

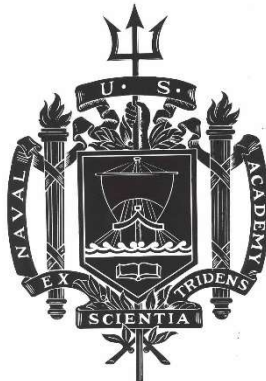
A TRIDENT SCHOLAR PROJECT REPORT

NO. 493

Improving the Security of Android Unlock Patterns Using New Iterations of the Standard Pattern Lock

by

Midshipman 1/C Timothy J. Forman, USN



UNITED STATES NAVAL ACADEMY
ANNAPOLIS, MARYLAND

This document has been approved for public
release and sale; its distribution is unlimited.

USNA-1531-2

REPORT DOCUMENTATION PAGE			Form Approved OMB No. 0704-0188	
Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing this collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden to Department of Defense, Washington Headquarters Services, Directorate for Information Operations and Reports (0704-0188), 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302. Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to any penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number. PLEASE DO NOT RETURN YOUR FORM TO THE ABOVE ADDRESS.				
1. REPORT DATE (DD-MM-YYYY) 7/6/20		2. REPORT TYPE		3. DATES COVERED (From - To)
4. TITLE AND SUBTITLE Improving the Security of Android Unlock Patterns Using New Iterations of the Standard Pattern Lock Interface		5a. CONTRACT NUMBER		
		5b. GRANT NUMBER		
		5c. PROGRAM ELEMENT NUMBER		
6. AUTHOR(S) Forman, Timothy J.		5d. PROJECT NUMBER		
		5e. TASK NUMBER		
		5f. WORK UNIT NUMBER		
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)		8. PERFORMING ORGANIZATION REPORT NUMBER		
9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES) U.S. Naval Academy Annapolis, MD 21402		10. SPONSOR/MONITOR'S ACRONYM(S)		
		11. SPONSOR/MONITOR'S REPORT NUMBER(S) Trident Scholar Report no. 493 (2020)		
12. DISTRIBUTION / AVAILABILITY STATEMENT This document has been approved for public release; its distribution is UNLIMITED.				
13. SUPPLEMENTARY NOTES				
14. ABSTRACT Android mobile devices use a unique method of authentication in the form of a single-stroke graphical pattern on a 3x3 grid that a user is required to create and recall. In this research project, we are going to explore improved iterations of this Android Pattern Lock in the pursuit of guiding users towards creating more secure patterns. Within the past five years, Mobile Authentication methods have continually progressed towards creating a more secure means to safeguard a mobile device. Such methods now include biometric identification, system assisted password guidance via blacklists, and longer minimum passcode lengths. While many methods have progressed, the standard authentication interface for Android devices remains similar in comparison to its initial model. In this work, we sought to explore the effects of changing the existing Android pattern lock interface to an interface we deemed the Double Pattern. We examined the methodologies by which users chose their Double Patterns using our new interface, specifically metrics related to the complexity of the patterns created, pattern frequency within each treatment population, usability aspects of the interface itself, security strength of our interface, and perceived security strength related to existing authentication methods. Ultimately, we found that our Double Pattern had a significant increase in security related to lower partial guessing entropy and lower susceptibility to simulated guessing attacks, due to the low occurrence rate of each Double Pattern. Equally important, participants perceived the Double Pattern as a more secure interface than the original interface, specifically within our users who previously utilized Android unlock patterns. We are confident based on these results that the Double Pattern could be feasibly implemented as a progression of the original Android unlock pattern interface.				
15. SUBJECT TERMS Double Pattern, Android Unlock Pattern, Biometrics, Mobile Authentication, Security, Usability				
16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES 36
a. REPORT	b. ABSTRACT	c. THIS PAGE		
				19a. NAME OF RESPONSIBLE PERSON
				19b. TELEPHONE NUMBER (include area code)

**IMPROVING THE SECURITY OF ANDROID UNLOCK PATTERNS USING
NEW ITERATIONS OF THE STANDARD PATTERN LOCK**

by

Midshipman 1/C Timothy J. Forman
United States Naval Academy
Annapolis, Maryland

(signature)

(date)

Certification of Adviser(s) Approval

Dr. Adam Aviv
The George Washington University
Washington, D.C.

(signature)

(date)

Dr. Daniel S. Roche
United States Naval Academy
Annapolis, Maryland

(signature)

(date)

Acceptance for the Trident Scholar Committee

Professor Maria J. Schroeder
Associate Director of Midshipman Research

(signature)

(date)

Abstract

Android mobile devices use a unique method of authentication in the form of a single-stroke graphical pattern on a 3x3 grid that a user is required to create and recall. In this research project, we are going to explore improved iterations of this Android Pattern Lock in the pursuit of guiding users towards creating more secure patterns. Within the past five years, Mobile Authentication methods have continually progressed towards creating a more secure means to safeguard a mobile device. Such methods now include biometric identification, system assisted password guidance via blacklists, and longer minimum passcode lengths. While many methods have progressed, the standard authentication interface for Android devices remains similar in comparison to its initial model. In this work, we sought to explore the effects of changing the existing Android pattern lock interface to an interface we deemed the Double Pattern.

We examined the methodologies by which users chose their Double Patterns using our new interface, specifically metrics related to the complexity of the patterns created, pattern frequency within each treatment population, usability aspects of the interface itself, security strength of our interface, and perceived security strength related to existing authentication methods. Ultimately, we found that our Double Pattern had a significant increase in security related to lower partial guessing entropy and lower susceptibility to simulated guessing attacks, due to the low occurrence rate of each Double Pattern. Equally important, participants perceived the Double Pattern as a more secure interface than the original interface, specifically within our users who previously utilized Android unlock patterns. We are confident based on these results that the Double Pattern could be feasibly implemented as a progression of the original Android unlock pattern interface.

Keywords: Double Pattern, Android Unlock Pattern, Biometrics, Mobile Authentication, Security, Usability

Table of Contents

1	Introduction	4
1.1	Mobile Device Authentication	4
1.2	Motivation	4
1.3	Organization of This Report	5
2	Android Unlock Patterns	6
2.1	Graphical Passwords	6
2.2	An Introduction to the Android Unlock Interface	6
3	Problem Statement	8
3.1	Known Shortcomings of Android Unlock Patterns	8
3.2	Updates to Android Unlock Patterns	8
3.3	Previous Solutions to Known Shortcomings	9
3.4	Our Proposed Solution	9
4	Methodology	11
4.1	Recruiting Survey Participants	11
4.2	Survey Structure	11
4.3	Limitations	14
5	Fielding Our Double Pattern Study	16
5.1	Initial Iterations of Survey	16
5.2	Design Changes and the Implementation of Blacklisting	17
6	Results	18
6.1	Blacklisting and Ideal Choice	18
6.2	Pattern Features Among Treatments	19
6.3	Pattern Frequency	19
6.4	Partial Guessing Entropy	20
6.5	Simulated Guessing Attack	22
6.6	Recall Rates Among Participants	22
6.7	Entry Time Using the Enhanced Interface	23
6.8	Usability	23
6.9	Comparison to Existing Authentication	24
6.10	Qualitative Analysis of User Feedback	25
7	Work in Progress	27
7.1	Multi-functionality of Our Survey	27
7.2	Updating the Blacklist for Future Collection	27
8	Conclusions	28

Appendices

Chapter 1

Introduction

Data privacy is of the utmost concern in our digital age. With the exponential growth of computing power and inter-connectivity between individuals that has occurred in the last decade, substantial amounts of user data have been collected, disseminated, and studied to improve the technology that makes our everyday lives easier. At the heart of this change is a conflict between usability and security. As mobile computing devices, i.e. smartphones, have developed and become more robust in nature, they have come to represent this conflict in a very real way. These devices contain a large amount of personally sensitive data, including banking information, social media credentials, and private conversations with family and friends. When a user makes the decision to store this type of information on a mobile computing device, there is an understanding that they expect privacy of their data.

Privacy in mobile computing begins with a user being able to securely authenticate themselves as the intended owner of their own device. Once trust is established between a user and their device, they are given access to the information contained on that device. The main conflict then, stems from allowing users to assuredly authenticate themselves, while maintaining a usable and timely security interface. There has been extensive research specifically concerned with this conflict, as it relates to authentication on mobile devices.

1.1 Mobile Device Authentication

Mobile authentication is the means by which a mobile device user verifies their identity to gain entry into their device. On smartphones, user authentication schemes fall into the categories of (i) knowledge-based, including PINs and graphical passwords, (ii) biometric, including facial recognition and fingerprints, and (iii) security tokens for two-factor authentication. The most commonly utilized are the knowledge-based schemes such as PINs and graphical passwords, which includes Android Unlock Patterns [1].

1.2 Motivation

Mobile Devices are used on a global scale, at rate that increases daily. The amount of smartphones in use worldwide is well over 3 billion, and expected to grow to near the figure of 6.8 billion by the year 2022 [2]. With over half of these users utilizing an Android operating system, the refinement and improvement of Android mobile authentication has become a research field with global implications.

