ANALYSIS AND STUDY OF USABILITY IN SMARTPHONE AUTHENTICATION

SERIN BAZZI

Bachelor Thesis

January 10th 2020

Rheinische Friedrich-Wilhelms-Universität Bonn
Institute of Computer Science 4
Methods in Multi-Layer Usable Security Research

Analysis and Study of Usability in Smartphone Authentication
Bachelor Thesis

Submitted by Serin Bazzi
Date of submission: January 10th 2020

First examiner/Erstgutachter: Dr. Emanuel von Zezschwitz
Second examiner/Zweitgutachter: Prof. Dr. Matthew Smith
Supervisor/Betreuer: Christian Tiefenau, M. Sc.

Rheinische Friedrich-Wilhelms-Universität Bonn
Institute of Computer Science 4
Methods in Multi-Layer Usable Security Research

ABSTRACT

This thesis represents a complementary research contribution to an ongoing study, which is concerned with improving the usability of smartphone authentication mechanisms. More specifically, the improvement of the perceived efficiency of authentication concepts is of interest. Our goal was to validate and complement the findings and observations made in the ongoing study. We improved its approach by taking into account the limitations which were faced, and by adding further improvements and modifications to it. Based on a proposed dissection of the authentication process, it was observed that a certain part of the process, called orientation, has a significant effect on the perceived efficiency of an authentication concept. Orientation time is defined as the time a user spends preparing themselves to enter a secret, when authenticating. Another crucial part of the authentication process is input, which represents the time period in which a secret is entered. With the help of a specifically developed concept, intended to emulate an authentication concept, we represent certain ratios of orientation and input time. These ratios are then tested and evaluated in a user case study (n=19). Through a specifically designed quantitative and qualitative evaluation, we confirm the findings and observations made in the ongoing study and show that users generally dislike authentication concepts, in which orientation time is not only long, but also exceeds the duration of its corresponding input time. Moreover, the importance of taking the aspect of perceived efficiency into account, when evaluating the usability of an authentication mechanism, as it may deliver more specific and comprehensible information on smartphone users generally perceive and interpret to be efficient.

ZUSAMMENFASSUNG

Kurze Zusammenfassung auf Deutsch

ERKLÄRUNG ZUR BACHELOR-THESIS

Hiermit versichere ich, die vorliegende Bachelor-Thesis ohne Hilfe Dritter nur mit den angegebenen Quellen und Hilfsmitteln angefertigt zu haben. Alle Stellen, die aus Quellen entnommen wurden, sind als solche kenntlich gemacht. Diese Arbeit hat in gleicher oder ähnlicher Form noch keiner Prüfungsbehörde vorgelegen.

Bonn, January 10th 2020

Serin Bazzi

CONTENTS

1 INTRODUCTION

Nowadays, smartphones are approved to be one of the main essentials in people's day to day lives. Besides serving as a medium for essential communication, mobile phones have evolved remarkably, offering advanced features and functions which were formally known to only be possible on a personal computer [7]. Besides storing and granting access to private photos, videos, emails, and social media, smartphones enable their users to do money transfers, online shopping and even track their health through the tips of their fingers [9, 6, 20].

Being the powerful and capable devices that they are, it is said that smartphones have the potential to replace the need for a personal desktop [7]. Hence, they should be capable of protecting their users' sensitive and private data confidentially and securely. The fact that users carry their mobile phone with them wherever they go causes a threat of their device getting lost or even stolen [9]. An American software company, named **Symantec**[1], conducted an experiment, where they purposely "lost" fifty unprotected smartphones in five destinations. The company did so, to observe how the finders of the devices would behave and how they would treat the data stored on these devices. Surprisingly, they found that the data was accessed on 96% of the smartphones and that only half of the finders offered to return the devices [21]. This experiment portrays a security risk that is likely to affect any smartphone user. It is safe to assume that a smaller amount of the data would have been compromised, had the phones been protected by a security mechanism. Therefore, it is evident that securing smartphones with an authentication mechanism is vital for users' data security and privacy.

1.1 THE PURPOSE OF AUTHENTICATION MECHANISMS

The purpose of an *authentication mechanism* is to allow a person access to a particular medium, only after verifying and approving that they indeed are who they claim to be. There are many ways in which this action could take place. In general, an authentication mechanism asks the person, who is requesting access, to enter a secret which only the owner of the medium should know. It serves as a countermeasure to the exploitation of the owner's personal and confidential information. There are many types of authentication mechanisms, and these can be categorised as follows [16]:

- **biometric** - describe "what You are" e.g., fingerprint scanner and facial recognition.
- **knowledge-based** - describe "what You know" e.g., pattern, password, pin.
- **token-based** - describe "what You have" e.g., cryptographic key or chip.

When speaking of authentication in smartphones, there are a couple of well-known mechanisms that come to mind. These can also be categorized as follows [22, 16] :

1 https://www.symantec.com/de/de - last accessed: 2019/11/04

- **alphanumeric** e.g., password and pin
- **gesture-based** e.g., Android Pattern Unlock
- **ID-based** e.g., fingerprint scanner and facial recognition

To this day, researchers have worked on improving smartphone authentication by developing new concepts and designs for them. One might wonder why this is necessary when there is a decent collection of methods already available. Are the current mechanisms not sufficient or secure enough?

The answer to this question is twofold:

On the one hand, specific authentication mechanisms lack in security and are vulnerable towards certain attacks [20]. For instance, Android Pattern Unlock is known to be vulnerable towards so-called **smudge attacks**. These are attacks that occur when the victim draws their secret pattern, leaving an oily trace of their finger on the touch screen. These smudge marks help the attacker to guess the secret pattern, bypass the security measure, and gain access to the device [22]. Another popular attack, which occurs primarily "in the wild" are **shoulder surfing attacks**. These happen when the victim attempts to authenticate themself in public and uncontrolled surroundings. If the attacker is situated in a near distance, behind or beside the victim, they can observe the input of the secret and memorize it for later use [22]. Authentication mechanisms (e.g. pin, password, and Android Pattern Unlock) are prone to such threats, especially when the alphanumeric or graphical secret is short and simple enough to memorize easily. There have been many research contributions that proposed improvements for existing mechanisms as well as the development of new ones to counteract these security threats. Zezschwitz et al. [23] developed an authentication concept called **SwiPIN**, intended to protect pin authentication from shoulder surfing attacks. Another proposal, **TinyLock**, made by Kwon et al. [14], acts against both smudge and shoulder surfing attacks[2].

On the other hand, certain authentication mechanisms still lack in user-friendliness and are therefore not as usable as their developers intend for them to be [20]. As a result, research has shown that many users consciously choose not to use an authentication mechanism on their smartphone [22, 6, 9]. Studies have indicated that one of the main reasons for such behavior is because users perceive screen locks as an inconvenience [6, 22, 13]. Another reason was found to be a lack of knowledge about smartphone security [6, 4]. Researchers discovered that some users decide not to install a screen lock, because they underestimate the risk that comes with not having one and because they do not comprehend to which extent their data is at stake [9]. Through these findings, investigations were made on how to create authentication mechanisms that are not only secure, but also usable.

2 There are many solutions to these attacks other than TinyLock and SwiPIN. In Section 2.2.3, we will only present SwiPIN as an example for all, to not exceed the scope of our thesis.

1.2 THESIS AIM AND OUTLINE

The aim of this thesis is to contribute towards enhancing the usability of smartphone authentication mechanisms. In previous studies, researchers evaluated an authentication concept's usability by solely measuring its *input time*, meaning the time needed to enter a particular secret (e.g. password, pin, pattern) [1]. However, recent research has shown that there are more factors, other than *input time*, that affect the usability of an authentication concept. The most effective factor has been found to be *orientation time* which is the time that a user spends thinking about the input prior to entering it [1]. Zezschwitz et al. [1] made an effort to examine the effect of *orientation* and many other factors more closely by redefining the structure of a general authentication process and by dividing it into multiple phases, including the *orientation* and *input phase*. Through a user case study, they tested the validity of their approach by analyzing three authentication concepts, each representing a different representation (ratio) of the *orientation* and *input phases*. They discovered that the efficiency, more specifically, the perceived efficiency of an authentication concept is crucial for determining how usable it is. Moreover, the perceived efficiency is mostly impacted by the representation of the *orientation phase*.

The aim of this thesis was to complement the findings of Zezschwitz et al. [1] by testing their approach, using a different technique. Instead of testing the different variations of *orientation* and *input time*, by analyzing different concepts, only one concept was used, called **FiPa**, which was specifically developed for the purpose of this thesis. Next, a complementary user case study was conducted with the purpose of proving that *orientation time* truly causes the effects, discovered by Zezschwitz et al. [1].

The thesis will be organized as follows:

Chapter 2 will contextualize the improvement of smartphone authentication in the research field of *Usable Security*, by first discussing their aim and ambitions and then presenting a set of selected related work, which have contributed towards solving the problem of usability in smartphone authentication, using different approaches. Lastly, the main approach of this thesis will be extracted from these findings, by discussing and outweighing their true potential and effect.

Chapter 3 will illustrate the theoretical groundwork of this thesis, which is the approach and the findings of the ongoing study conducted by Zezschwitz et al. [1]. In the end of the chapter, the limitations of their work will be pointed out and balanced by selection improvement proposition which were implemented in the contribution to this thesis.

Chapter 4 will introduce the concept **FiPa**, which was intentionally designed and developed to serve as a tool in the user case study, presented in Chapter 5. The development process involved a series of HCI principles and was constructed to follow the nature of a user-centered design approach, as much as possible.

Chapter 5 will present the user case study, which was conducted to validate the findings, presented in Chapter 3. It thoroughly illustrates the design, procedure and results

of the study.

Chapter 6 will discuss the results of the study, presented in Chapter 5 and will analyze whether the complementary contribution of this thesis truly evaluated the findings of Zezschwitz et al. [1]. Moreover, the chapter will elaborate on the limitations which were faced along the way.

Lastly, Chapter 7 will provide a conclusion regarding the findings from the study in Chapter 5 and will present a set of possible future work propositions, which may help in achieving further progress in the enhancement of usability in smartphone authentication.

2

RELATED WORK AND FOCUS

2.1 CONTEXT

The purpose of this chapter is to fill the gap of knowledge on the research field of **Usable Security** by explaining its aim and by portraying the steps that researchers are taking to increase usability in smartphone security, in general. In addition, a selection of approaches and scientific contributions will be presented to lay the groundwork for main approach of this thesis.

2.1.1 *Improving Usability in Smartphone Authentication*

As mentioned earlier, security, alone, is not sufficient enough to guarantee the success of an authentication mechanism. A lack of usability in security mechanisms defeats their purpose, no matter how secure they are in theory. **Usable security** is a growing, and widely popular research field whose aim is to create a balance between **usability** and **security** in security systems and mechanisms and thereby make them more suitable for human use. [18, 1]. In order to better understand their ambitions, we will first give an understanding of what usability is.

Usability generally describes the degree to which a user can accomplish a certain task with *"effectiveness, efficiency, and satisfaction"* when utilizing a certain product.[1] This definition applies to all designed and developed products imaginable, including security mechanisms. The goal of usable security experts is to construct the design process of security measures similar to the design process of any product intended for human use. In other words, security designers implement a **User-Centered Design** (UCD) approach when designing security mechanisms which allows them to involve certain *human factor principles*, crucial to their success [4, 19, 8]. Another important research field that collides with **Usable Security** is **Human-Computer Interaction** (HCI). Researchers in HCI thoroughly analyze the physical and cognitive abilities of human beings which helps designers and developers create systems and technologies that appear common and familiar to humans and that enable natural and intuitive interaction [8]. The collaboration of these research fields contributes towards developing systems and mechanisms that are secure and, most importantly, usable.

As mentioned in the introduction of this thesis (see Chapter 1, despite current achievements regarding system security, the usability of authentication mechanisms still remains a conundrum that has not yet been solved. While users have found it hard to comply with required security guidelines and have, therefore, behaved insecurely [4, 19], security experts have perceived users as *"the weakest link in the chain of system security"* [19] and have found that they are *"a security risk that needs to be controlled and managed"* [4]. Hackers have noticed the flaws of current security systems and are able can foresee how users

1 https://www.interaction-design.org/literature/topics/usability - Last accessed: 2019/11/10

will behave. By using certain attacks or procedures such as *social engineering* they are able to steer individuals into sharing their authentication secrets and personal information [4, 19]. Users, however, are not entirely at fault for this issue. The reason why hackers have been able to attain unauthorized access to systems so easily is because they have been more attentive to users' perception of security than security designers were [4].

It is natural for humans to try and find shortcuts and time-saving methods when it comes to challenging tasks [19]. This behavior also applies when using security mechanisms which demand actions that are either impossible or unnatural to follow [19]. For instance, when using a password-protected system, some requirements are to use an alphanumerical secret that is at least eight characters long, consists of lower and upper case letters as well as special characters [17, 19]. Moreover, passwords are required to be changed regularly [3, 16]. These regulations might be possible to comply with when a user only has one password to memorize. However, nowadays, users have to manage a multitude of passwords, which makes following the guidelines more tiresome and difficult. To that end, users are bound to seek for a solution that helps them bypass security measures in order to work on the task which they initially intended to achieve.

