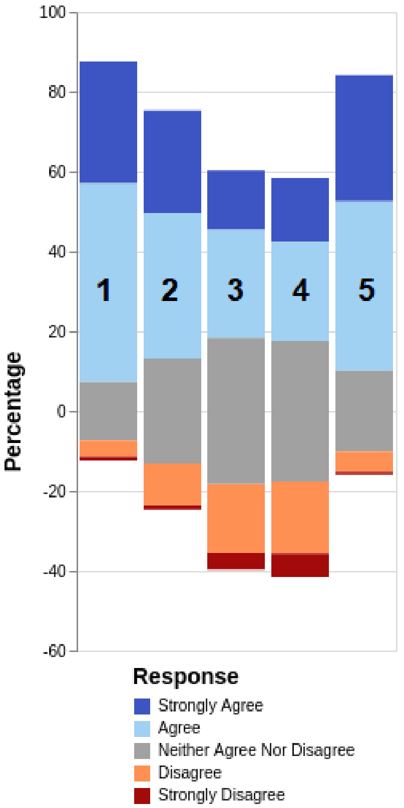


Figure 5: Authentication method comparison, order of results detailed in Figure 3

Component Pattern treatment may have motivated the participants to revise their first component pattern by adding more complex features, to overcome the blacklist they initially encountered.

Time Cost of the Enhanced Interface. Based on an online survey by Harbach et al. ($n = 260$) and field study ($n = 52$), users took on average 3.0 seconds (*sd* = 13.3s, median = 1.69s) to activate and unlock a phone utilizing a lock pattern, and 4.7 seconds (*sd* = 20.72s, median = 2.85s) when utilizing a numeric PIN [4]. Across all treatments in our study ($n = 634$), our Double Pattern interface took an average of 3.82 seconds (*sd* = 2.18s, median = 3.17s). These results reflect only a marginal increase in timing during the unlocking process, while increasing the complexity of the pattern space exponentially. Table 4 shows a more detailed breakdown of time usage for the Double Pattern interface.

System Usability Scale and Existing Authentication Sentiments. Among all users, the System Usability Scale score was 73.2. This equates to a good, acceptable system, with a passive promoter score. As well, these users on average, agreed that Double Patterns were a secure authentication method, and that Double Patterns are a more secure form of authentication than 4-digit PIN's and the original Android Unlock Pattern. 162/634 (26%) of the users surveyed utilize an Android unlock pattern as their form of knowledge based authentication. Among users that already utilize an Android unlock pattern, the System Usability Scale score was 78.3. This equates to a good, acceptable system, with an active promoter score. As for direct comparison of Double Pattern to other forms of authentication, these users not only agreed on average that Double Patterns are a secure authentication method, but they also agreed that Double Patterns are a more secure form of authentication than 4-digit PIN's, 6-digit PIN's, alpha-numeric passwords, and the original Android unlock pattern. Both System Usability Scores and our own comparison confidence scores among users previously utilizing the Android unlock pattern interface were higher and more distinct in sentiment across all treatments and metrics than the remaining participants.

Summary Discussion. There is strong evidence from these preliminary results that Double Patterns could be a viable and more secure alternative to the single, Android pattern. Participants expressed positive usability, particularly amongst those that already use an Android pattern. Entry and recall time (a proxy for usability) is relatively stable, even when participants experience a blacklist and are forced to choose a different Double Pattern. While future work is needed to evaluate the security using standard guessability metrics, these preliminary results that the straightforward interface change can be highly effective.

Future Work

Continuing our work with Double Patterns, we will begin examining the qualitative data we have collected. Initial observations indicate that users are optimistic about the implementation of Double Patterns; some users have gone so far as to say that they would utilize the new interface when it became available. These types of responses show promise and are a good indication that our subtle changes have positively impacted users.

Acknowledgments. This material is based upon work supported by the National Science Foundation under Grant No. (1845300).

REFERENCES

[1] Adam J. Aviv, Devon Budzitowski, and Ravi Kuber. 2015. Is Bigger Better? Comparing User-Generated

Passwords on 3x3 vs. 4x4 Grid Sizes for Android's Pattern Unlock. In *Annual Computer Security Applications Conference (ACSAC '15)*. ACM, Los Angeles, California, USA, 301–310.

[2] Adam J. Aviv and Markus Dürmuth. 2018. A Survey of Collection Methods and Cross-Data Set Comparison of Android Unlock Patterns. *CoRR* abs/1811.10548 (Nov. 2018), 1–20.

[3] Geumhwan Cho, Jun Ho Huh, Junsung Cho, Seongyeol Oh, Youngbae Song, and Hyoungshick Kim. 2017. SysPal: System-Guided Pattern Locks for Android. In *IEEE Symposium on Security and Privacy (SP '17)*. IEEE, San Jose, California, USA, 338–356.

[4] Marian Harbach, Emanuel von Zezschwitz, Andreas Fichtner, Alexander De Luca, and Matthew Smith. 2014. It's a Hard Lock Life: A Field Study of Smartphone (Un)Locking Behavior and Risk Perception. In *Symposium on Usable Privacy and Security (SOUPS '14)*. USENIX, Menlo Park, California, USA, 213–230.

[5] Youngbae Song, Geumhwan Cho, Seongyeol Oh, Hyoungshick Kim, and Jun Ho Huh. 2015. On the Effectiveness of Pattern Lock Strength Meters: Measuring the Strength of Real World Pattern Locks. In *ACM Conference on Human Factors in Computing Systems (CHI '15)*. ACM, Seoul, Republic of Korea, 2343–2352.

[6] Harshal Tupsamudre, Vijayanand Banahatti, Sachin Lodha, and Ketan Vyas. 2017. Pass-O: A Proposal to Improve the Security of Pattern Unlock Scheme. In *Proceedings of the 2017 ACM on Asia Conference on Computer and Communications Security (ASIA CCS '17)*. ACM, New York, NY, USA, 400–407. DOI: http://dx.doi.org/10.1145/3052973.3053041

[7] Sebastian Uellenbeck, Markus Dürmuth, Christopher Wolf, and Thorsten Holz. 2013. Quantifying the Security of Graphical Passwords: The Case of Android Unlock Patterns. In *ACM Conference on Computer and Communications Security (CCS '13)*. ACM, Berlin, Germany, 161–172.