This field should be of particular interest to Naval Academy, as security of information is always a concern for any military force. Specific to the Navy, we are a global force that operates

in theatres around the world. In those theatres, the Navy consists of service members who use Android devices. While the majority of military members do not intentionally store sensitive data on their mobile devices, the applications that have access to this data are likely unsecured and if an adversary gains access to the device, they then subsequently gain access to those vulnerable applications. In a worst case scenario, creating a more secure means of authentication for those Android devices may mean the difference between an unusable stolen phone, and gigabytes of sensitive data being lost to an adversary.

1.3 Organization of This Report

This report will first identify the space in which our research is being conducted. We will then present issues of focus in this space, and previous work to address them. We propose our own solution, and justify the methodology behind how we conducted our work. Next, we present our current work and findings thus far, and future work we will conduct to further these efforts. Finally, we will present and discuss our conclusions based on the data we have collected and our analysis of this data.

Chapter 2

Android Unlock Patterns

Android unlock patterns are one of, if not the most prevalent form of graphical passwords in use today. Unlock patterns are a knowledge-based authenticator, and by incorporating visual aspects the interface, the patterns form a memorable image in the users' mind, as opposed to a string of characters. Despite there being many different forms of mobile authentication available to users, such as PINs, Android patterns remains quite popular, with 26% in our Double Pattern study having reported using it as a their primary, knowledge based authentication; this equates to likely millions of Android pattern users worldwide.

2.1 Graphical Passwords

One widely utilized type of mobile authentication is a graphical password, which was first proposed in 1999 as an alternative means to using the text based methods previously employed [3]. Graphical passwords utilize users' image based recognition, something their brains are well-suited for [4]. The most widely recognized and utilized graphical pattern on mobile devices is the Pattern Lock used on Android phones [5]. Using a Pattern Lock, users "draw" a pattern within a 3x3 grid that connects a continuous set of four or more contact points. If the selected pattern matches the pattern established during the creation of the pattern, the user is granted entry into the device.

2.2 An Introduction to the Android Unlock Interface

Android graphical patterns are a form of authentication used to unlock Android smartphones and tablets. Android unlock patterns are graphical passwords, and can be seen as an evolution

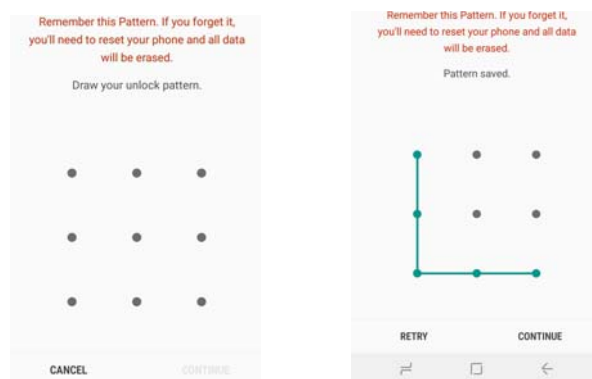


Figure 2.1: Android Pattern Lock interface on a Galaxy S8.

from the Pass-Go architecture [3], as they rely on a basic graphic interface. However, the Android specific interface has a more stringent set of rules for pattern selection. A pattern consists of a 3x3 grid, where a user "draws" a pattern with a single stroke during the selection process. When a user selects a pattern, it must adhere to the following ruleset:

1. No less than four contact points must be selected.
2. No repetition of contact points.
3. Only straight lines are allowed.
4. All contact points along a path must be connected, unless previously selected.

For an example of the pattern interface typically by seen by users, refer to Figure 2.1.

Chapter 3

Problem Statement

While Android Unlock Patterns are widely used, they are not without some well known shortcomings [6, 7, 4, 8]. Our goal at the onset of this project was to identify shortcomings of the interface, gain a deeper understanding of these problems, propose our own solutions, and test their implementation with real mobile device users.

3.1 Known Shortcomings of Android Unlock Patterns

One of the primary shortcomings associated with Unlock Patterns is that they are a knowledge-based authentication method, and require human interaction during the pattern selection phase. Aviv et al. showed that there are 389,112 possible patterns [7], yet given these options users select from a very limited variety of common and often guessable patterns. The resulting user-generated patterns are approximately as random as selecting a 3-digit, numeric PIN [4]. This shortcoming is one of the primary focal points of our work, and one we seek to address with our design extensions to the Android Unlock Interface.

Studies have also shown that patterns are vulnerable to a multitude of attack vectors. One such vector is a smudge attack, common to smartphones that utilize a touchscreen for authentication [9]. In a previous study, researchers were able to partially identify up to 92% of patterns and fully identify 68% of patterns, solely based on smartphone screen smudges [9]. Another relevant attack vector concerning Android Unlock Patterns is shoulder surfing, by which an attacker observes a user authentication entry [10]. These attacks both directly impact Android Unlock Patterns, and countering these attack vectors is another primary focal point of our work.

3.2 Updates to Android Unlock Patterns

Compared to other forms of unlock authentication, namely PINs, the design and deployment of patterns have remained mostly static since first launch in 2008 [1]. While most platforms, such as iOS, request that users select 6-digit as opposed to 4-digit PINs, as originally designed, the same basic design and implementation of patterns, namely the use of a 3x3 contract grid, remains the dominant form today without any substantial design change.

There have been a number of proposals to improve the current state, such as providing user guided selection [8] or password-meters [11], however, these interfaces require add-on design principles that change the user-interface (UI) of Android unlock patterns. Our works seeks to design a natural extension to Android patterns that will improve security while keeping the original design features in place.

3.3 Previous Solutions to Known Shortcomings

To address these shortcomings, previous work in this space has varied in the approach taken to improve the interface. Some proposals have chosen to alter the existing interface to enhance security. One such example of this approach is the implementation of password meters during the selection phase of patterns [12, 11]. Another approach to modifying the interface consisted of changing the contact point layout [4, 13]. Aviv et al. explored the results of expanding from a 3x3 to a 4x4 grid of contact points [7]. One key drawback of these proposed changes is that they place an extra burden on the user by changing the visual user-interface (UI) of Android unlock patterns. The ease of use associated with the Android UI is one of the factors that we believe makes it appealing for users to begin with.

The alternative to subtle changes to the existing interface is instead to implement an alternative rule set during pattern selection. One such example of this is detailed by Cho et al. in *SysPal*, where users are required to use system specified contact points during the pattern selection phase [8]. Another related work in this space is that of Colley et al., who released a preliminary study focused on the repetition of contact points as well as measured time duplication during pattern selection [14]. Both of these studies focused on using the existing UI, implementing an incremental rather than substantial change to the authentication scheme in place.

Along the lines of alternative rule sets, we also sought to explore the effects of blacklisting on pattern choice. Interfaces such as Apple’s 6-digit PIN already utilize blacklisting on their devices. As it pertains to Android unlock patterns, previous work in the field has consisted of physical blacklisting, by changing the interface appearance or omitting commonly used contact points [4], but no notable studies have been published on the effects of blacklisting patterns themselves.

3.4 Our Proposed Solution

As an alternative to drastically changing the UI, we sought to study the effects of fielding slight alterations to the existing interface, with the goal in mind that the resulting patterns will be more secure according to quantifiable security metrics, such as guessability. Our motivation for creating more secure iterations of the Pattern Lock interface stems from the realistic approach that users would not openly receive a vastly different form of mobile authentication that we propose. With this in mind, we would enhance the already existing means by which users secure their devices, using both slight behavioral alterations and minimal interface modifications to increase the security of the system.

We proposed a set of four new interfaces, two of which were to alter the existing interface, and two of which modified the existing rule set. Based on these four new interfaces, our goal was to collect data on how users react and compare them to a control study conducted in the same experimental space. We deemed the four new interfaces Double Pattern, Lift and Repeat, 4x4 Unlock, and Repeat. Visual prototypes of each interface can be seen in Figure 3.1.

After our initial data collection process and data analysis from Double Patterns, we chose to pursue studying this new interface specifically. We felt that the results of further studying this interface alone would be much more promising than comparing four interfaces against one another. We decided on implementing two types of blacklists alongside our control treatment, with the goal of collecting 200 samples from each of these populations. Our work builds on previous studies

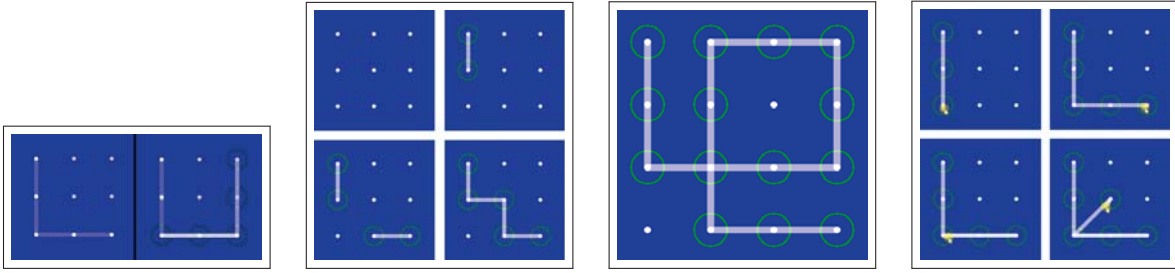


Figure 3.1: From left to right: Our prototype interface for Double Pattern, Lift and Repeat, 4x4 Unlock, and Repeat.

in the field, by studying metrics such as notable pattern features, interface usability, timing, recall rates, and security metrics such as guessability [7]. We compare our Double Pattern populations against a corpus of previously collected 3x3 and 4x4 Android Unlock Patterns, as well as 4-digit and 6-digit PIN's.