Experts in *human factors* differentiate between two types of tasks: *productive tasks* and *supportive tasks*. *Productive tasks* are the activities needed to accomplish a certain goal or to reach a certain outcome. They fulfill the purpose of a system's existence [19]. **Supportive tasks** are ones intended to help productive tasks in being executed efficiently and permanently [19]. According to Sasse et al. [19], security mechanisms are considered to be supporting tasks. However, the issue is that oftentimes the requirements of current security mechanisms are not coherent with the demands and needs of the task which they support. In turn, the efficiency of a productive task is reduced due to the delay of its accomplishment. Therefore, users are involuntarily put in a position to choose between which task to prioritize. Since the production task generally is their initial goal, they find themselves looking for ways to bypass or neglect the supporting task, namely security mechanism.

In order to protect users from making insecure decisions that put their identity and privacy at stake, have made the effort to find out the true triggers that negatively affect the usability of security mechanisms and how to improve them. Thus the main focus of this thesis is the usability of smartphone authentication, we will be presenting certain approaches and suggestions made in that field, in the following section.

2.2 RELATED WORK

In general, when solving the matter of usability in security mechanisms, we cannot expect to find a sole solution that will solve all problems. Usability is a very complex and broad subject, and there is a wide range of factors that have been found to play a role in increasing or decreasing it [1, 13, 6, 11]. In order to give well-structured insight on the recent findings, we will group them according to their focus. Thereby the following research questions will be of interest:

- *What are the factors that affect usability in smartphones authentication?*
- *Why do many smartphone users behave insecurely and how can we change it?*

- *How can we compare multiple authentication mechanisms based on their usability and how can we evaluate them accordingly?*

2.2.1 *Users' Security Behavior and Perception*

In the recent years, researchers have made an effort to find the reason for smartphone users' insecure behavior by observing their perception of security. For instance, Harbach et al. [13], were interested in finding out how users behaved in real-life scenarios regarding unlocking their smartphones and how they perceived smartphone security, in general. They were also interested in discovering how much time the act of unlocking took up from their overall smartphone usage. For that, they conducted an online survey that yielded 260 participants to obtain qualitative data on users' perception of smartphone authentication. They also conducted a field study that lasted one month and yielded 57 participants to examine users' authentic behavior towards smartphone security. They found that, on average, participants turned on their smartphone 83.3 times and authenticated 47.8 times. These numbers implied an average of 5.2 screen switch-ons and 3 authentications per hour. The number of screen switch-ons and unlocks was underpredicted by 36 participants by an estimated 141%. Harbach et al. [13] also found that the necessity of smartphone security was perceived as environment-dependent, meaning it was rated as redundant in trusted environments.

Furthermore, Harbach et al. [13] discovered that when participants used their smartphone, sensitive data was only accessed ca. 25% of the time, which means that about 75% of the overall smartphone interaction, did not include any data or action in need for security. On that note, Harbach et al. [13] suggested that by minimizing the amount of daily smartphone unlocks, the practice of smartphone security would require less effort and thereby be much more manageable for users. They imagined to implement this solution by applying security measures solely to the applications and features that require access to sensitive data. Furthermore, Harbach et al. [13] identified that users take different measures other than authentication mechanisms to protect their phones, such as not leaving their phones unsupervised in public. Consequently, by taking such measures, users consider that their device is protected and, therefore, no longer feel the need to install a security mechanism.

In 2016, Harbach et al. [12] conducted an international study in which over 8000 participants were surveyed on their smartphone security behavior. The purpose of this research was to examine whether history and culture dictated users' security behavior. In total, participants were surveyed in eight countries: Japan, Germany, Italy, the Netherlands, the UK, Australia, Canada, and the US. Harbach et al. [12] noticed a difference between the countries when they examined the likelihood of participants adopting a screen lock for their smartphone. They found that up to 76% of the non-American participants were more likely to secure their phones with a security mechanism than Americans participants. They also found that security behavior varied in terms of their participants' age. It was more probable for younger users to install a screen lock than elder ones.

Furthermore, Harbach et al. [12] analyzed the reason why some of their study participants did not use a screen lock on their smartphone. They found the primary reason to

be "inconvenience" [12]. This reason was mostly given by participants from non-English speaking countries who also justified their choice by stating that security mechanisms were not useful because they were not secure enough to protect their phones. Moreover, a large number of their participants mentioned an "absence of threat" [12] to be a reason for not having a screen lock. Harbach et al. [12] also observed that participants from Germany were 4.5 times more probable to acknowledge the importance of protection than the other participants. Overall European participants have shown to be more conscious about their smartphone security, which implied awakening the awareness of smartphone users towards existing security threats to be more effective in Europe. Through this research, Harbach et al. [12] has shown that smartphone security has to be improved and managed according to a country's culture and its people's needs. That way, authentication mechanisms could be developed or improved to match a country's most common threats and its people's perception of security [12].

Based on the findings introduced above, which focused on examining smartphone users' perception of security, Alsaleh et al. [7] made an effort to search for behavioral patterns in smartphone users regarding their security practices and their awareness thereof, by conducting 30 interviews. Their results have shown that the majority of participants that did not use a screen lock also did not practice a data back-up on their smartphone. These participants were found more likely to accept a Wi-Fi connection from public hotspots. Alsaleh et al. [7] also validated a previously introduced finding by Harbach et al. [12], which stated that younger users behave more security conscious towards their smartphones than elder users do. Based on related and personal findings, Alsaleh et al. [7] proposed a list of improvement suggestions for developers and designers to include and regard in their applications and platforms. They encouraged security experts not to rely the security of smartphones on users only.

Analogous to Harbach et al. [13], they suggested reducing the number of security-related decisions that users have to make, by requiring security measures in situations in which they are truly needed. In addition to that, they recommended that developers created unique "indicators" [7], which inform the user whether a particular smartphone application is safe or unsafe to use. Another recommendation was to increase security procedures in smartphone platforms. They suggested that an application upload could only be permitted once the developer included certain security features in their application, which ensure that the application is safe and that users' data will not be exploited. Furthermore, they added that through particular "social triggers" [7], it could be possible to attract users to adapt to security practices. An example was to make smartphone users witness a known person execute ideal security behaviors.

Similar to Alsaleh et al. [7], Albayram et al. [6] also made the realization that by using certain social communication methods, one could be able to motivate users to be more security conscious with their smartphone. They noticed that one of the prominent reasons why users take smartphone security for granted or why they do not practice it correctly, was due to a lack of awareness of the risks and threats that might consequently occur. Albayram et al. [6] proposed a method of intervention by creating a video that explained what consequences resulted from not using an authentication mechanism. It also included an instruction on how to install a screen lock on an Android smartphone. This method

was applied in a survey where participants were divided into two groups: a *control group* and a *treatment group*. Albayram et al.'s [6] intention was to construct the survey similarly for both groups. The only difference would be that the video would only be shown to the *treatment group*. When participants were asked why they did not use screen locks for their smartphone, the primary reason was that they found them "inconvenient" and "time-consuming" [6]. A similar observation to Harbach et al. [13], was that participants did not find that their phone were at risk since they kept it with them at all times [6]. Also, some participants stated that they had "nothing to hide" and, therefore, did not see the necessity of installing a screen lock.

A week after the survey, Albayram et al. [6] conducted a follow-up survey, in order to observe the effect that the educational video had on the *treatment group* and to see whether it influenced them to adopt security habits on their smartphone. They found that 50% of the participants that watched the video had installed a screen lock after the first study. However, in the *control group*, only 21% of the participants improved their smartphone security behavior. In this way, Albayram et al. [6] proved that by informing smartphone users about the urgency and importance of security mechanisms and by changing their perception on security, one could motivate more users to adapt to using a screen lock regardless of its usability.

2.2.2 *Analysis of Existing Smartphone Security Mechanisms*

Researchers have made an effort to compare existing authentication mechanisms to find out which ones smartphone users perceive as more usable. A research paper by Zezschwitz et al. [25], published in 2013, presented a study in which two popular security mechanisms (*pattern* and *pin*) were tested by participants for 21 days to examine which of both they preferred. The study included a qualitative as well as a quantitative evaluation of both mechanisms. Quantitatively, Zezschwitz et al. [25] discovered that *pin* had a much shorter authentication duration than *pattern*. Moreover, *pin* had a prominently lower error rate than *pattern*. However, in the qualitative evaluation, participants expressed a higher preference for *pattern*. Reasons were an "ease-of-use, better feedback, and likeability" [25]. Zezschwitz et al. [25] also asked participants to rate the error recovery in both mechanisms. The majority found that *pattern* handled errors better than *pin*.

A one-month long field study was done by Harbach et al. [11], which compared popular unlocking mechanisms to each other. Also, certain behavioral patterns were observed. In terms of users' behavior, Harbach et al. [11] found that when users used a *pin* mechanism, they tended to utilize their phone less often during the day. *Slide-to-unlock* users used their smartphone more often than *pin* users but for shorter periods. They also needed less time to unlock their phone. The case was similar for *pattern* users. They also utilized their phone more frequently than *pin* users, yet for shorter intervals. In terms of unlocking, the duration of *pin* and *pattern* authentication was the same. However, analogous to Zezschwitz et al. [25], participants encountered a higher amount of errors with *pattern* than with *pin*. Moreover, they found that *pin* users needed double the time that *pattern* users needed to prepare themselves for the authentication. Harbach et al. [11] assumed that *pin* users spent this time recalling their input. Also, Harbach et al. [11] discovered that most of the participants were not in favor of using a particular security

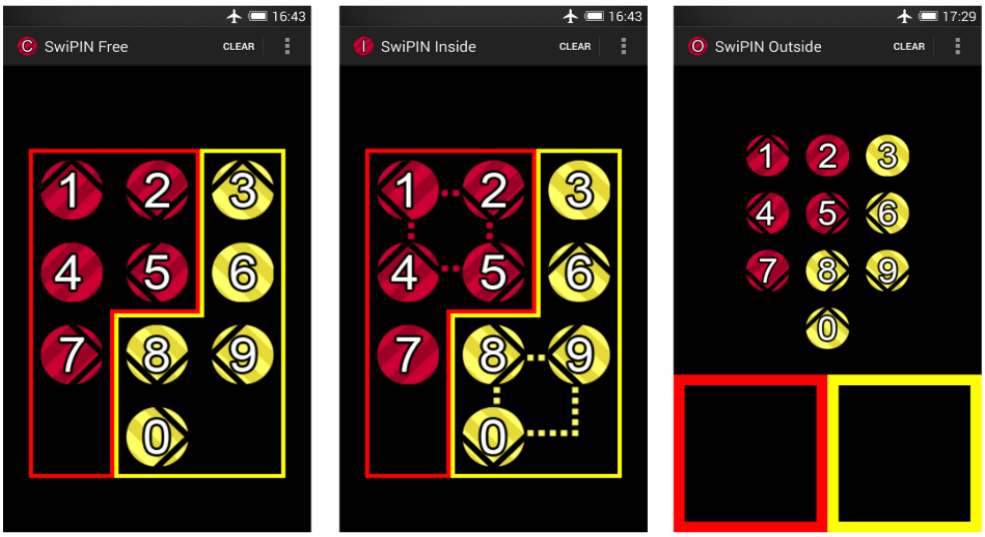


Figure 2.1: The three variations of **SwiPIN** by Zezschwitz et al. [24]. The version that was proven to be most usable is **SwiPIN** *(outside)* on the far right [24].

mechanism, even if it were more secure than others. However, they were in favor of using one, if it allowed a fast performance [11, 6].

2.2.3 *Approaches towards Novel Authentication Concepts*

In addition to the previously discussed findings, researchers have also contributed towards proposing novel authentication methods. Although their intentions were primarily directed towards solving certain security issues, such as *smudge* and *shoulder surfing attacks* (see Chapter 1), some of the authentication concepts have the potential of being more usable than the existing ones.

Zezschwitz et al. [24] created an authentication mechanism called **SwiPIN** (see Figure 2.1). It was intended to support the original *pin* method in situations in which stronger authentication security is needed. Its main task was to prevent *shoulder surfing attacks*. Zezschwitz et al [24] created three variations of the concept, of which **SwiPIN** *(outside)* showed to have the best usability (see Figure 2.1). It is comprised of entering the pin through gestures rather than by tapping the buttons (numbers) on the screen. The interface presents a number pad, and on each of the buttons, there is a black arrow, which indicates the direction in which the gestures should be performed. Also, for each button, a specific color is assigned (*yellow* or *red*). To enter one's pin, one would simply perform the gestures of the respective numbers in one of two "boxes" displayed at the bottom of the screen. Gestures of red buttons are performed in the red box and gestures of yellow buttons, in the yellow box (see Figure 2.1). The black arrows, which are assigned to each number, change for each authentication run. This design increases the effort and memory needed to "successfully" perform a shoulder surfing attack because the attacker must try to memorize the gestures, their order, and the color of the boxes in which they are performed in order to obtain which numbers were entered.

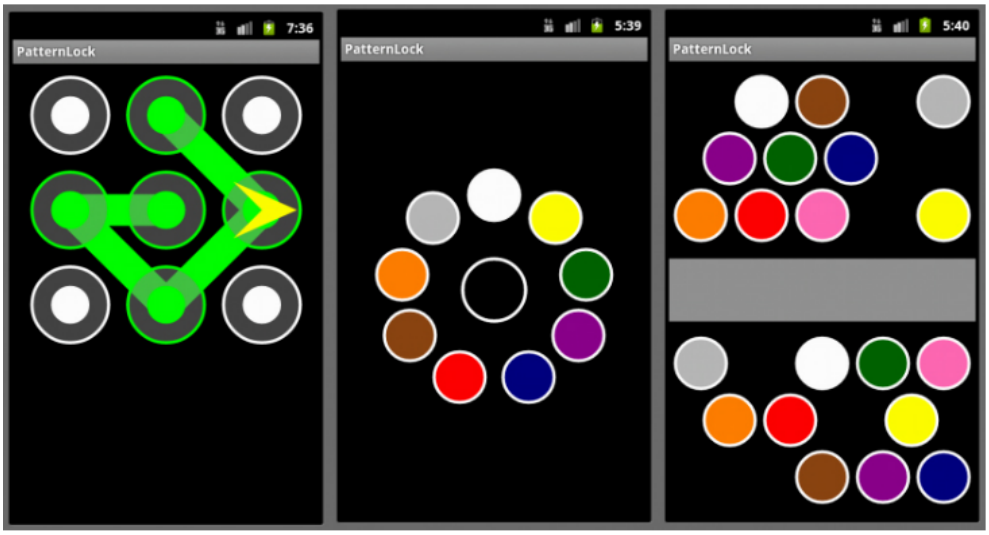


Figure 2.2: The three concepts made by Zezschwitz et al. [26]. (Left) Pattern 90, a special version of Pattern Rotation, (Middle) Marbles, (Right) Marble Gap, a variation of Marbles.

Zezschwitz et al. [24] further conducted a study in which **SwiPIN** and the original *pin* concept where compared to each other. They noticed that the utilization of **SwiPIN** lead to a slightly longer authentication process than *pin*. A notable disadvantage of the concept **SwiPIN** was that users had to approach it differently than usual. Since entering a memorized pin into a number pad usually depends on muscle memory, users had to consciously recall their pin, while using **SwiPIN**. This lead to an increase of mental effort during utilization. Nonetheless, all participants of the study approved of the concept and imagined themselves using it in unsafe environments.

Another contribution towards designing novel security concepts was made by Zezschwitz et al. [26]. Their goal was to create a protection mechanism against *smudge attacks*. They created three concepts: **Marbles**, **Marble Gap** and **Pattern Rotation** (see Figure 2.2). The idea for **Marbles** is to create an interface that presents colored dots (marbles) aligned in a circular order. The marbles represent the elements that define a specific password. In order to authenticate, the user would enter their password by dragging the marbles into the center circle in the right order. **Marble Gap** is based on the same idea, yet differs in its mapping (see Figure 2.2). The marbles are displayed at the top and bottom of the screen, separated by a centered rectangle (gap). To enter the password, the user would drag in the marbles into the gap, either from the top or bottom. It is important to note that the arrangement and display of the marbles were random for each authentication run in both concepts. **Pattern Rotation** is based on the traditional *Android Pattern Unlock* mechanism. The interface presents a 3x3 grid of nodes, which changes its orientation every time a user wants to authenticate. A special version of **Pattern Rotation**, namely *Pattern 90*, enables four different grid orientations: 90°, 180°, 270°, and 360° (see Figure 2.2).

To examine which one of the three concepts users' preferred best in terms of efficiency and effectiveness, Zezschwitz et al. [26] conducted a study in which all three concepts were analyzed. They adopted a specific approach to measure the authentication times by

dissecting the authentication process into *orientation* and *input* time. Harbach et al. [11] made a similar approach when they analyzed the difference between *pin* and *pattern* (see Section 2.2.2). Zezschwitz et al. [26] defined the *orientation* time as the period between the initiation of the authentication and the first input event, made by the user. *Input* time was interpreted as the period between the first input event and the moment in which the input is either approved or rejected. Through this distinction, they realized that the factor of randomization in each of the concepts affected their overall authentication time in different ways. For instance, with **Marbles** and **Marble Gap**, randomization was shown to elongate the *input time*, because the marbles were positioned differently in every authentication run, and so the user had to search for each marble before entering it. In contrast, the *orientation time* of **Pattern Rotation** was increased through randomization because participants needed more time to familiarize themselves with the current position of the grid. Another discovery made, through the distinction of *orientation* and *input*, was participants' perception of speed. While **Pattern Rotation** was measured to be the second quickest of all three, participants rated it as the slowest. Nonetheless, **Pattern Rotation** had the longest measured *orientation time*. This discovery allowed Zezschwitz et al. [26] to realize that users disliked mechanisms which had long *orientation times*. Therefore, **Pattern Rotation** was considered not usable. Security analysis also showed that it was not sufficiently secure. In contrast, participants approved of **Marbles** and **Marbles Gap** and perceived them as very usable.

2.3 FOCUS

In retrospect, the previously presented research contributions underline how crucial efficiency and effectiveness are for the user-acceptance of a particular authentication mechanism. Yet, the question remains, which of the two has the potential to achieve more successful and desired results, when enhanced. The following section will justify the author's choice of focus by elaborating on the potential effect of each factor, based on the related work (see Section 2.2).

Many instructive propositions were made towards improving effectiveness, from using social intervention methods, to specifically adapting the maintenance of smartphone security to users' country of origin (see Section 2.2.1). Although these propositions have a potential to cause improvement in usability, they are either only successful to a certain extent, or complicated to implement. For instance, when Albayram et al. [6] used an educational video as a method of intervention, it was effective, yet the desired effect was only noticeable in 50% of their treatment group. The other half of the group still persisted on not to use a screen lock on their smartphone. In addition, in order to implement the proposition made by Harbach et al. [12], one would need to study each country to specifically design smartphone authentication methods that satisfy the wants and needs of smartphone users around the world. This approach does not only require much time and many resources, yet it also is difficult to implement thus, realistically, all people differ in their wants and needs, despite their country of origin. So, it would be strenuous to create a smartphone authentication method that satisfies the majority of the people of a particular country.

On the contrary, people are similar in their instinctive behaviour. As mentioned in Section 2.1.1, humans are naturally prone to facilitate certain tasks or actions that appear complicated or unnatural to them, which is the case with current authentication methods. This implies that humans instinctively favor tasks and actions that are fast and easy to perform, and that are, therefore, efficient. Findings in Section 2.2, described that the primary reason why users persist to not use screen locks is because they perceive them as *inconvenient*. Another study revealed that users prefer to use a screen lock if it delivers a faster performance than the existing ones. On that note, laying focus on increasing the efficiency of authentication mechanisms could be more productive towards the improvement of their usability.

However, the creation of authentication concepts that are fast and easy to use is not as intuitive as it seems. As Zezschwitz et al. [25] compared two commonly used authentication mechanisms, *pin* and *pattern*, they noticed that their participants preferred using *pattern* more than *pin*. Reason being, that *pattern* handled errors better than *pin* did, and that it needed less time for preparation. Nonetheless, time measurements showed that with *pattern* participants needed more time to authenticate than with *pin*. This implies that only focusing on time measurements to evaluate efficiency could lead to making false conclusions [1]. Instead, human perception of time and speed should be used as the metric to do so. For that, research should be directed more specifically towards enhancing *perceived efficiency*. For that, specific methods of approach are called for to observe the factors that affect the human perception of efficiency.

On that note, Zezschwitz et al. [26] compared newly developed authentication concepts by using a specific manner of approach. In noticing that preparation time played a role in the perceived efficiency of authentication mechanisms, they dissected the overall authentication time into *orientation* and *input* (see Section 2.2.3). Consequently they noticed that the concept which had the second shortest overall authentication time, was perceived least usable. The outcome was due to the concept's long *orientation time*. Participants seemed to dislike this aspect of the authentication concept.
This observation arises the question on whether the length of *orientation time* has an effect on the perceived efficiency of an authentication mechanism or not. An ongoing work at Rheinische Friedrich-Wilhelms-Universität, by Dr. Emanuel von Zezschwitz and Christian Tiefenau (M.Sc.), is directed towards answering this question. They proposed an extended method on improving perceived efficiency of authentication mechanisms by redefining the anatomy of a general authentication process. In Chapter 3, their work will be discussed in detail, thus it serves as the theoretical groundwork of this thesis. Lastly, it is important to note that although, in this section, efficiency was shown to outweigh effectiveness, based on the findings in Section 2.2, the solutions for enhancing effectiveness in authentication still remain important and useful and could be implemented as supportive solutions to further enhance usability in efficient authentication mechanisms.

3

THEORETICAL FOUNDATION AND HYPOTHESES

The following chapter presents an ongoing scientific work of *Methods in Multi-Layer Usable Security Research* group at Rheinischische Friedrich-Wilhelms-Universität Bonn. It will serve as the theoretical core of this thesis. The The scientific paper goes by the title

"Designing Efficient Authentication Mechanisms: There is More to Efficiency than Input Speed."

and the researchers who have contributed to it are Dr. Emanuel von Zezschwitz and Christian Tiefenau (M.Sc.). Throughout this thesis they will be referred to as Zezschwitz et al. [1]. In the first section of this chapter the findings of this work will be presented. In the second section, the limitations of their approach will elaborated and discussed. The last section will illustrate how the author of this thesis intends to validate their findings by reevaluating their approach and proving their hypotheses.

3.1 APPROACH

As mentioned in Section 2.3, researchers have tried to detect the factors that most affected the efficiency of smartphone security. They realized that these factors could not be assessed by simply measuring the duration of authentication processes. Also, they discovered a factor that had often been disregarded during the evaluation of efficiency, and that is *orientation time* (see Section 2.2). The amount preparation and mental effort that is needed to accomplish an authentication task is found to be crucial for user-acceptance [1]. Therefore, new measurement methods are in need which approach the practice of authentication on a human level and which are designed with respect to humans' perception of time and their cognitive abilities.

To that, Zezschwitz et al. [1] made an effort of examining a specific measurement method to better evaluate the usability of authentication mechanisms in terms of their perceived efficiency [1]. They noticed how previous studies indicated that users commonly prefer authentication mechanisms that require little to no mental effort [1, 11]. So, they redefined the architecture of a general authentication process in order to detect the triggers that make authentication exhaustive and inconvenient to users. When found, Zezschwitz et al. [1] propose that their approach could be considered a prime step towards setting a standard for measuring usability in authentication mechanisms. Moreover, they suggest that their approach could help preventing the formation of false conclusions, in regard the usability aspect of authentication mechanisms, especially when they are evaluated or compared to each other.

The following list describes the phases that defince the structure of an authentication process, according to Zezschwitz et al. [1] (see Figure 3.1):

- **Orientation:** In previous research, this phase was commonly defined as the *preparation* phase . It defines the period, beginning from the moment when a smartphone

Figure 3.1: Component phases of an authentication process. While Orientation and Active Authentication (input) phase are the core components of an authentication procedure, Error Recovery may also be included. Clean up phases are not considered part of the authentication process, yet in some designs they are crucial for its completeness [1].

screen is switched on, to the moment when the first input action is made . It usually takes place before the user enters their secret. It is the time which they spend either recalling their secret, preparing themselves for its input, or both . Also, it is considered to be the part of the authentication process which requires the most mental effort.

- **Active Authentication:** This phase defines the time a user needs to enter their secret. It begins with the very first input action and ends with the very last[1]. This phase will be called the **input** phase, for simplicity reasons.
- **Error Recovery:** This phase is useful in situations in which an input error occurs. Its purpose is to signify to the user that an error had been made. The recovery can take place by requesting a restart of the authentication process, or by allowing so called *undo operations*, which allow the user to correct their mistake and proceed with the input.
- **Clean Up:** This phase is not considered to be a solid part of the authentication process, yet in some newly developed mechanisms, it is crucial for completing the authentication. An example for its use, is found in the concepts **TinyLock** by Kwon et al. [14] and **Whispercore** by Airowaily et al. [5]. In these designs, the clean up phase is intended to remove oily residues on the smartphone screen and thereby counteracts the chance for potential smudge attacks.

According to Zezschwitz et al. [1], *orientation* and *input* phases are considered to be the most essential parts of an authentication process. In previous approaches, the *input* phase has often been considered to define the actual authentication procedure. Consequently, *orientation time* was often disregarded and ignored in usability evaluations. Ananymous et al. [1] describe *error recovery* to be not essentially mandatory for successful authentication, yet very useful for its error management. They also observed that its implementation could have a significant effect on the efficiency of an authentication mechanism. In some cases, its implementation may even trigger the need for further *orientation* or *clean up* phases [1]. This, in return, may cause a longer authentication duration. The implementation of the *clean up* phase depends on the design of the authentication concept. Authentication is possible with or without it (see Figure 3.1).

By outlining the structure of the authentication process, Zezschwitz et al. [1] proposed a collection of observations and factors to prove in a user case study. First, they observed that the proportioning of the authentication phases may affect the perceived efficiency of

1 *Last input action* means the moment which determines whether unlocking is permitted or denied [1].