Chapter 4

Methodology

We utilized a survey framework to collect information on our Double Pattern interface. The data collected within each survey includes information such as participants' demographic data, pattern selection results, timing information on user interactions, recall attempts, and responses to simple usability questions based on the interface the participant was given within their respective survey. Our survey also gauged sentiment on how the newly proposed interface compares to existing methods familiar with the participants.

4.1 Recruiting Survey Participants

We recruited our participants using Amazon Mechanical Turk. Our pilot study was comprised of 286 participants, and we ensured that participants who conducted our pilot 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 4.1. Participants were compensated \$1.00 for their participation. The study was approved by our institutions' IRB.

4.2 Survey Structure

Our survey begins with device utilization questions after participants have agreed to our informed consent. These questions relate to their device usage and the authentication methods they currently utilize. The device utilization questions, detailed in figure 4.4, also address if they utilize a biometric, and if so, which type they use. As well, regardless of whether or not they utilize a biometric, there is a secondary question that ascertains which knowledge-based authenticator they use, either as a primary means of authentication, or a secondary means to their biometric. We were particularly interested in participants who are currently using the original Android unlock pattern interface and their responses within our survey.

We introduce and describe the Android unlock pattern interface as an authentication method that employs a participant to "draw" a shape connecting at least four contact points. We include the screenshot in figure 2.1 to familiarize the participant with the appearance of the interface, however there is no pattern displayed as we do not want to bias participants towards any selection. To reiterate, the ruleset for Android unlock patterns is as follows:

1. No less than four contact points must be selected.
2. No repetition of contact points.
3. Only straight lines are allowed.

4. All contact points along a path must be connected, unless previously selected.

	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
High School	18	15	25	58
Trade	15	6	5	26
Some-College	42	43	47	132
Associates	24	27	16	67
Bachelor's	82	92	89	263
Master's	19	16	26	61
Professional	0	5	4	9
Doctorate	4	3	1	8
Prefer not to say	4	0	0	4
Total	209	211	214	634

	Control	BL First	BL Double	Total
Tech	62	66	55	183
No-Tech	140	139	154	433
Prefer not to say	7	6	5	18
Left-Handed	24	16	31	71
Right-Handed	177	188	176	541
Ambidextrous	7	7	7	21
Prefer not to say	1	0	0	1
Rural	34	32	36	102
Suburban	98	108	116	322
Urban	75	71	62	208
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 4.1: Demographic Information of the Participants

We introduce our new interface, and the ruleset that governs Double Patterns, with these instructions:

Double Pattern Locks are the same as Pattern Locks but require you to "draw" two shapes on the same 3x3 grid of contact points. The combination of the two patterns entered in the same order is now used to unlock your smartphone. Each pattern in a Double Pattern is drawn the same way as before, but once you finish drawing your first pattern by lifting your finger, you then draw a second pattern. When drawing your second pattern, the first pattern will be displayed, and you may reuse contact points from your first pattern in drawing your second. However, you may not use your first pattern as your second pattern.

Participants are given an opportunity to utilize the pattern interface, with minimal direction other than the introduction on the previous page of the survey. Our purpose for this is to allow a realistic initial experience with this interface, and determine participants' sentiment on interacting and creating a Double Pattern for the first time without assistance. Following the interface in which we allow participants to practice creating a Double Pattern, we prime the participant by informing them that they will create a Double Pattern that they would likely use on their own smartphone. We ask that they do not annotate their Double Pattern or use other means to aid them in recalling it at a later point.

Participants are presented with a similar interface to the practice page previously seen in the survey, with two adjustments. The first adjustment being, once they select and confirm a valid Double Pattern, they proceed to the next section of the survey, rather than being given the chance

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 4.1: Questions fielded in our survey gauging the participant’s sentiment on real world utilization of the Double Pattern they chose.

to create more patterns. The second adjustment is that at this point in the survey, the participant has been divided into one of three treatment groups, which will be discussed in a later segment. After creation of a Double Pattern, the participant answers sentiment questions about their process for creating the Double Pattern. The questions, detailed in figure 4.2, focus on their creation strategy, if they felt the Double Pattern they created provides adequate security, and if it was difficult for them to create a Double Pattern.

Post Creation

1. I feel that the Double Pattern I created provides adequate security for unlocking my personal device. (Likert Scale)
2. It was difficult for me to select a Double Pattern that I would use to unlock my personal device. (Likert Scale)
3. Everyone has a strategy when choosing their authentication, what was your strategy when choosing a Double Pattern?

Figure 4.2: Questions fielded in our survey relating to the creation strategy the participant used when choosing a Double Pattern.

Once pattern creation is completed, we field a set of Simple Usability Scale questions to gauge participant sentiment on the usability of our new system. Within the usability questions, we include an attention question to verify they are paying attention to our survey and not rushing through. If the participant did not select the correct answer for the attention question, we look at the validity of their responses to ensure that we would like to include them in our data.

Participants are asked to recall their Double Pattern. They are given three attempts to do so, before being presented with an option to forego recall because they cannot recall their Double Pattern. After five attempts, they are automatically opted into this and proceed with the survey. The results of this entire process are recorded to analyze how accurately participants can recall their Double Pattern, how many attempts it takes on average, and the timeliness of using this interface.

We include an additional sentiment based set of questions, this time asking for a comparison between Double Patterns and existing knowledge based authenticators, including:

- 4-Digit Personal Identification Number (PIN)
- 6-Digit Personal Identification Number (PIN)
- Android Unlock Patterns (Original Interface)
- Alpha-Numeric Passwords

We also ask if the participant feels that the Double Pattern itself is a secure form of device authentication. These questions are displayed in figure 4.3 and the results are shown in figures XXX.

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.
--

Figure 4.3: Questions fielded in our survey asking the participant to compare familiar authentication methods to Double Pattern.

We present participants with a situation in which they are required to use a Double Pattern to unlock their personal mobile device. We ask if given this situation, would they use the Double Pattern they created in the survey, or would they create a new Double Pattern. Following this, we reiterate to the participant their choice and ask them to explain their decision on why they would, would not, or are unsure if they would utilize the Double Pattern created in the survey. These questions are detailed in figure 4.4.

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 4.4: Questions fielded in our survey gauging the participant's sentiment on real world utilization of the Double Pattern they chose.

We collect standard demographic information based on age, gender, education, as well as information that may influence usability aspects of our interface, such as dominant handedness and involvement in the information technology field. At the end, 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.

4.3 Limitations

One of the primary limitations of our study is the participant base we are collecting our sample from; the participant group may not accurately represent a larger population. The majority of our participants 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 participant base of Android devices, and we would argue

that they likely generalize or, at least, provide an important data point for usability and security for modifications of Double Patterns. The demographics are also inline with prior work on the topic.

Chapter 5

Fielding Our Double Pattern Study

We propose *Double Patterns*, whereby a user selects two patterns, entered in sequence, as their unlock authentication. Drawn on the same 3x3 grid, the user draws their first pattern, lifts, and then draws their second pattern, with both patterns being displayed at the same time. The authentication is based on the combination of patterns, entered in the correct order.

We performed an online user study ($n = 634$) to assess the feasibility of Double Patterns based on its security and usability. From a security framework, Double Patterns greatly increases the complexity of the password space. There are 389,112 possible patterns, and thus, there are $(389112)^2$ possible double patterns, or roughly 151×10^9 (which is far less than 4.3×10^{12} possible 4x4 patterns). And, 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.

An important note about terminology; the term "component pattern" refers to one of the two individual patterns that comprise a Double Pattern. This term may be described as the "first" or "second", to denote in which order it appears in a Double Pattern.

5.1 Initial Iterations of Survey

Prior to fielding the current iteration of our survey, we fielded a preliminary study of $n = 286$ users. Our original survey focused on dividing the participants into treatments based on types of applications in which they would use a Double Pattern to authenticate themselves. Every user would create a Double Pattern for securing their personal mobile device, as well as either a Double Pattern to authenticate themselves with a banking or shopping application on their mobile device. Reviewing the results from this, we felt there were two notable takeaways. The first being, multiple scenarios did not show a discernible difference in user behaviour and sentiment; the users were not primed in a strong enough manner to distinguish the types of patterns produced.

Independent from this, we also discovered that our results seemed very biased towards one specific Double Pattern and one specific first component pattern. We believed that this was due to a visual aid used early in the survey as a demonstration of how to draw a Double Pattern. For these reasons, we decided to shift the focus and implementation of our survey towards only one scenario, mobile device authentication, and we would implement a blacklist based on the top 20 most common Double Patterns and first component patterns from this initial fielding of the survey.

5.2 Design Changes and the Implementation of Blacklisting

One of the changes we made from the previous iteration to the current one, was that we omitted any visual representation of an Android Unlock Pattern or a Double Pattern from the introductory section of our survey. The most utilized Double Pattern was an imitation of our visual example, and appeared in 36/286 of our participants. As well, the most utilized first component pattern stems from this Double Pattern, and appeared in 57/286 of our participants. We decided to implement two types of blacklists on users and study the effects alongside a control treatment. The three treatments were,

- Control Treatment
- Blacklist First Component Pattern (Blacklist First)
- Blacklist Double Pattern (Blacklist Both)

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. Figure 6.1 shows the blacklist rates that occurred in our study.