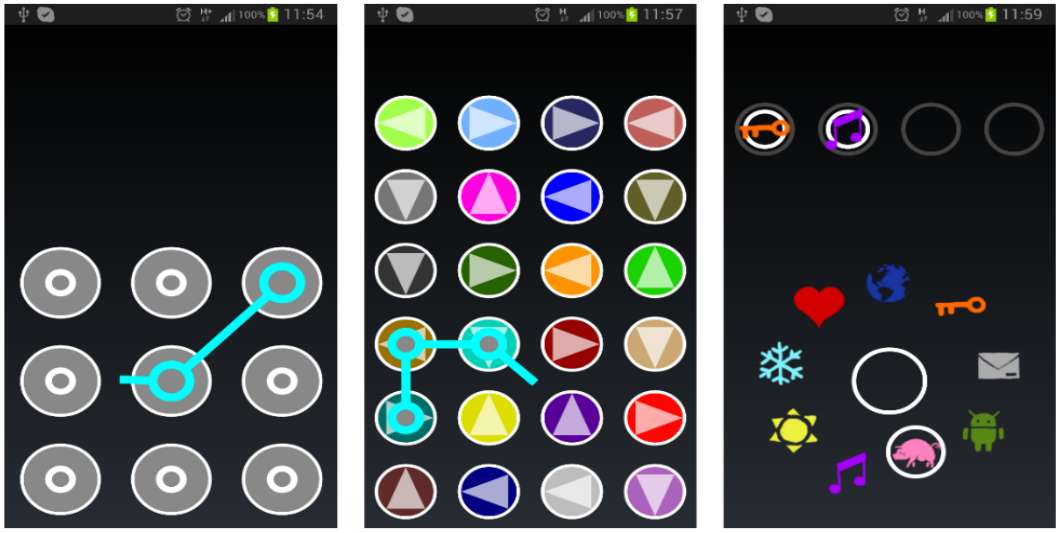


Figure 3.2: The concepts that Zezschwitz et al. [1] used in their study. Left: Android Pattern Unlock (baseline); Middle: Pattern Rotation; Right: Marbles. Compare with Figure 2.2 to see how the concepts were modified in this study [1].

an authentication mechanism. For instance, they noticed that the longer the *orientation* of an authentication mechanism is, the slower and less efficient it is perceived. In fact, cases in which the duration of the *orientation* phase exceeded the *input* phase, have been seen to be widely disliked by users.

Second, they noticed that the ordering of the phases might impact perceived efficiency. For instance, **Pattern Rotation** only consists of two phases, with the *orientation* phase preceding the *input* phase. **Marbles**, on the other hand, has multiple short *orientation* and *input* phases, which are ordered in an alternating manner. Zezschwitz et al. [1] suggested that the latter has the possibility of decreasing the perceived duration of authentication.

Third, they suggested that the coherence of the *orientation* and *input* phases also have a potential influence on a mechanism's perceived efficiency [1]. Meaning, the less coherent the contexts of *orientation* time and *input* time are, the less efficient and convenient they are perceived. This factor was regarded in the design of **Marbles** [26]. Thus its tasks alternate between finding the marbles and dragging them into the gap, their contexts complement each other. Through further research Zezschwitz et al. [1] found that humans tend to perceive periods longer than they are, if they consist of many incoherent contexts [1, 27].

Lastly, Zezschwitz et al. [1] added that *error recovery* should be cautiously managed throughout an authentication process [1]. As mentioned above, the implementation of *error recovery* may result in further *orientation* and *clean up* phases. This observation was shown in findings by Zezschwitz et al. [25], discussed in Section 2.2. They discovered how users tended more towards *pattern* authentication than *pin* because they preferred its management of errors. *Pin* manages the errors through *undo-operations*, which have been shown to be disliked amoungst users. Therefore, they are seldomly used in designs [25, 1].

3.2 USER CASE STUDY

Zezschwitz et al. [1] decided to conduct a study in which they mainly focused on the phases, *orientation*, and *input*, as they are the most important phases of an authentication process. To prove their assumptions and observations, they selected three authentication concepts, each representing a different ratio of both phases [1][2]:

- **Android Pattern Unlock** represented a "short orientation/short input" ratio,
- **Pattern Rotation** represented a "long orientation/short input" ratio,
- **Marbles** represented a ratio in which orientation and input time were interlaced.

It is important to note that *Pattern Rotation* and *Marbles* [26] were slightly modified in this study. *Pattern Rotation* presented a larger grid than the original design, and in *Marbles*, the elements (marbles) were small images rather than colored dots (see Figures 3.2 and 2.2). All three concepts were implemented in a prototype which was then installed on the Android smartphones of study participants [1]. The prototype was intended to serve as an authentication system on the participants' phones. Each of the concepts was planned to be tested for ten days [1]. After each ten-day period, an online survey was required to be taken. Also, during the concept-tests, *orientation* and *input* times were logged for each authentication [1]. *Orientation* time was logged from the moment the screen was switched on, to the first input event. *Input* time was logged from the first to the last input event [1]. Participants were allowed to choose their own secrets for the concepts. However, fixed guidelines were set, for instance, patterns for *Android Pattern Unlock* had to consist of six nodes, patterns for *Pattern Rotation* had to consist of five nodes, and secrets in *Marbles* had to consist of four elements [1].

3.2.1 *Results*

The study yielded 19 participants and delivered a set of 18 valid data entities [1]. Zezschwitz et al. [1] were interested observing the different outcomes that would result, if they used three different approaches to evaluate the efficiency of all three authentication concepts. They began with analyzing the overall authentication times of the concepts and noted the following ranking regarding their **measured performances**[3] [1]:

1. **Android Pattern Unlock**,
2. **Pattern Rotation**,
3. **Marbles**.

Then, they only analyzed the measured *input* times of the concepts and noted the following difference:

1. **Pattern Rotation**,

2 To better understand the functionalities of the concepts listed above, it is recommended to revisite the approach by Zezschwitz et al. [26], presented in Section 2.2.3.

3 The concepts are ordered from fastest to slowest (or best to worst) in this and the following rankings of this section.

2. **Android Pattern Unlock**,
3. **Marbles**.

Last, they analyzed the measured *orientation* time of the concepts and realized another significantly different outcome. *Android Pattern Unlock* had the shortest *orientation* time of all three concepts, as it required the least amount of mental effort [1]. *Pattern Rotation* and *Marbles* did not notably differ from each other, in terms of their average *orientation* times [1].

The perceived efficiency of the concepts was rated qualitatively through five-point Likert scales [1]. Results showed that *Android Pattern Unlock* was seen as the fastest of all three concepts. More than half of the participants considered *Marbles* to be efficient, despite it having been measured slower than *Pattern Rotation*. Moreover, half of the participants also perceived *Pattern Rotation* as efficient [1]. Participants were asked if the concepts contented a fast and easy *orientation*. The results delivered the following ranking [1]:

1. **Android Pattern Unlock**,
2. **Marbles**,
3. **Pattern Rotation**.

Lastly, when asked about the required cognitive effort, all participants approved that *Android Pattern Unlock* required the least amount of mental effort, followed by *Pattern Rotation*, then *Marbles* [1].

3.2.2 *Design Recommendations*

Based on the results of their study, Zezschwitz et al. [1] made a list of design recommendations to consider in the creation of authentication concepts. They are intended to optimize the usability of an authentication concept by regulating the following aspects [1]:

- **Recommendation 1:** *"Measure all Stages"*
  By including *orientation time* into the time measurements, the possibility of making false conclusions about a concept's usefulness could be prevented.
- **Recommendation 2:** *"Keep Orientation Time Low"*
  As *orientation times* are disliked by users, it is suggested to keep them as short as possible, as the effect of long *orientation times* cannot counteracted by short *input times*.
- **Recommendation 3:** *"Optimize the Ratio between Orientation Time and [Input Time]"*
  Orientation phases should not be longer than the corresponding *input* phases, because they are not well accepted by users, regardless of how fast or efficient a concept's performance is.

- **Recommendation 4:** *"Avoid/Minimize Randomization"*
  Although randomization is often used as a countermeasure towards attacks (e.g., shoulder surfing), it impacts the perceived efficiency of a concept negatively and should, therefore, be avoided. Especially in between the tasks of an authentication procedure.

- **Recommendation 5:** *"Measure Perceived Speed"*
  It is recommended that the performance of an authentication concept is not only assessed quantitatively, yet also qualitatively, in order to obtain information on how users' perceive certain aspects of the concept (e.g. *orientation time*).

- **Recommendation 6:** *"Optimize Context Switches"*
  The tasks in an authentication concept should be coherent in terms of their contexts, otherwise they are not perceived as usable.

- **Recommendation 7:** *"Provide Efficient and Non-interrupting Error Recovery"*
  Error Recovery should be designed to be as "fast" and simple as possible. A given example for good *error recovery* is *Android Pattern Unlock*, as its method is non-disturbing, thus errors are indicated through colors.

3.3 LIMITATIONS AND SUGGESTIVE IMPROVEMENTS

This section will first begin by presenting some of the limitations of the study, given by Zezschwitz et al. [1]. Next, observations on specific qualities of the study will be presented and suggestive improvements on these qualities will be discussed.

According to Zezschwitz et al. [1], the overall perception of the tested concepts could have been influenced by the participants' general preference [1] because a person's culture and history have shown to influence their acceptance of a particular system [12] (Section 2.2.1). The complementary study, presented in Chapter 5 is intended to exclude this limitation by developing a single concept in which particular ratios are represented. That way, a more genuine evaluation of the ratios would be possible, without any interference of participants' preferences regarding a particular concept. Moreover, Zezschwitz et al. [1] stated that the measured times for *orientation* might have differed from the actual times [1]. Reason being, that the measurements for the *orientation times* began as soon as the smartphone screen was turned on. However, not every screen activation was always immediately followed by an authentication [1]. A possible solution for rectifying this inaccuracy, is to isolate the *orientation* phase from any other possible action. The concept for the complementary study was designed in a way which required the user to actively initiate the authentication process. That way, a more fix and accurate starting point for the *orientation time* could be defined.

Further limitations, observed by the author of this thesis are the following: The ratios chosen by Zezschwitz et al. [1] might not have been suitable enough to receive a definite result on whether users truly prefer short *orientation time* over long *orientation time*. It would be interesting to observe the outcome of testing ratios that have the same temporal arrangement, yet are contrasting regarding the lengths of their phases. Thus not included by Zezschwitz et al., it is considered to include the ratio *"short orientation/long input"* into the complementary study. The author suggests that by mainly focusing on the ratios *"long*

orientation/short input" and *"short orientation/long input"*, and by setting the ratio *"short orientation/short input"* as a baseline, one could receive more detailed results on users' attitude towards authentication concepts with different lengths of *orientation* phases. A further suggestion is to observe whether different lengths of *input* phases might play a role in users' preference and perception of efficiency. Lastly, it is suggested that by allowing study participants to qualitatively evaluate the ratios in comparison to each other, one could receive more detailed and precise information about which ratio is generally perceived as efficient and which is not.

The next chapter of this thesis will present a concept which was specifically designed for the sake of the complementary study, later presented in Chapter 5. It was created to implement a specially designed to represent each of the previously mentioned ratios. Its sole purpose was to serve as supportive tool in the study and no further. Nonetheless it is important, for the scope of this thesis, to understand the design choices and the thought processes that were involved in creating it, as they were made from a user-centered design approach and also included HCI principles, to assure the creation of a system that is suitable for the intentions and desired goals of this study.

4

DEVELOPING THE CONCEPT FIPA

The following chapter represents a concept called **FiPa** (**Fi**nd **Pa**ttern) which was developed to contribute towards the ongoing work of Zezschwitz et al. [1], discussed in Chapter 3. Before entering into the development process, it is crucial to note that the following concept was created solely to serve as a tool in the user case study, which will be presented in Chapter 5. The system is in no means a suggestion for an authentication concept and was not intended to be utilized as such. Its sole purpose was meant for the scope of this thesis, and no further. Therefore certain aspects (e.g., security and effectiveness) have consciously not been considered during the design and the development of this concept. Nonetheless, the design process was based on a **User-Centered Design** (UCD) approach and included a selection of **Human Computer Interaction** (HCI) principles, to make the concept easier to understand and function. The exact procedure of this process will be documented through the direct voice of the author to convey her thought process and intentions in this part of her contribution towards this thesis.

4.1 REQUIREMENTS

As mentioned above, the concept was intended to be utilized as a tool to help examine certain factors later on in the study, which are *orientation time* and *input time*, previously introduced in Chapter 3. In order to do so, the nature of the concept had to be specially designed to suit the anatomy of an authentication process. The concept had to be divided into two coherent and related small tasks: a **mental task** and a **practical task**. The intention behind this division was to be able to measure the *orientation time* (duration of the mental task) and the *input time* (duration of the practical task), separately. For that, a timer feature had to be implemented, in order to undertake the measurements, which would automatically be saved in a local database (see Section 4.3).

Furthermore, as indicated in Section 3.3, the goal of the research contribution in this thesis, is to examine the impact that *orientation time* has on the perceived efficiency of an authentication concept, with respect to its *input time*. To complement and also validate the findings from the ongoing study by Zezschwitz et al. [1], we proposed to analyze the following two contrasting time ratios:

"long orientation/short input"
vs.
"short orientation/long input".

The crossing descriptors *long* and *short* were meant to define a certain length, meaning *long orientation* had to have the same duration as *long input*, and vice versa. In order to have a baseline to which the measured times of the ratios above could be compared, a third ratio was included. It is called short orientation/short and its *orientation time* and *input time* are equally long.

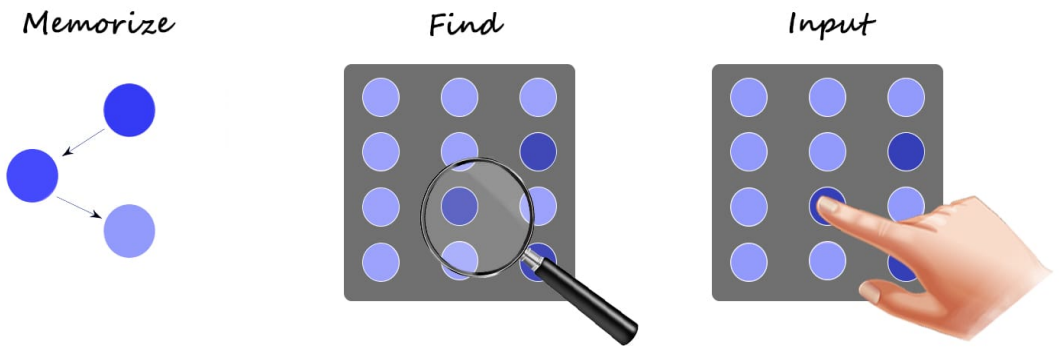


Figure 4.1: Simple illustration of the initial idea for **FiPa**. The procedure is composed of three steps: (1) **Memorize** a pattern; (2) **Find** the memorized pattern, hidden inside a grid; (3) **Input** of the pattern.

In addition, we were interested in directly comparing both contrasting ratios against each other by using *only one concept*, instead of three (see Chapter 3). Through unifying all three ratios into one concept, it was possible to eliminate the chance of future results being influenced by the study participants' personal preferences of the concepts. For that reason, the created concept had to be malleable in a such way, that the complexity of each task (**mental** and **practical**) could be adjusted, according to the represented ratio. For "long phases", we intended to be represented through difficult tasks (**mental** or **practical**). An analogous approach was taken for the "short phases" of the ratios.

4.2 DEVELOPMENT

In the following section, we will present the design and evaluation attempts that were necessary to generate **FiPa**: the concept presented and utilized in our study.

4.2.1 *Fundamental Concept Idea*

During the creation of **FiPa**, we were interested in creating a concept which activated an interaction that reminded users of a smartphone authentication. We assumed that by making the interaction resemble an authentication process, future study participants' could better understand and adapt to the context of the study. A further one of our intentions was to construct a concept that was as usable, to direct participants focus and attention towards the actual usability issues, intended for them to test. For that, we decided to create a *graphic-based concept*, as researchers have discovered them to be commonly accepted by users and perceived as comfortable to use [25].

The name of our concept, **FiPa**, is inspired by its functionality. **FiPa** is an abbreviation for the phrase "**Fi**nd **Pa**ttern" and its meaning will be comprehensible through the following description of its procedure (see Figure 4.1): First, a predefined pattern is presented which has to be memorized well by the user. This pattern consists of a certain combination of buttons. Each button has a certain characteristic, that makes it distinguishable

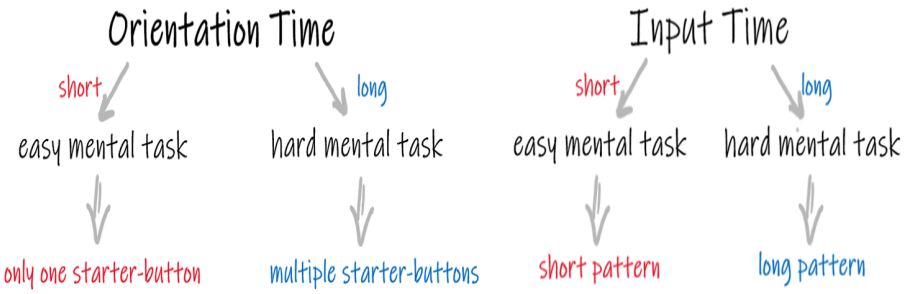


Figure 4.2: Depiction of how the **mental** and **practical tasks** were intended to be designed, depending on whether *orientation time* and *input time* were long or short.

from the others. Memorizing the order of the buttons and their distinct characteristics is crucial for successfully accomplishing the **mental** and **practical task** (Section 4.2.1). After memorizing the pattern, a large grid, filled with buttons, is presented. The **mental task** defined by finding the memorized pattern, hidden inside the grid. When found, the **practical task** is comprised of entering (input) the found pattern correctly into the grid (see Figure 4.1).

The idea of using a grid of buttons for the **mental task** was derived from the concept *Pattern Rotation* [26, 1]. The choice of using specific characteristics for each button was inspired by the concept *Marbles* [26, 1][1]. We tried to limit the amount of mental effort required for interacting with **FiPa** was reduced as much as possible by making a set of intentional design choices. We assumed the pattern would certainly not be memorized permanently and that it would, therefore, be stored in participants' short-term memory. Therefore, we attempted to reduce the load of mental effort by letting the pattern be searched for, instead of completely reproduced from memory. That way, during the **mental task**, when the user stumbles upon the hidden pattern inside the grid, they are more likely to detect it because they recognize it. As mentioned above, this is a measure that was taken to ease the interaction with **FiPa** and to shift participants' focus onto the important matters, namely the ratios represented in the study.

4.2.2 *Concept Design*

In the following section the design approaches, that were involved in creating and developing the concept **FiPa**, will be presented.

4.2.2.1 *First Draft*

The initial layout design for **FiPa** is illustrated in figure 4.3. As in *Marbles* [26, 1], different elements of the concept, meaning the buttons, were distinguishable through small images, emojis to be exact. To provide a clear overview of the vision, I will first begin by explaining how we the design for the **practical task** and then presenting my intentions regarding the **mental task**. As mentioned in Section 4.1, the first step of the concept is to memorize a pattern at the very beginning of the activity. For simplicity reasons I decided to mark the beginning of each pattern, by setting their first button to contain a key-emoji

1 To familiarize with the concepts *Marbles* and *Pattern Rotation*, please revisit Section 2.2.3 and Chapter 3.

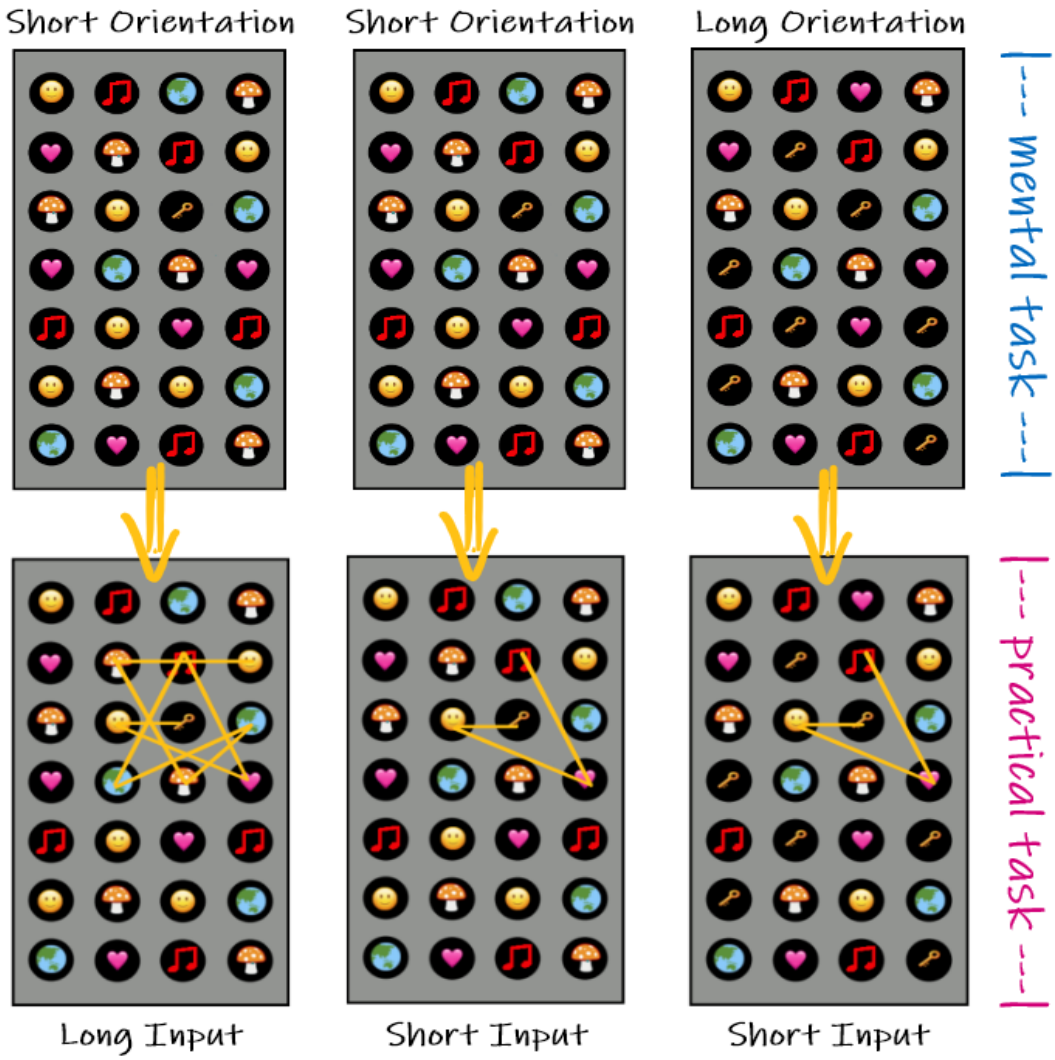


Figure 4.3: Detailed representation of the initial layout design for **FiPa**. **Mental** and **practical task** are marked to provide a better understanding of the concept.

(see Figure 4.3). We will call this button the *starter-button*. Examples for the patterns are shown in figure 4.3. Moreover, I envisioned the input method of **FiPa** to be similar to *Android Pattern Unlock*. As the concept is intended to be implemented as smartphone application, I assumed that the chosen method of input would be suitable for a touch screen user interface.

For the **mental task** (see Figure 4.3), the design of the grid depended on whether long *orientation time* or short *orientation time* was intended. As mentioned earlier in Section 4.1, we assumed that for a long *orientation time*, we need to create a difficult and more complex search process. We imagined that by incorporating multiple *starter-buttons* inside the grid, besides the one belonging to the hidden pattern, we could complicate and elongate the search process. In contrast, we imagined it would be possible to facilitate the pattern search, by having the only *starter-button* in the grid belong to the hidden pattern. That way, our future participants could spot the pattern much easier and quicker. An analogous approach was considered for adjusting the complexity of the **practical task**.

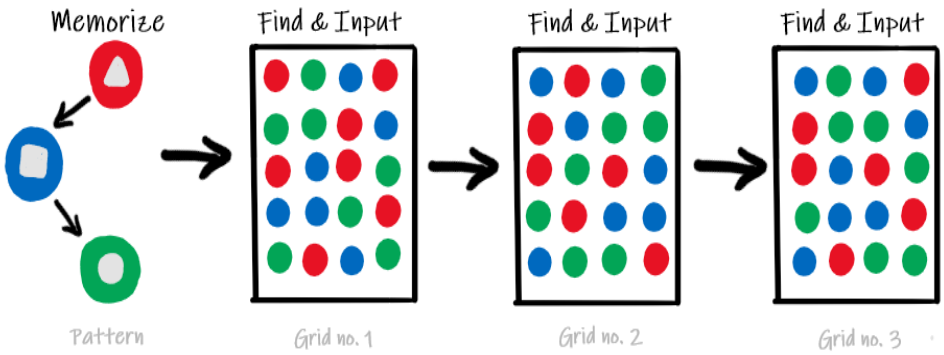


Figure 4.4: A sketch that presents the basic structure of each phase of the prototype. Each grid represents a **couple**: a **mental task** (find) and a **practical task** (input). After memorizing the given pattern, three uniquely designed grids followed. The pattern had to be found and entered in each of the grids, one after the other.

Depending on whether long or short *input time* was intended, the pattern designed for memorization and input was accordingly short or long (see Figure 4.2).

4.2.2.2 *Evaluation: First Draft*

The first draft of **FiPa** was evaluated, using a paper prototype. The prototype encompassed the three ratios (see Section 4.1) and was composed of three patterns[2] and three grids[3]. We used the same grid and pattern constellation, shown in figure 4.3.
It was important to examine how the design choices affected the usability of the concept and to see whether it was easy to use and to understand. Six participants were recruited to evaluate the first draft. Before presenting the prototype to each participant, I explained the purpose of the study and the functionality of the prototype. The structure of the prototype was based the concept of *Wizard Of Oz* prototyping [8]. This meant that during a participant's interaction with the prototype, I would uncover its following event (grid or pattern), depending on the participant's *input* or *action*.