In the *Blacklist First* 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 Both* 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 start the process from the beginning. With these changes in place, we re-implemented the survey and collected results from 634 users, ensuring there were at least 200 from each treatment.

Chapter 6

Results

Among our three treatment populations we sought to analyze the results of implementing our blacklists. We first examined blacklisting frequency among our treatments as an assurance that a measurable portion of the population had been affected. We performed analysis on measurable security metrics within each population, focusing on aspects such as pattern complexity, pattern frequency, guessing entropy, recall rates, and time cost associated with interface interaction. We also examined qualitative responses to our interface, in the form of Simple Usability Scale questions, sentiments regarding the comparison of our interface to existing methods, and free response questions posed to the participants regarding Double Pattern selection.

6.1 Blacklisting and Ideal Choice

In our Blacklist First treatment, 70/211 (33.2%) users encountered a blacklist after drawing their initial component pattern in their Double Pattern entry. In our Blacklist Both treatment, 19/214 (8.9%) users encountered a blacklist after drawing their initial Double Pattern.

Treatment	Participants Affected	Blacklist Rate
Blacklist First	211	70 (33.2%)
Blacklist Both	214	19 (8.9%)

Treatment	Participants Affected	Change Rate
Control	209	26 (12.4%)
Ideal Choice Blacklist First †	211	97 (46.0%)
Ideal Choice Blacklist Both ‡	214	45 (21.0%)

† Population of Blacklist First including the blacklisted members.
‡ Population of Blacklist Both including the blacklisted members.

Table 6.1: Participant Blacklist Rates and Change Rate of Ideal Choices

Aside from each treatment population, we were equally interested in a cross-treatment population we deemed the "Ideal Choice" group. This collection of patterns consisted of the ideal first choice of each participant: If a participant had drawn a Double Pattern but failed to confirm it, if their first Double Pattern was blacklisted, or if they changed their Double Pattern for any reason, this population contained the first full Double Pattern drawn. Due to the nature of the Blacklist First interface, we excluded those who were affected by this blacklisting treatment. Examining this population, we discovered that 46% of the participants from the Blacklist First treatment and 21% of the participants from the Blacklist Both treatment changed their pattern from their initial choice, based on the blacklist as well as the interface itself. This represents a significant alteration in user choice behaviour from the initial state of the Ideal Pattern set. We sought to examine quantifiable ways to determine if this alteration of behaviour improved the security of the Double Patterns, while not inhibiting the usability and timeliness of the interface.

6.2 Pattern Features Among Treatments

Regarding complexity within a Double Pattern, we looked at the frequency with which the following features appeared in the overall Double Pattern, as well as each component pattern. 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". The features we evaluated were:

- 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

Examining each feature, we used an Anderson-Darling Pairwise Test to determine if treatment populations had a normal distribution in regard to the 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 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 treatment showed significant statistical differences from the other two treatment populations in overall amount of turns ($p < 0.0001$), amount of turns in the first component pattern ($p < 0.0001$), first pattern knight moves ($p < 0.05$), first pattern non-adjacency moves ($p < 0.05$), and total contact point utilization ($p < 0.05$). We conjecture that within the Blacklist First treatment, the high rate of encounters with the blacklist may have motivated the participants to revise their first component pattern by adding more complex features, to overcome the blacklist they initially encountered.

6.3 Pattern Frequency

Only 8.0% of all Double Patterns were utilized twice or more. More striking however, was that in our Blacklist First treatment no Double Pattern occurred more than twice, and these patterns comprised a mere 3.8% of our Double Patterns collected in this set. For comparison, in the Blacklist Both treatment 5.1% of the patterns occurred twice or three times, and in the Control treatment 8.1% of patterns were utilized twice or more. In previous work on Android unlock patterns, Aviv et al. reviewed repetitions in a self-report and pen and paper study of 3x3 patterns [7]. 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. Tables and illustrate the three most frequently occurring Double Patterns within each population, and can be found in the Appendix.

6.4 Partial Guessing Entropy

A known evaluation technique to measure the performance of a guesser is partial guessing entropy [15]. Partial guessing relies on the notion that an attacker will be satisfied guessing a portion of the overall passwords or patterns within a set. In our analysis regarding partial guessing entropy, we examined a throttled attacker who has limited guesses [16]. We examined

1. Min-entropy H_∞ : The probability of the most likely pattern being chosen in the distribution. It is used as a worst-case security metric for human-chosen distributions. This metric is based on Rényi entropy as a distribution tends towards an infinite limit [17].

$$H_\infty = -\lg(p_1)$$

2. $\lambda_\beta(X)$: The β -success-rate measures the expected success for an attacker limited to β guesses per account. This metric was formally defined by Boztaş [18].

$$\lambda_\beta(X) = \sum_{i=1}^{\beta} p_i$$

3. μ_α : Formalized by Pliam [19], this metric is related to the β -success-rate. The α -work-factor evaluates the fixed number of guesses per account needed to break a desired proportion α of accounts.

$$\mu_\alpha(X) = \min \left\{ j \left| \sum_{i=1}^j p_i \geq \alpha \right. \right\}$$

4. $\tilde{G}_\alpha(X)$: The partial guessing entropy is commonly expressed as bits of entropy.

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

We performed a perfect knowledge guessing scenario, where the attacker knows the frequency of every pattern/PIN in the population, and subsequently leverages guesses in that order. The results of the perfect knowledge attacker are detailed in table 6.2. Examining the self reported Android unlock patterns from data collected by Aviv et. al [7], a throttled attacker would be able to guess 29.4% within 20 guesses. When expanding the grid size to 4x4, that percentage drops to 27.5%. Within our Double Pattern populations, the decline in guessability is sharper. A throttled attacker would be able to guess 23.4% of our control population, but when a blacklist is implemented that percentage drops to 15.5% for a blacklist on the entire Double Pattern, and 13.4% for a blacklist on the first component pattern.

	n	H_∞	λ_5	λ_{10}	λ_{20}	μ_{05}	μ_{10}	μ_{20}	$\tilde{G}_{0.5}$	$\tilde{G}_{0.10}$	$\tilde{G}_{0.20}$
Self Reported 3x3 †	440	3.27 [3.26]	12.55% [12.44%]	19.55% [19.62%]	29.42% [29.19%]	2 [2]	4 [4]	11 [11]	3.48 [3.50]	3.76 [3.77]	4.62 [4.64]
4x4 Grid Expansion †	501	3.45 [3.40]	11.51% [11.48%]	18.33% [18.18%]	27.46% [27.27%]	2 [2]	5 [5]	13 [12]	3.58 [3.58]	3.91 [3.96]	4.78 [4.79]
4-Digit PIN †	10000	3.23 [3.26]	13.01% [12.92%]	20.13% [20.10%]	29.63% [29.67%]	2 [2]	4 [4]	11 [10]	3.42 [3.43]	3.70 [3.74]	4.56 [4.53]
6-Digit PIN †	448185	2.16 [2.16]	14.99% [14.83%]	17.46% [17.22%]	22.25% [22.01%]	1 [1]	1 [1]	16 [16]	2.16 [2.16]	2.10 [2.12]	5.22 [5.31]
Control	209	3.73 [3.73]	9.57% [9.57%]	15.31% [15.31%]	23.44% [23.44%]	3 [3]	6 [6]	15 [15]	3.93 [3.93]	4.22 [4.22]	5.12 [5.12]
Blacklist First †	211	4.65 [4.65]	4.78% [4.78%]	8.61% [8.61%]	13.40% [13.40%]	6 [6]	13 [13]	34 [34]	4.76 [4.76]	5.27 [5.27]	6.45 [6.45]
Blacklist Double †	214	4.24 [4.24]	5.74% [5.74%]	10.53% [10.53%]	15.54% [15.79%]	5 [5]	10 [10]	30 [29]	4.56 [4.56]	4.88 [4.88]	6.24 [6.21]
Ideal Choice ‡ *	570	4.11 [4.24]	6.22% [6.22%]	10.72% [10.53%]	16.09% [16.27%]	5 [4]	10 [9]	29 [28]	4.43 [4.40]	4.82 [4.78]	6.18 [6.20]

† Results were down-sampled to the size of the smallest data set, reporting average of 500 randomized runs with medium inset

‡ Ideal Choice Double Patterns are those that were initially selected, without intervention, but perhaps not confirmed either due to a blacklist or memory. These results were also down-sampled to the smallest data set.

Table 6.2: Perfect Knowledge Attacker Guessing Metrics. Detailed above: the number of patterns/PINs contained within the set being attacked.; the minimum entropy of the most frequently occurring member within the set; the β -success-rate at 5, 10, and 15 guesses; the α -work-factor for 5%, 10%, and 20% of the set; the partial guessing entropy measured in bits for 5%, 10%, and 20% of the set.

Self Reported Data [7]				All Related Data [4, 7, 20, 21]			
	μ_{10}	μ_{20}	μ_{50}	μ_{max}	Total Perc.	Guessed	
Control	1054	11261	-	82297	31.10%	Control	85.17%
Blacklist First	18277	-	-	71479	17.54%	Blacklist First	76.30%
Blacklist Both	2845	21124	-	84673	21.96%	Blacklist Both	81.78%
Ideal Choice	3030	23437	-	84673	24.21%	Ideal Choice	78.77%

Table 6.3: Using Simulated Data to Guess in Frequency Order. For our unthrottled guessing, we were interested in the α -work-factor for 10%, 20%, 50%, and the maximum percentage guessed.

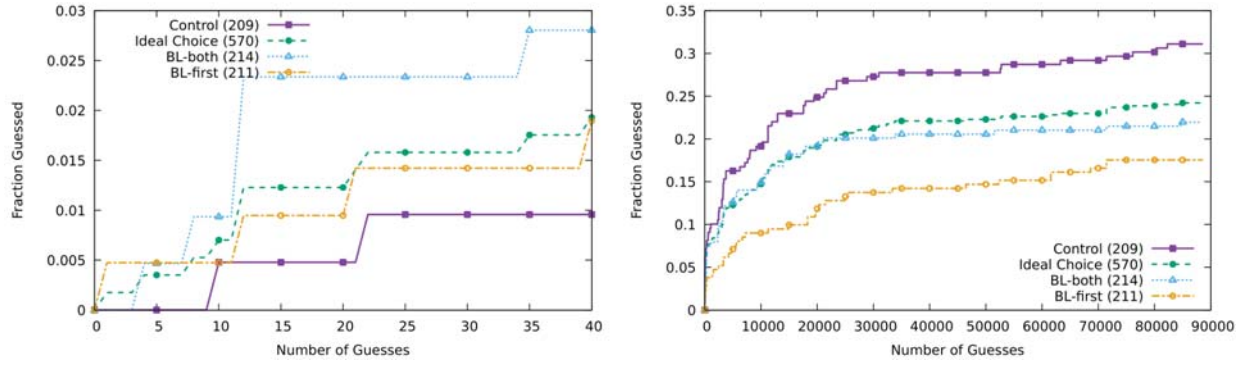


Figure 6.1: Results of throttled and unthrottled guessing using self reported data.

6.5 Simulated Guessing Attack

In a simulated guessing attack, the attacker creates a set of Double Patterns based on the 3x3 patterns from a data set provided. We examined a throttled and an unthrottled scenario in which the attacked guesses in frequency order. We used two collections of publicly available 3x3 patterns from previous studies. For the first attack scenario, the guesser used the self-report 3x3 patterns ($n = 440$ patterns) collected by Aviv et. al [7] to create Double Patterns and leverage guesses against each treatment. The results of using this collection are detailed in figure 6.1. For the second scenario we used a collection of all related data sets we had access to ($n = 4637$ patterns) from related works UDWH [4], ABK-MP-self [7], LDR [1], and ZEBODLAH [21]. The throttled and unthrottled results of this simulated guesser can be found in figure 6.2.

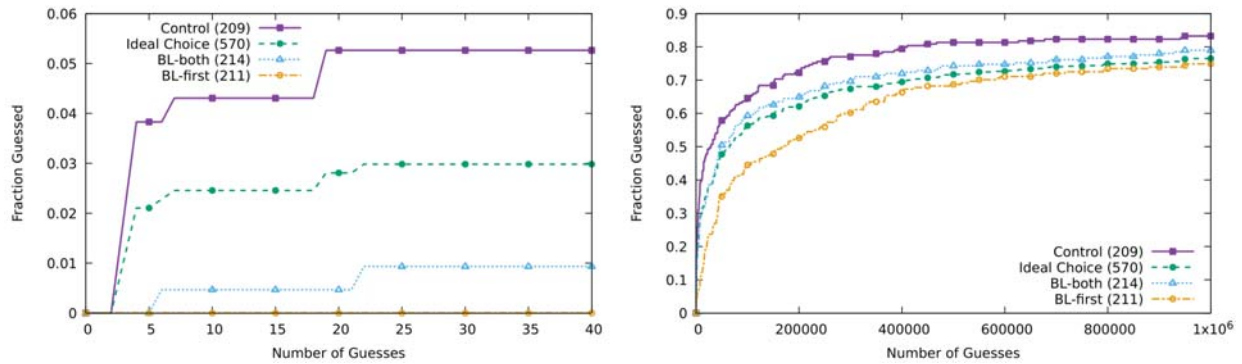


Figure 6.2: Results of throttled and unthrottled guessing using all related pattern data.

6.6 Recall Rates Among Participants

An important metric we examined relating to the usability of our Double Pattern interface was the recall rates among our treatments. We found the rates of recollection across all populations was high: With an overall rate of 96.4% among all participants, the least recalled treatment group

was that of Blacklist First, with a rate of 94.8%. On average, it took participants 1.38 attempts to recall their Double Pattern. For comparison, Uellenbeck et. al reported an average of 1.28 attempts for original Android unlock patterns ($n = 113$), and 1.42 attempts for their interface modifications ($n = 366$) [4]. For a more in depth breakdown of recall rates among each treatment, refer to table 6.4.

	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 6.4: Participant Recall Rates

6.7 Entry Time Using 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 [5]. 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 6.5 shows a more detailed breakdown of time usage for the Double Pattern interface.

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 6.5: Time to Recall Double Pattern

6.8 Usability

To evaluate the usability of our interface, we incorporated a set of Simple Usability Scale questions within our survey. Our measurements ranged from a score of Strongly Disagree[0] to Strongly Agree[4]. The following tables present the number of participants represented in each score, the overall Likert scores, and the individual average sentiment scores for each question, with their corresponding qualitative value. Among all users, the System Usability Scale score was 73.2. This equates to a good, acceptable system, with a passive promoter score.

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

Simple Usability Scale for All Participants vs Established Pattern Users				
	Control	Blacklist First	Blacklist Both	Overall
Number of Participants	209	211	214	624
<i>Established Pattern Users</i>	57	49	56	162
I think that I would like to use this system frequently	2.32 NAND	2.26 NAND	2.30 NAND	2.29 NAND
<i>Established Pattern Users</i>	2.68 Agree	2.90 Agree	2.80 Agree	2.79 Agree
I found the system unnecessarily complex	1.46 Disagree	1.59 NAND	1.31 Disagree	1.45 Disagree
<i>Established Pattern Users</i>	1.25 Disagree	1.12 NAND	1.18 Disagree	1.19 Disagree
I thought the system was easy to use	3.01 Agree	2.84 Agree	3.15 Agree	3.00 Agree
<i>Established Pattern Users</i>	3.25 Agree	3.06 Agree	3.38 Agree	3.23 Agree
I think that I would need the support of a technical person to be able to use this system	0.59 Disagree	0.66 Disagree	0.66 Disagree	0.64 Disagree
<i>Established Pattern Users</i>	0.39 Strongly Disagree	0.78 Disagree	0.70 Disagree	0.61 Disagree
Overall Likert Score	72.99	71.56	75.04	73.21
<i>Established Pattern Users</i>	78.55	77.81	78.39	78.27

NAND: Neither Agree Nor Disagree

Table 6.6: Simple Usability Scale sentiment among participants.

score. Notably, System Usability 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, detailed in tables 6.8 and 6.8. Appendix figures 5 through 8 provide a visual representation of participants' sentiment in terms of the Simple Usability Scale.

6.9 Comparison to Existing Authentication

Within each treatment, participants generally 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. As for participants previously utilizing an Android unlock pattern as their form 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. Table 6.8 displays these averages in more detail. As well, Appendix figures 1 through 4 provide a visual representation of participants' sentiment in terms of comparison to existing authentication methods.

Simple Usability Scale for All Participants vs Established Pattern Users (cont.)				
	Control	Blacklist First	Blacklist Both	Overall
I found the various functions in this system were well integrated	2.88 Agree	2.94 Agree	3.02 Agree	2.95 Agree
<i>Established Pattern Users</i>	3.11 Agree	3.16 Agree	3.16 Agree	3.14 Agree
I thought there was too much inconsistency in this system	0.91 Disagree	0.92 Disagree	0.82 Disagree	0.88 Disagree
<i>Established Pattern Users</i>	0.67 Disagree	0.65 Disagree	0.86 Disagree	0.73 Disagree
I would imagine that most people would learn to use this system very quickly	3.11 Agree	3.25 Agree	3.23 Agree	3.19 Agree
<i>Established Pattern Users</i>	3.21 Agree	3.41 Agree	3.36 Agree	3.32 Agree
I found this system very cumbersome to use	1.24 Disagree	1.38 Disagree	1.16 Disagree	1.26 Disagree
<i>Established Pattern Users</i>	0.67 Disagree	0.78 Disagree	0.88 Disagree	0.77 Disagree
I felt very confident using this system	2.96 Agree	2.81 Agree	3.07 Agree	2.95 Agree
<i>Established Pattern Users</i>	3.21 Agree	3.10 Agree	3.29 Agree	3.20 Agree
I needed to learn a lot of things before I could get going with this system	0.88 Disagree	0.92 Disagree	0.81 Disagree	0.8 Disagree
<i>Established Pattern Users</i>	0.67 Disagree	0.78 Disagree	0.88 Disagree	0.77 Disagree
Overall Likert Score	72.99	71.56	75.04	73.21
<i>Established Pattern Users</i>	78.55	77.81	78.39	78.27

Table 6.7: Simple Usability Scale sentiment among participants.