Five of the participants found that the many different emojis created an overwhelming appeal on the eyes and that it made the grid appear very crowded. Moreover, the long pattern (see Figure 4.3) was considered too complicated and was hard to memorize by all of the participants. As mentioned earlier, the reason behind the complicated pattern, was to represent long *input time*. Thus the modified complexity of the pattern was not well accepted, a different solution is called for, to help control the length of the represented *input time*. Nonetheless, the idea behind the concept was liked by all of the participants. Especially, the notion of starting each pattern with a specific *starter-button*. Despite the flaws mentioned above, they understood the basic functioning of our concept well.

The information gained and the lessons learned through the previous evaluation phase gave us a closer insight into humans' perception and cognitive ability. At this point, we were one step closer to creating a more usable and effective concept.

2 Two short patterns intended for *short input time* and one long pattern intended for *long input time*.
3 Two grids with only one *starter-button*, for *short orientation time* and one grid with multiple *starter-buttons*, for *long orientation time*.

4.2.2.3 *Second Draft*

For the second draft of **FiPa**, a few adjustments were made regarding its overall aesthetics and the design. Through further research, I discovered that due to the *pictorial superiority effect* [15], humans can retain information through images, much better than through letters or numbers [15, 2], which is why I decided to continue representing the characteristics of the buttons through images.
To reduce the crowded appeal from the first draft, I replaced the emojis with three simple shapes: *circle*, *square*, and *triangle*. The initial choice of colors for the design was: *red*, *green* and *blue*. They are known to be the basic colors that the human eye perceives naturally [8]. The *starter-button* was designed to be a red containing a triangle (see Figure 4.4). The triangle shape was chosen because it is a symbol that has been shown to convey the meaning of *power*[4] and *permanence* [10]. Moreover, the human eye is naturally attracted to its shape [5]. I assumed that through the mentioned effect of the triangle and the alerting appeal of the color red, users' vision would initially be attracted to these button through the ability of their *pre-attentive perception* [8].

To properly design the patterns and grids design of this draft, it was crucial to define a fixed size for the grid. After a few of trials, I found the size 4x7 to be most suitable for the concept, big enough to hold a decent amount of buttons and to provide a clear overview of the grid's content. An additional design feature for this draft are so-called *traps*. *Traps* are a set of buttons, that have a similar constellation and set of characteristics as the hidden pattern, yet are not identical to it. Their purpose is to mislead the user, during the **mental task** and thereby elongate the search process as needed. Another modification made was the input method. As participants did not improve of the complexity of the long pattern, in the first draft, I decided to change the input method. I discovered that pressing the buttons in the right order, instead of connecting them (see Section 4.2.2.1), would allow more control over the approximate duration of the *input time*. That way, long *input time* could represented without requiring participants to memorize complicated patterns. Moreover, the created patterns no longer covered much space inside the grid, which made it easier to shuffle the buttons and set more *traps*.

4.2.2.4 *Evaluation: Second Draft*

Analogous to the evaluation of the first draft (see Section 4.2.2.2), I created a *Wizard of Oz* [8] paper prototype (see Figure 4.6) to evaluate the changes and improvements, made in the second draft of the concept. However, this time, the prototype was created differently. I was interested in testing a certain structure for the concept to see if it would be suitable for the its implementation as a smartphone application. The paper prototype was structured into three parts as there are three ratios (see Section 4.1) to examine. In the previous draft, there was only one **mental** and **practical task** per ratio. For simplicity, we will call the pairing of a **mental** and a **practical task**, a **couple**. Instead of having only one **couple** per ratio (as in the first draft), I decided to assign three couples to each ratio (see Figure 4.5). My intention behind this decision was to assure that participants would have a better memory of the different ratios during the qualitative segment of

4 http://www.whiteriverdesign.com/meaning-shapes-design/ - last accessed: 2019/11/16
5 https://designshack.net/articles/layouts/the-sometimes-hidden-meaning-of-shapes/ - last accessed: 2019/11/16

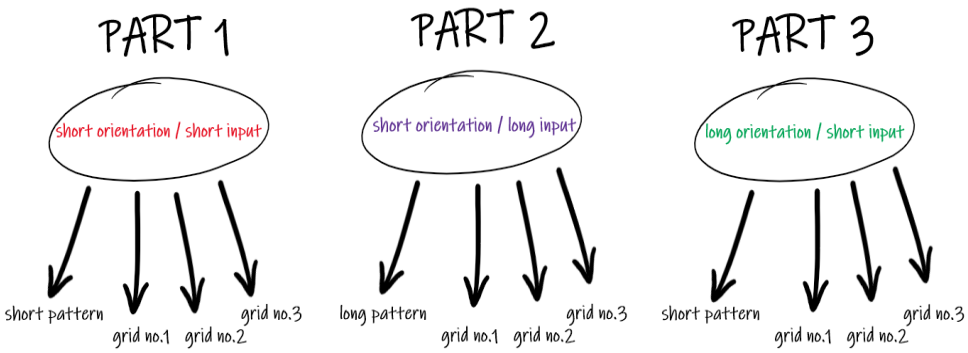


Figure 4.5: Simple representation of the structure of the second design. Each part is assigned to a particular ratio. For each ratio there are three grids. Each grid presents a **mental task** (find) and **practical task** (input), a so called **couple**. The order of the ratios presented in this figure is only a suggestion. The exact order of the ratios was not important in the evaluation phase.

the study, if they interacted with each one more than once. The modification of the concept was tested with the same set of participants who tested the first draft, in order to receive a more detailed feedback on whether the flaws, detected in the previous draft, were correctly fixed. It was possible to interview the same set of participants, as the design and the structure of the **mental** and **practical tasks** differed completely from the first draft. Fortunately, both, layout and structure of our prototype were well accepted.

To ensure that the average duration needed for the accomplishment of the **mental** and **practical tasks** corresponded with the represented ratio, I manually timed each participant using a stopwatch. Although each part of the paper prototype was comprised of three **couples**, only the time measurements for every third **couple** were. The first and second **couples** of each part were considered exercises for the participants to get acquainted with the concept.
Analogous to the measurement approach made by Zezschwitz et al. [1] (see Chapter 3), I defined a distinct interval for each of the tasks. A **mental task** began immediately after a particular grid was uncovered and ended as soon as the hidden pattern was found. A participant would indicate that they found a pattern by tapping its *starter-button*. The **practical task** began with the *first button press* of a pattern and ended with its the *last button press*. During the input, the *starter-button* had to pressed once again, even if it had already been tapped to signify the find. I was aware that the measured times would not be completely accurate. They were only intended to serve as a rough estimate for the duration of the phases. Fortunately, the designed grids and patterns created for the paper prototype (see Figure) delivered proper time estimates for the represented ratios and were, therefore, suitable to be included in the implementation of the concept.

4.3 IMPLEMENTATION

The following section presents the implementation of the concept **FiPa**. I will begin by explaining the structure of the application and certain features which were embedded

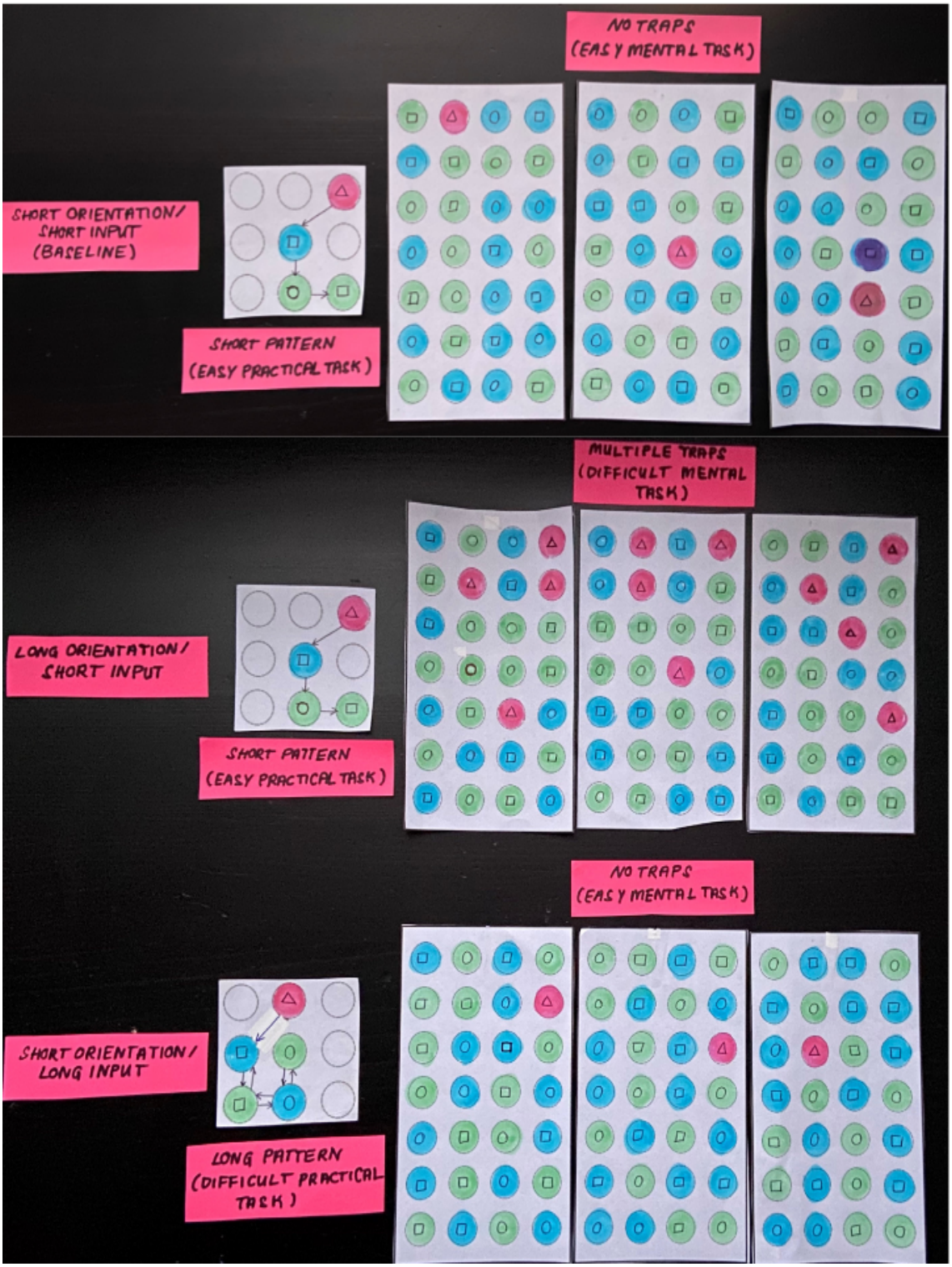


Figure 4.6: This is an picture of the paper prototype which was used to evaluate the second draft of the concept. In the picture the cards are categorized by ratio. To better understand the purpose of the *traps* (see Section 4.2.2.3), it would be useful to try and search for the pattern, in the three grids of the ratio *long orientation/short input* (middle row).

into it. As mentioned in the beginning of this chapter, **FiPa** was solely intended to be a supportive tool to help us validate the findings made by Zezschwitz et al. [1], later in our

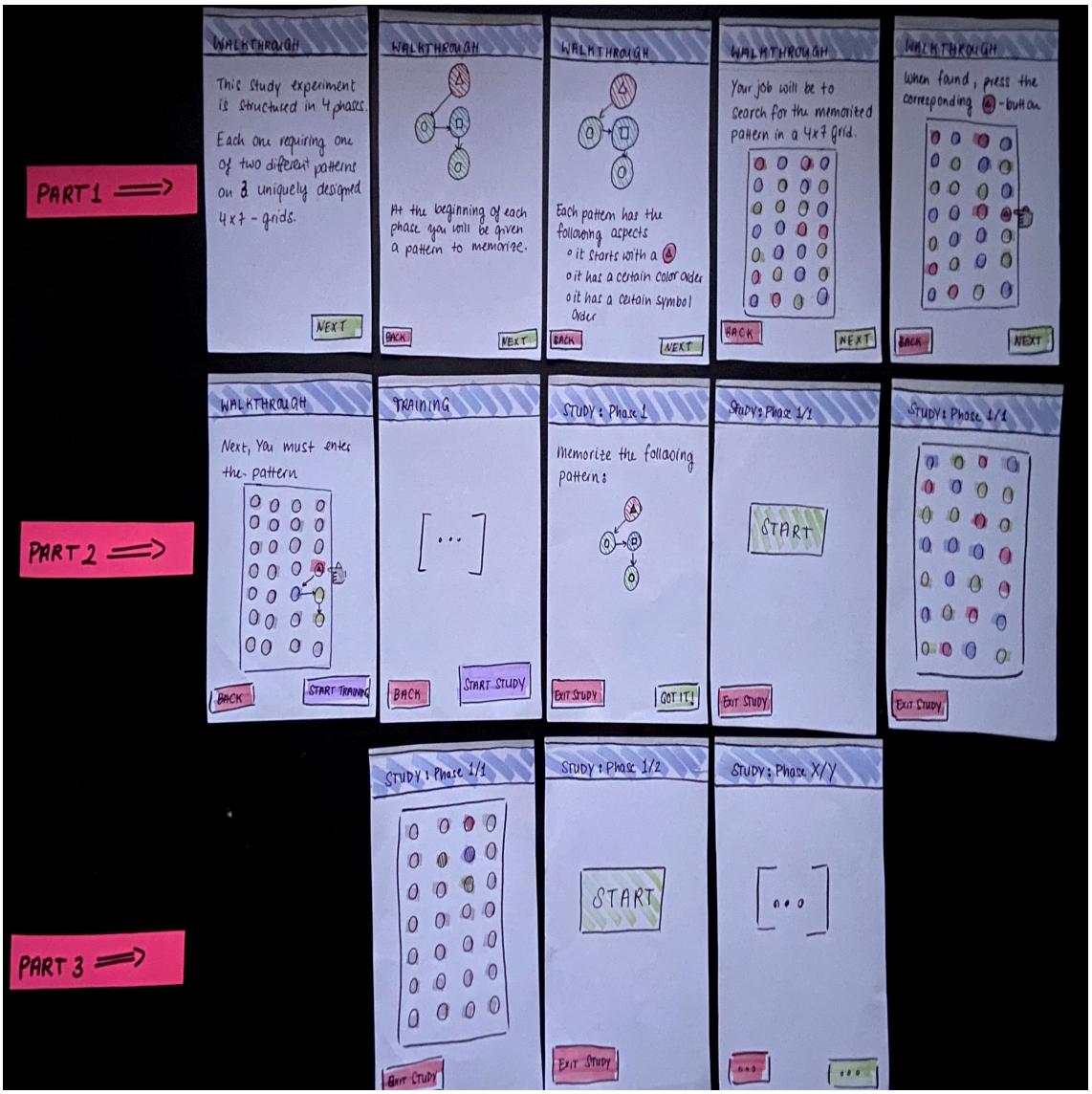


Figure 4.7: This picture illustrates the initial conception of the application's structure and flow. Although the developed application sightly differs from the cards, they served as a helpful base for the implementation of **FiPa**.