6.10 Qualitative Analysis of User Feedback

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. This is a strong indication that users already familiar with the interface believe that a Double Pattern would be a more secure and equitably usable form of mobile authentication.

In addition to these qualitative metrics, we also classified and coded participants' feedback in regards to Double Patterns, based on their responses to pattern creation methodology questions and real world utilization of a Double Pattern. We took a cross section of our treatments ($n = 150$) and looked at what motivated them during creating their Double Pattern. Not surprisingly, 88

Device Authentication Comparison Among All Participants vs Established Pattern Users				
	Control	Blacklist First	Blacklist Both	Overall
Number of Participants	209	211	214	624
<i>Number of Pattern Users</i>	<i>57</i>	<i>49</i>	<i>56</i>	<i>162</i>
Double Patterns are a secure way to unlock my personal device	3.02 Agree	3.00 Agree	3.12 Agree	3.05 Agree
<i>Established Pattern Users</i>	<i>3.21</i> <i>Agree</i>	<i>3.24</i> <i>Agree</i>	<i>3.38</i> <i>Agree</i>	<i>3.28</i> <i>Agree</i>
Double Patterns are more secure than 4-digit PIN codes for unlock my personal device	2.78 Agree	2.69 Agree	2.78 Agree	2.75 Agree
<i>Established Pattern Users</i>	<i>2.95</i> <i>Agree</i>	<i>3.10</i> <i>Agree</i>	<i>3.05</i> <i>Agree</i>	<i>3.03</i> <i>Agree</i>
Double Patterns are more secure than 6-digit PIN codes for unlock my personal device	2.33 NAND	2.27 NAND	2.34 NAND	2.31 NAND
<i>Established Pattern Users</i>	<i>2.56</i> <i>Agree</i>	<i>2.63</i> <i>Agree</i>	<i>2.50</i> <i>Agree</i>	<i>2.56</i> <i>Agree</i>
Double Patterns are more secure than alpha-numeric passwords for unlocking my personal device	2.33 NAND	2.27 NAND	2.34 NAND	2.31 NAND
<i>Established Pattern Users</i>	<i>2.56</i> <i>Agree</i>	<i>2.61</i> <i>Agree</i>	<i>2.45</i> <i>NAND</i>	<i>2.54</i> <i>Agree</i>
Double Patterns are more secure than the original Android Patterns for unlocking my personal device	2.33 NAND	2.27 NAND	2.34 NAND	2.31 NAND
<i>Established Pattern Users</i>	<i>3.18</i> <i>Agree</i>	<i>3.29</i> <i>Agree</i>	<i>3.16</i> <i>Agree</i>	<i>3.20</i> <i>Agree</i>

Table 6.8: Of note is our users' evaluation of how Double Pattern compares to existing methods. Below is a comparison of all users in the survey versus established pattern users, and how their sentiments differed on this evaluation.

participants (58.7%) reported utilizing some form of visual stimulus in creating their pattern. These strategies included imitating letters, numbers, simple shapes, and mirroring component patterns. With respect to usability aspects such as memorability and timeliness, 91 participants (60.7%) reported this as a motivating factor in their decision. Table 6.9 reflects participants' responses to the security of the Double Pattern they chose.

Question	Strongly Agree	Agree	NAND	Disagree	Strongly Disagree
I feel that the Double Pattern I created provides adequate security for unlocking my personal device.	40	82	17	9	1
It was difficult for me to select a Double Pattern that I would use to unlock my personal device.	24	24	21	45	35

Table 6.9: Participant Post Creation Sentiment

Chapter 7

Work in Progress

7.1 Multi-functionality of Our Survey

As stated previously, our survey framework has stayed largely the same. The benefit of this is twofold; One being that in cross-treatment comparison, both the research environment and user-base has been consistent among all populations. The other benefit is that as we have refined our Double Pattern study, the framework itself has become increasingly polymorphic in nature, meaning we are able to further explore other aspects of work in the field with ease. One of the most time-consuming aspects of this work is the writing of code to process and extract the collected data, and run analysis on that collection of data. With the completion of Double Pattern collection and analysis, we have the tools to extract and process our collected data with ease.

7.2 Updating the Blacklist for Future Collection

Based on our work with Double Patterns, we believe that there is further work to be done in relation to blacklisting Android unlock patterns. Incorporating aspects of work done by Markert et al. [22], we took the list of most prevalent patterns from the data sets UDWH [4], ABK-MP-self [7], LDR [20], and ZEBodLAH [21], and created multiple blacklisting treatments related to the frequency of occurrence of each pattern. Within our current study, our treatments include:

- Control
- ≥ 32 Occurrences Blacklisted
- ≥ 16 Occurrences Blacklisted
- ≥ 8 Occurrences Blacklisted
- ≥ 4 Occurrences Blacklisted
- ≥ 2 Occurrences Blacklisted

We are currently collecting data and will be continuing work with this study moving forward. We look to compare our results from each blacklisted population to our work with Double Patterns as well as our 4x4 pattern and PIN data.

Chapter 8

Conclusions

To reiterate, our project is focused on the conflict internal to Mobile Authentication between user privacy, security, and the usability of the devices involved. We discussed the widespread use of mobile devices, specifically devices that employ an Android operating system. This allows our work to be properly framed within the research environment of Android Mobile Authentication. Historically, the Android Unlock Pattern interface has not changed since its conception in 2008 [1]. For this reason, many researchers have sought to identify issues with this interface, and proposed their own solutions. Our work continues in this fashion, examining their contributions and seeking to make our own as well.

Using a uniform methodology of collection, we sought to establish continuity across each treatment associated with our new interface. Referring to previous work, we incorporated well-known measures of usability, such as the Simple Usability Scale, and security, such as guessability [7]. We have also included metrics we felt relevant, relating our new interfaces to existing methods of mobile authentication.

Ultimately, we found that the Double Pattern interface showed measurable increases in partial guessing entropy when compared to other forms of authentication such as 3x3 Android unlock patterns, 4x4 patterns, 4-digit PIN's, and 6-digit PIN's. This strength is even more-so with the inclusion of the blacklist on the first component pattern. Arguably just as important to an actual increase in security is the perception of a more secure interface by the user. We believe the Simple Usability, device comparison, and free form response questions are a strong indication that users are open to our new interface. Our results are a strong indication that Double Patterns represent an increase in security while maintaining a high level of usability, when compared to existing methods of authentication.

- [1] Marte Løge, Markus Dürmuth, and Lillian Røstad. On User Choice for Android Unlock Patterns. In *European Workshop on Usable Security*, EuroUSEC '16, Darmstadt, Germany, July 2016. ISOC.
- [2] Harshal Tupsamudre, Sukanya Vaddepalli, and Vijayanand Banahatti. Tinpal-an enhanced interface for pattern locks. 2018.
- [3] Hai Tao and Carlisle Adams. Pass-Go: A Proposal to Improve the Usability of Graphical Passwords. volume 7, pages 273–292. Femto Technology Co. Ltd., September 2008.
- [4] Sebastian Uellenbeck, Markus Dürmuth, Christopher Wolf, and Thorsten Holz. Quantifying the Security of Graphical Passwords: The Case of Android Unlock Patterns. In *ACM Conference on Computer and Communications Security*, CCS '13, pages 161–172, Berlin, Germany, October 2013. ACM.
- [5] Marian Harbach, Emanuel von Zezschwitz, Andreas Fichtner, Alexander De Luca, and Matthew Smith. 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, pages 213–230, Menlo Park, California, USA, July 2014. USENIX.
- [6] Adam J Aviv, Katherine Gibson, Evan Mossop, Matt Blaze, and Jonathan M Smith. Smudge attacks on smartphone touch screens. In *Proceedings of the 2010 Workshop on Offensive Technology*, WOOT'10, 2010.
- [7] Adam J. Aviv, Devon Budzitowski, and Ravi Kuber. 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, pages 301–310, Los Angeles, California, USA, December 2015. ACM.
- [8] Geumhwan Cho, Jun Ho Huh, Junsung Cho, Seongyeol Oh, Youngbae Song, and Hyounghick Kim. SysPal: System-Guided Pattern Locks for Android. In *IEEE Symposium on Security and Privacy*, SP '17, pages 338–356, San Jose, California, USA, May 2017. IEEE.
- [9] Adam J. Aviv, Katherine Gibson, Evan Mossop, Matt Blaze, and Jonathan M. Smith. Smudge Attacks on Smartphone Touch Screens. In *USENIX Workshop on Offensive Technologies*, WOOT '10, pages 1–7, Washington, District of Columbia, USA, August 2010. USENIX.
- [10] Florian Schaub, Ruben Deyhle, and Michael Weber. Password entry usability and shoulder surfing susceptibility on different smartphone platforms. In *Proceedings of the 11th International Conference on Mobile and Ubiquitous Multimedia*, MUM '12, 2012.
- [11] Youngbae Song, Geumhwan Cho, Seongyeol Oh, Hyounghick Kim, and Jun Ho Huh. 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, pages 2343–2352, Seoul, Republic of Korea, April 2015. ACM.

- [12] Chen Sun, Yang Wang, and Jun Zheng. Dissecting pattern unlock: The effect of pattern strength meter on pattern selection. *Journal of Information Security and Applications*, 19(4):308–320, 2014.
- [13] Harshal Tupsamudre, Vijayanand Banahatti, Sachin Lodha, and Ketan Vyas. 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 (ASIACCS 17)*, pages 400–407. ACM, 2017.
- [14] Ashley Colley, Tobias Seitz, Tuomas Lappalainen, Matthias Kranz, and Jonna Häkkinen. Extending the Touchscreen Pattern Lock Mechanism with Duplicated and Temporal Codes. In *Advances in Human-Computer Interaction*, volume 2016, Article ID 8762892, pages 1–11, Munich, Germany, November 2016. Hindawi Publishing Corporation.
- [15] Joseph Bonneau. The science of guessing: analyzing an anonymized corpus of 70 million passwords. In *Proceedings of the 2012 IEEE Symposium on Security and Privacy, SP’12*, pages 538–552, 2012.
- [16] Adam J. Aviv and Markus Dürmuth. A Survey of Collection Methods and Cross-Data Set Comparison of Android Unlock Patterns. volume abs/1811.10548, pages 1–20, November 2018.
- [17] Alfréd Rényi. On measures of entropy and information. In *Proceedings of the Fourth Berkeley Symposium on Mathematical Statistics and Probability, Volume 1: Contributions to the Theory of Statistics*, pages 547–561, Berkeley, Calif., 1961. University of California Press.
- [18] S. Boztas. Entropies, guessing and cryptography. 1999.
- [19] John O. Pliam. On the incomparability of entropy and marginal guesswork in brute-force attacks. In *INDOCRYPT*, 2000.
- [20] Marte Loge, Markus Duermeth, and Lillian Rostad. On user choice for Android unlock patterns. In *1st European Workshop on Usable Security*, 2016.
- [21] Emanuel von Zezschwitz, Malin Eiband, Daniel Buschek, Sasch Oberhuber, Alexander De Luca, Florian Alt, and Heinrich Hussmann. On quantifying the effective password space of grid-based unlock gestures. In *Proceedings of the International Conference on Mobile and Ubiquitous Multimedia, MUM’16*, 2016.
- [22] Philipp Markert, Daniel V. Bailey, Maximilian Golla, Markus Dürmuth, and Adam J. Aviv. This PIN Can Be Easily Guessed: Analyzing the Security of Smartphone Unlock PINs. In *IEEE Symposium on Security and Privacy, SP ’20*, San Francisco, California, USA, May 2020. IEEE.

Appendices

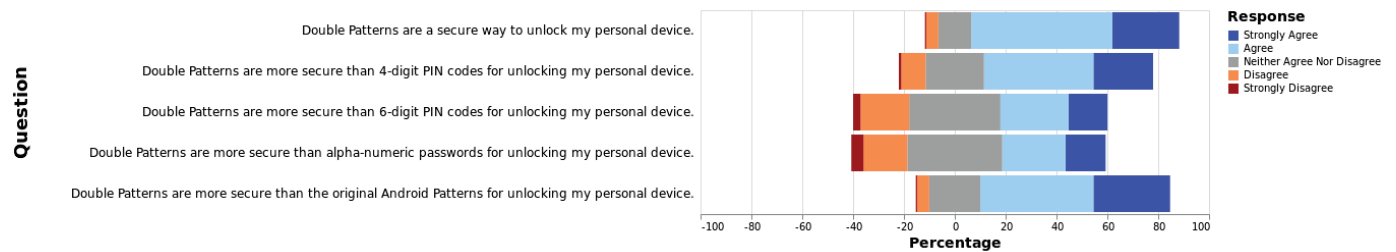


Figure 1: Authentication Method Comparison Scores in the Control Treatment for All Users

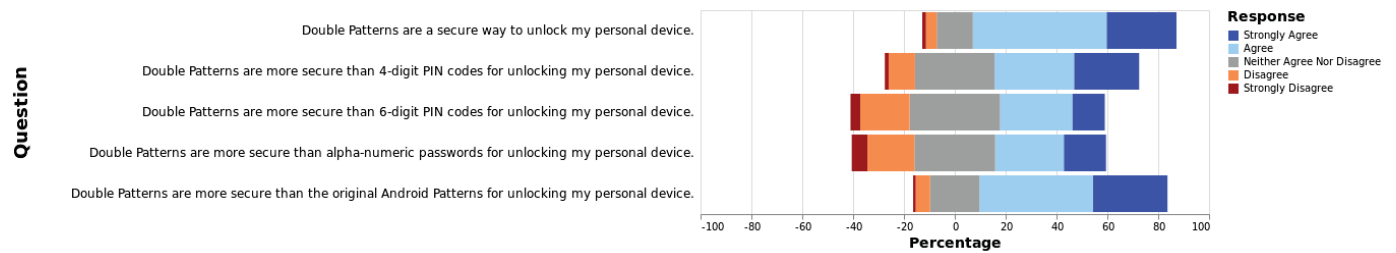


Figure 2: Authentication Method Comparison Scores in the Blacklist First Treatment for All Users

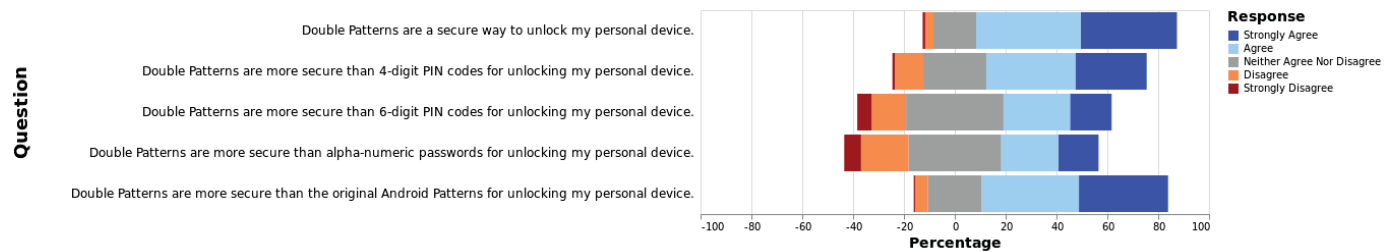


Figure 3: Authentication Method Comparison Scores in the Blacklist Both Treatment for All Users

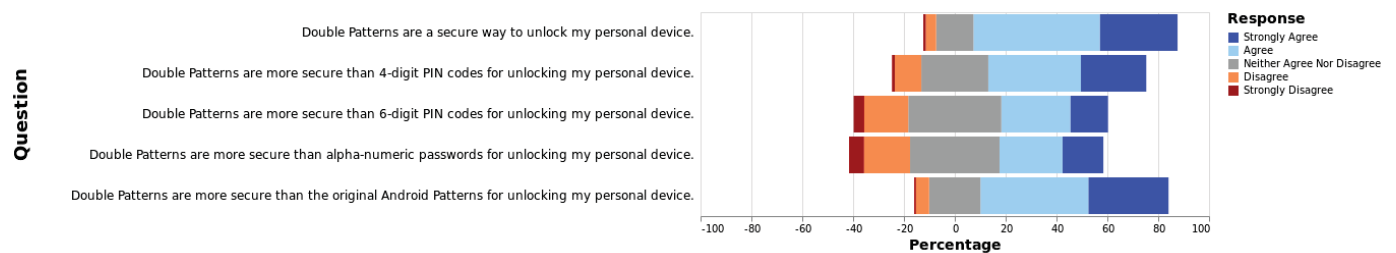


Figure 4: Authentication Method Comparison Scores Across All Treatments for All Users