complementary study (see Chapter 5). For that, I will not deal with exact details of its framework, to avoid distraction from the fundamental purpose of this thesis.

FiPa was implemented as an Android application, using the Software *Android Studio*, which is based on IntelliJ IDEA. It is comprised of a series of classes, called activities. They can be seen as the fundamental building blocks of an application. Each activity describes and controls the functions of the user interface (UI) presented in a window on the screen[6]. The structure of the UI is defined by a so-called layout, which is an XML-file that defines the features (i.e., images, buttons, strings) presented in a particular

6 https://developer.android.com/guide/components/activities/intro-activities - last accessed: 2020/01/03.

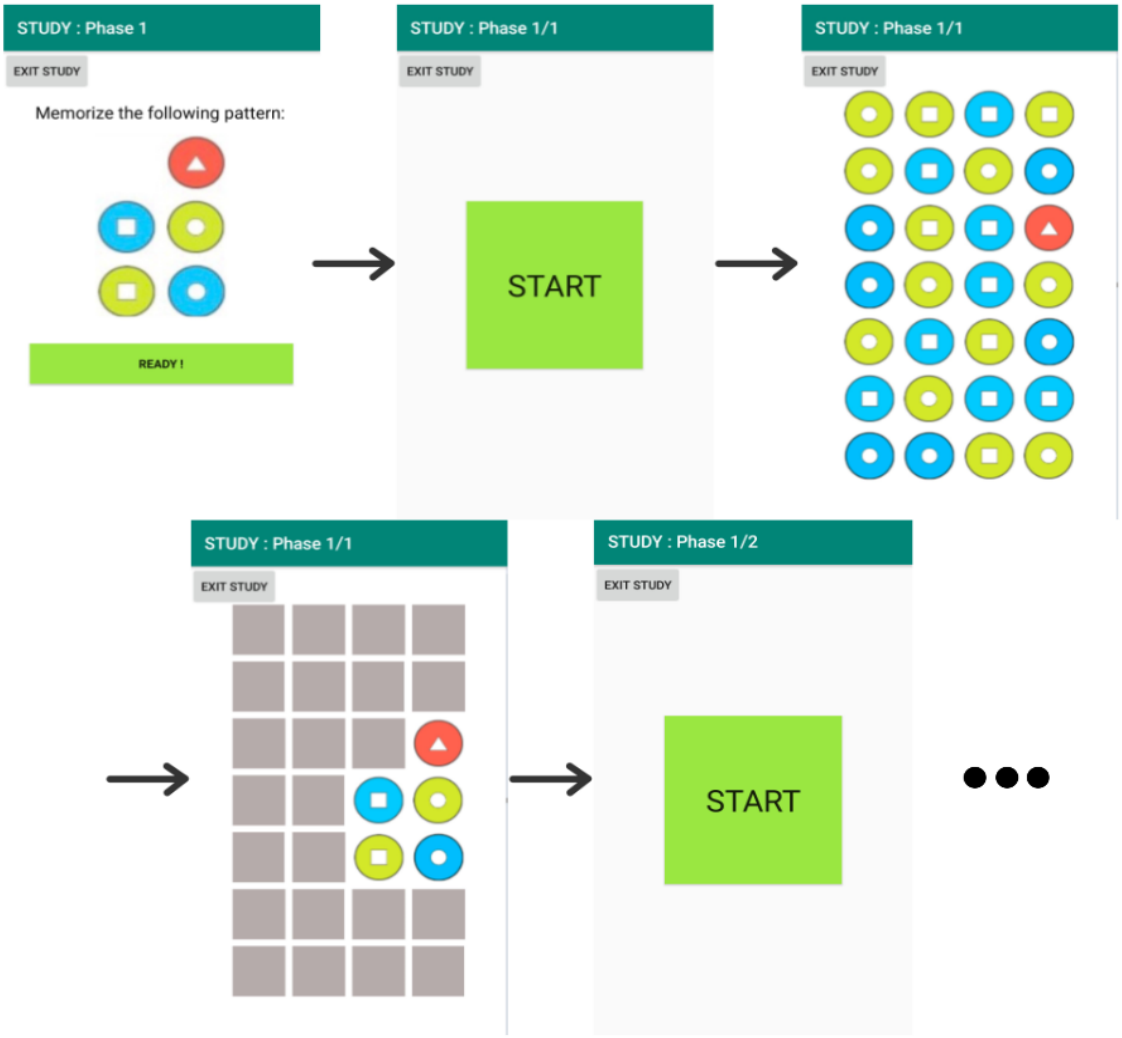


Figure 4.8: This image illustrates the structure of a phase in the application. The remaining parts of the phase (Phase 1/2 and Phase 1/3) are analogious to the first part (Phase 1/1).

window[7]. Activities within an application are able to communicate with each other and they determine the following event of each action inside a window.

4.3.1 *Phase Structure*

The elemental structure of the application was first assessed by creating a simple illustration using cards (see Figure 4.7). The intention behind this approach was to create a precise conception of the activity flow. Analogous to the design of our prototype (see Figure 4.6), the application consisted of three distinct parts. Each part represented a distinct ratio and was called *phase*[8]. Each phase consisted of three **couples** (a combination of **mental** and **practical task**). In the application each **couple** was described as a *level*, meaning each *phase* consisted of three *levels*. Similar to the paper prototype (see Figure 4.6), each *phase* also had a corresponding pattern assigned to it. As mentioned earlier in

7 https://developer.android.com/guide/topics/ui/declaring-layout - last accessed: 2020/01/03.
8 Not to confuse with Zezschwitz et al.'s interpretation of a phase, in Chapter 3.

this chapter, one of my goals for the design of the concept was to minimize the amount of mental effort required for the interaction. For that, the ratios *short orientation/short input* and *long orientation/short input* shared the same short pattern. That way, participants only had to memorize two patterns, instead of three.

All *phases* have the same flow. The first activity of each *phase* shows an assigned pattern on the screen (see Figure 4.8). The order in which the buttons should be entered, is conveyed through a simple animation. When the pattern is memorized, the user can proceed by pressing a green *"READY"*-button. The next activity presents a layout with a green squared *"START"*-button (see Figure 4.8). This activity is of great importance as it defines the starting point of the **mental task**, meaning the beginning of the *orientation phase*. The measurement of the *orientation time* is initiated as soon as the *"START"*-button is pressed and ends in the next activity, as soon as the user taps the correct *starter-button* in the grid (see Figure 4.8). This action causes a transformation: All buttons in the grid are blended out, except for the ones belonging to the pattern (see Figure 4.8). The transformation is meant to convey to the user that they can execute the **practical task**, meaning the *input phase*. The measurement of the *input time* is initiated through the first button-press, given the correct *starter-button* is selected, and ends when the last button of the pattern is pressed, given the pattern was entered correctly. If not, the time for *input phase* cannot be stored in the database, and is marked as *"failed"*. Analogous to the prototype, in Section 4.2.2.4, the *starter-button* was meant to be pressed twice: Once to signify the find of the pattern and end the measurement of *orientation time*, and once again to initiate the beginning of the *input phase*.

This process[9] repeats itself for the following two levels of each phase. At the end of each phase the following phase automatically begins by presenting the next pattern.

4.3.2 *Application Flow and Features*

In the following section, we will present the flow of our application **FiPa**, whilst introducing its special features along the way.

The first activity of the application presents window which allows the user to choose whether they would like to proceed with the training-segment or skip to the study (see Figure 4.9). Assume we were to proceed with the training. The training segment presents an exercise walk-through of the concept, meant to get the user acquainted with the concept of **FiPa** and to minimize the amount of errors made throughout the study. At the end of the training-segment, users have the option to proceed with the study or repeat the training (see Figure 4.9). It was important to assure that participants truly understood the functioning of the concept. For that they able to repeat the training-segment as often as they felt necessary. Assume we were to proceed with the study. The next activity is responsible for the maintenance of the collected data. It allows to enter a user-id for the user, which helped to pair a user's collected quantitative data (measurements) with their qualitative data (survey answers) later in evaluation (see Figure 4.9). Moreover, it was possible to view the content of the local database through the application (see Figure 4.9). This feature was useful during the development of the application, to assure that the phases (*orientation* and *input*) were measured correctly, and also in many cases during

9 Here we distinctively mean the process starting with the *START*-button onward.

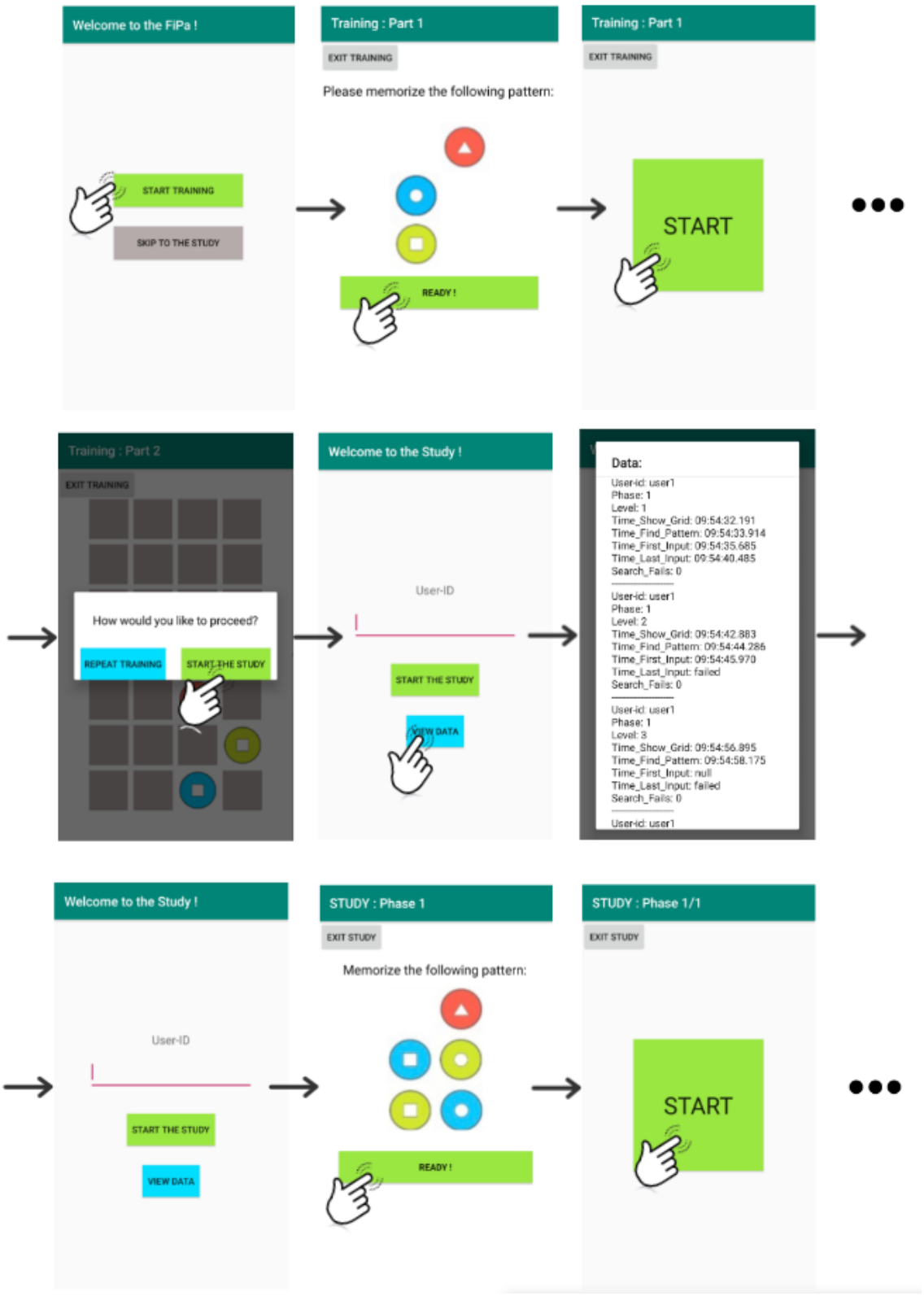


Figure 4.9: This images is a rough representation of the application flow.