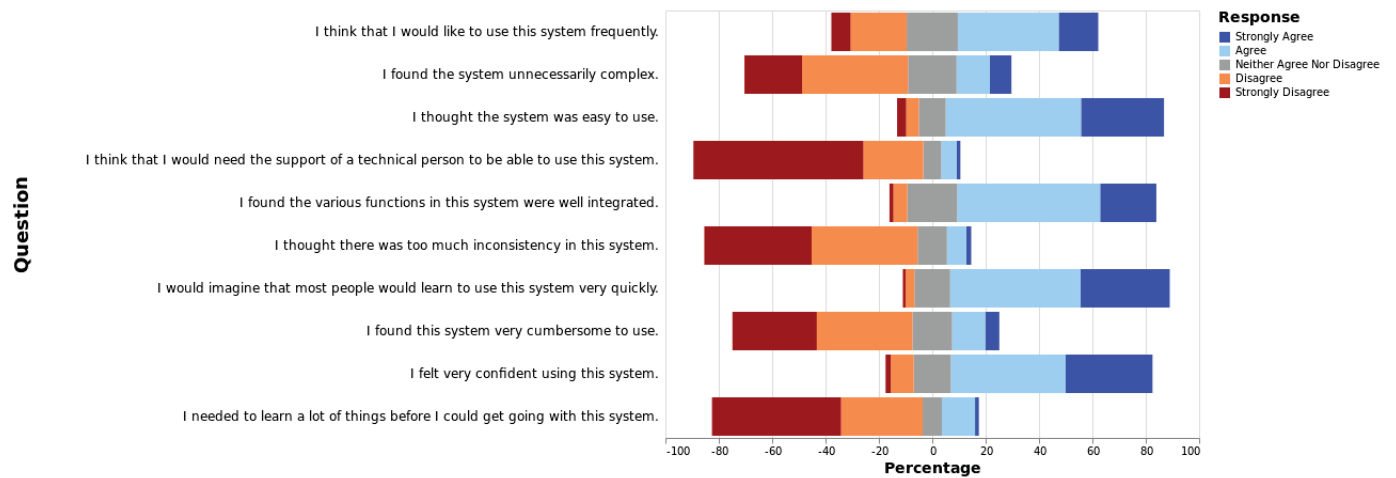


Figure 5: Simple Usability Scale Scores in the Control Treatment for All Users

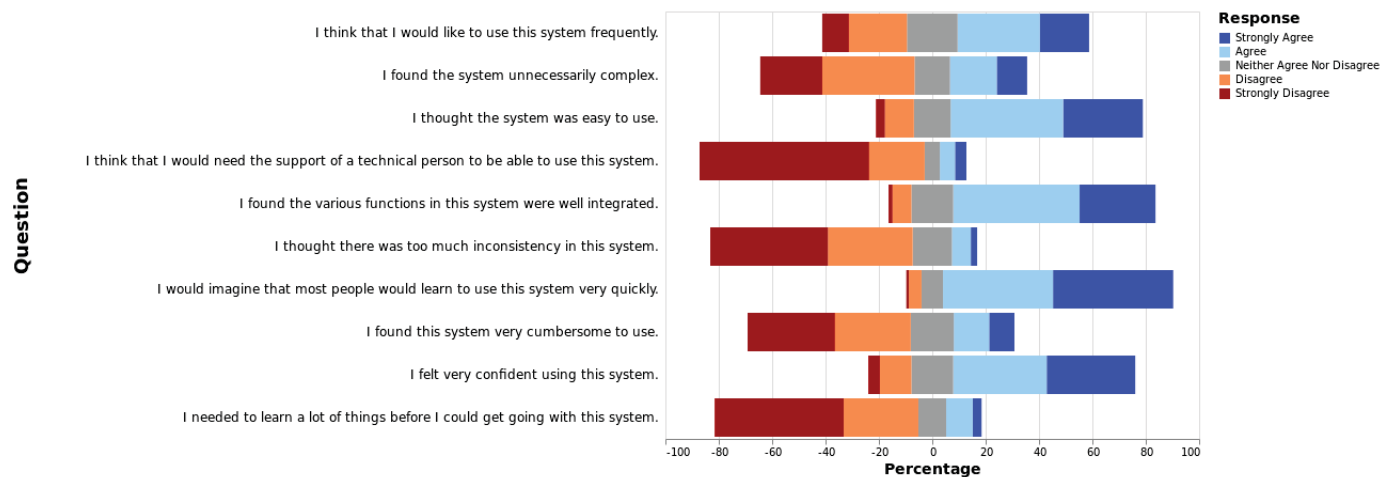


Figure 6: Simple Usability Scale Scores in the Blacklist First Treatment for All Users

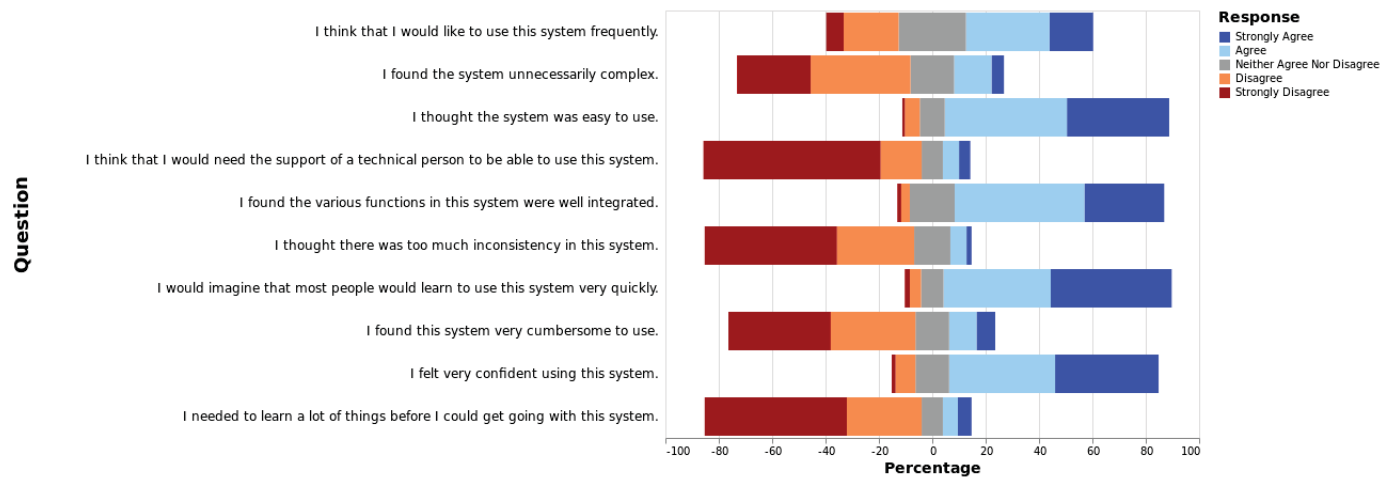


Figure 7: Simple Usability Scale Scores in the Blacklist Both Treatment for All Users

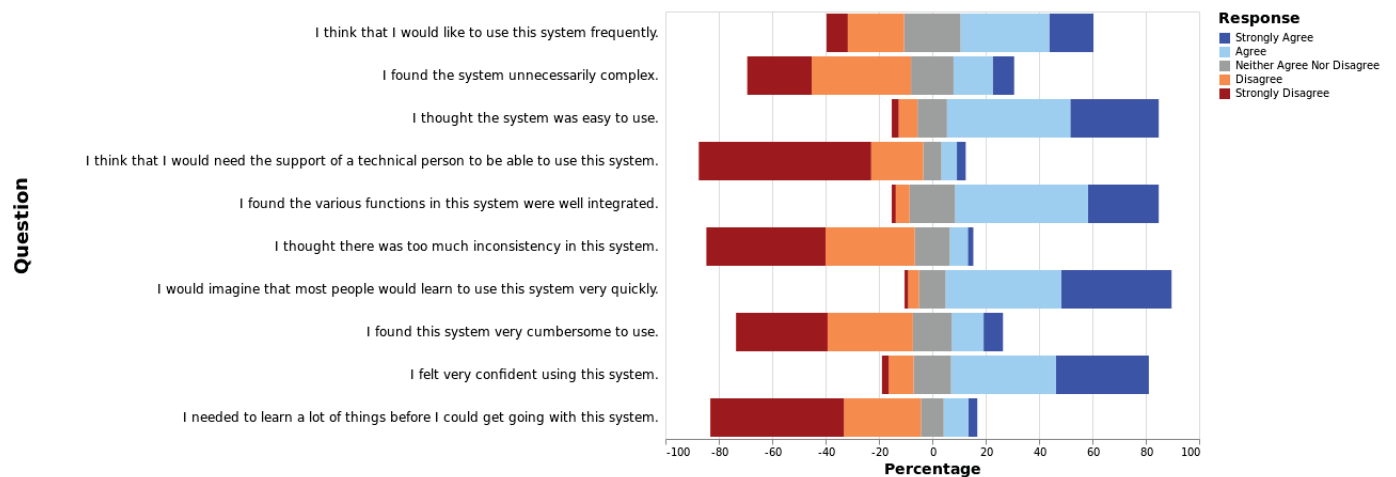


Figure 8: Simple Usability Scale Scores Across All Treatments for All Users

Most Frequent Patterns

Treatment	Survey Results		
	Double Pattern	First Component Pattern	Second Component Pattern
Control	    freq = 5 freq = 4    freq = 3	   freq = 10 freq = 9    freq = 8	    freq = 6 freq = 5   freq = 4
Blacklist First	    freq = 2 <i>Remaining Patterns with Single Occurrence Omitted</i>	    freq = 7 freq = 6 freq = 5	    freq = 2 <i>Remaining Patterns with Single Occurrence Omitted</i>
Blacklist Both	  freq = 3     freq = 2 <i>Remaining Patterns with Single Occurrence Omitted</i>	  freq = 9 freq = 8   freq = 7	    freq = 6 freq = 5 freq = 4

Table 1: Pattern Frequency by Treatment

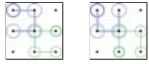
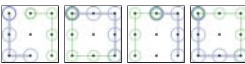
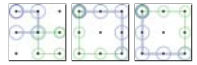
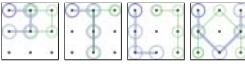
Most Frequent Patterns			
Treatment	Survey Results		
	Double Pattern	First Component Pattern	Second Component Pattern
All	 freq = 7 freq = 5    freq = 4	 freq = 20    freq = 17 freq = 16	 freq = 14   freq = 13 freq = 11
Ideal Choice	 freq = 6  freq = 5  freq = 4	 freq = 21   freq = 18 freq = 17	 freq = 15   freq = 14 freq = 11

Table 2: Pattern Frequency by Treatment (cont.)