the study. From this point, let us assume we were to start the study (see Figure 4.9). This action would lead us to the first phase of the concept. As described in Section 4.3.2,

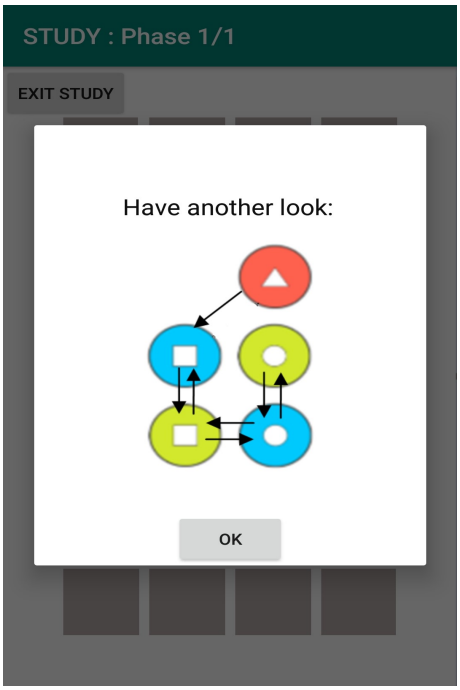


Figure 4.10: The *error-recovery* of the application of implemented as a pop-up window which appeared when three errors were made. The pop-up was the same for search and input errors.

each phase begins by presenting its corresponding pattern, intended for memorization (see Figure 4.9). When the pattern is memorized, the user can proceed by pressing the *"READY"*-button. It is important to note that buttons, used to approve or proceed, were intentionally given the color green, as it is it is commonly associated with the action "GO" or the approval "OK" in everyday life.

Assume we were to proceed and begin with the Level 1 of Phase 1 (see Figure 4.9). At this point, we have to complete the **mental task**, which is to find the hidden pattern inside the grid. During the search process, the *orientation time* is being measured in the background. The measurement is unnoticeable to the user during the interaction. As it is possible to press the wrong starter-button during the search process, we added a feature into the application which served as a form of *error-recovery* (see Chapter 3). It was realized through a pop-up window which appeared after the third search error was made (see Figure 4.10). The pop-up illustrated the pattern to remind the user, in case they had forgotten it. As soon as the user found the pattern, the grid transformed as described in Section 4.3.1 (see Figure 4.8), signifying the beginning of the **practical task**. As errors were also possible during the input, we also included *error-recovery* (see Figure 4.10). Here, the pop-up window appeared after the third input error. After it appeared, the app proceeded with the next action and marked the input of the particular level as *"failed"*. Although the main focus is to examine the effects of *orientation time* and *input time*, we could not avoid including an *error-recovery phase*, as it would have negatively impacted the user-friendliness of the application[10]. The procedure of the two follow-up

10 To assure that the *error-recovery phase* did not have an impact on the results of our study, we took specific measures, which will be presented in Chapter 6.

levels of the phase have the same presented procedure. The flow of the two following phases is analogous to the procedure presented in Section 4.3.1 (see Figure 4.8).

5 CASE STUDY

The following chapter presents a user case study which was intended to complement and validate the findings made by Zezschwitz et al. [1] (see Chapter 3). The chapter begins by introducing the design of the user case study. Next, the demographic of the recruited participants is presented, followed by a documentation of the study's procedure. Last, the quantitative and qualitative results of the study are discussed. The goal of this research contribution was to examine the effect of *orientation time* on the perceived efficiency of authentication mechanisms.

5.1 DESIGN

The user case study was designed as a lab study which was conducted in two destinations: at the computer science department of Rheinische Friedrich-Wilhelms-Universität Bonn (Uni Bonn) and at the experimenter's[1] home residence. The independent variable was *ratio* and it had three levels:

1. long orientation/short input (abbrv. *long/short*),
2. short orientation/long input (abbrv. *short/long*),
3. short orientation/short input (abbrv. *short/short*).

The implemented concept **FiPa**, presented in Chapter 4, served as a medium to represent the ratios of interest. The order of the ratios was counterbalanced amongst the participants (see Figure 5.1). Data was collected quantitatively by measuring the *orientation* and *input time* for each of the ratios, as explained in Chapter 4. Data was also collected qualitatively through a questionnaire, which required study participants to evaluate the aesthetic of the application[2], the ratios (*long/short* and *short/long*), and to also choose which of the two ratios they preferred most. On average, the duration of the study was 20 minutes per participant.

5.2 PARTICIPANTS

Twenty-five participants were recruited for the study. Initially, students were informed about the study through a social platform for computer science students at Uni Bonn. Another part was collected on campus of the university's computer science department, and four participants were acquaintances of the experimenter. There was no premise for participating in the study, meaning anyone was eligible to partake. Participants who made input-errors (see Section 4.3.2) were excluded from the evaluation. Nineteen valid data entities remained, of which 13 (62.4%) were male and 6 (31.6%) were female. The average age was 21 years, with 17 being the youngest and 31 being the oldest age. The

1 The experimenter in this study was the author of this thesis, herself.
2 Although this is slightly beyond the scope of the research, we were interested in seeing whether the design of the application had an impact on participants' performance.

1. Short Orientation /Short Input ⟹ Long Orientation /Short Input ⟹ Short Orientation /Long Input
2. Long Orientation /Short Input ⟹ Short Orientation /Short Input ⟹ Short Orientation /Long Input
3. Long Orientation /Short Input ⟹ Short Orientation /Long Input ⟹ Short Orientation /Short Input
4. Short Orientation /Short Input ⟹ Short Orientation /Long Input ⟹ Long Orientation /Short Input
5. Short Orientation /Long Input ⟹ Short Orientation /Short Input ⟹ Long Orientation /Short Input
6. Short Orientation /Long Input ⟹ Long Orientation /Short Input ⟹ Short Orientation /Short Input

Figure 5.1: The order in which the three ratios were counterbalanced amongst the participants during the study.

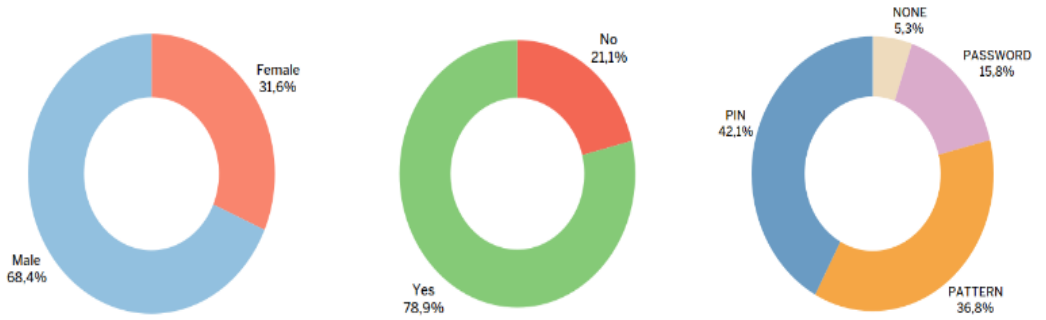


Figure 5.2: Demographic information on the *gender* (Left), *IT-Background* (Middle), and the *personal screen lock choice* (right) of the recruited participants.

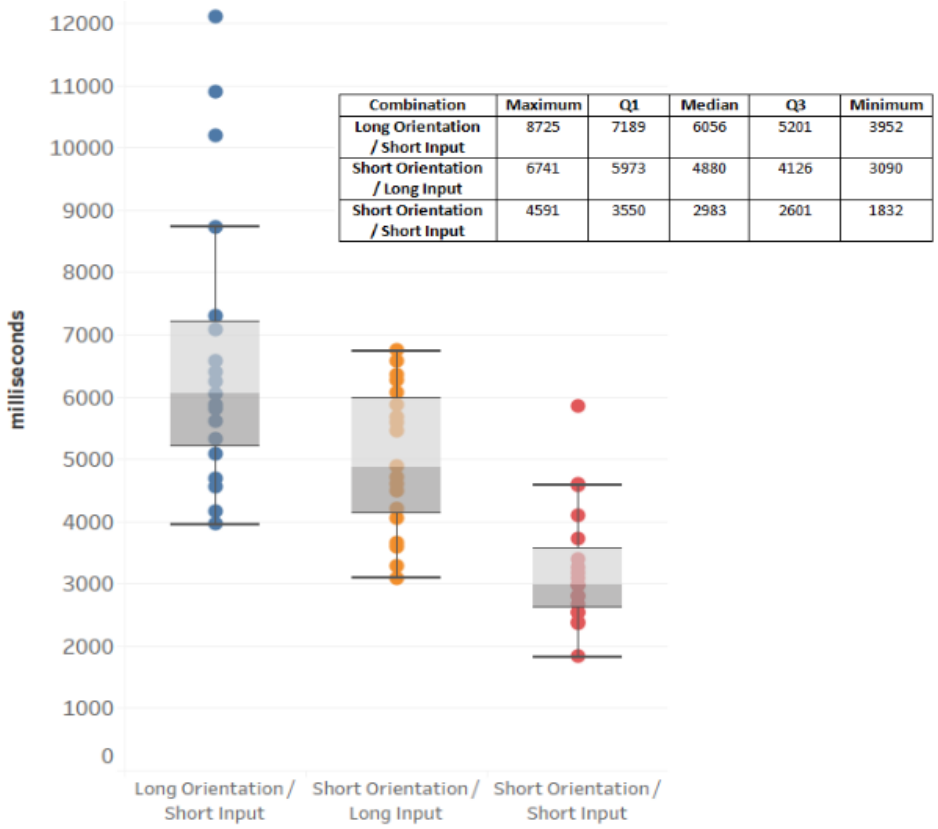
majority of the participants (78.9%) had an IT-Background and were computer science students. Also, all participants, except for one, used a screen lock for their smartphones: 42.1% used *Pin*, 36.8% used *Pattern*, and 15.8% used *Password* (see Figure 5.2).

5.3 PROCEDURE

The study was held for each participant, separately. First, the experimenter provided a brief introduction on the study's purpose. She explained that its aim was to analyze certain factors of smartphone authentication which might play a role in its usability. She also emphasized that the security aspect of the presented concept **FiPa** was outside the scope of this research study. Moreover, participants were assured that the testing of **FiPa** was not intended to evaluate their cognitive skills or intelligence. It was important that they felt comfortable and that they did not feel nervous or put under pressure during the course of the study, as it could negatively impact the validity of the obtained results.

Next, the experimenter described the structure of **FiPa**'s implementation. She explained that it was meant to emulate an activity, which resembled an authentication concept and that it presented a series of small "challenges", for the participant to solve[3]. These challenges were demonstrated with the help of the paper prototype, shown in Figure 4.6.

3 "Challenges" meant the **mental** and **practical tasks**, explained in Chapter 4.



Combination	Maximum	Q1	Median	Q3	Minimum
Long Orientation / Short Input	8725	7189	6056	5201	3952
Short Orientation / Long Input	6741	5973	4880	4126	3090
Short Orientation / Short Input	4591	3550	2983	2601	1832

Figure 5.3: A plotted representation of the overall times for each ratio, presented in the study.

After ensuring that the participant had no further questions, the experimenter proceeded by presenting the application to the participant. The application was installed on an Android smartphone which was provided by our research group.
First, the participant was advised to begin with the training-segment of the application, presented in Section 4.3.2 (see Figure 4.9). The purpose of the training-segment was to ensure that the participant understood the concept of **FiPa** and to reduce the number of potential errors in the quantitative data set. As mentioned in Section 4.3.2, the participant was allowed to repeat the training-segment, until they felt ready to start with the actual testing of **FiPa**. During the training-segment, the experimenter guided the participant through the process, when help was needed, and she explained to them certain features, such as the *error-recovery* and the method of input.

When the participant felt ready to start the test, the experimenter entered a unique *user-id* for the participant. The experimenter did not intervene, as the participant was executing the actual test in the application. Once the participant was done, they were given a questionnaire to fill out (see Appendix A). At the end of the study, each participant was compensated with 5 Euros.

5.4 RESULTS

5.4.1 *Measurements*

As mentioned earlier, *orientation* and *input times* were measured for each ratio. Analogous to the measurement approach, presented in Section 4.2.2.4, the first and second levels of each phase were considered to be an exercise for the user. Despite the training-segment, participants made many mistakes during the first two levels of each phase, and made very little, to non, in the third. After excluding all data entities which contained unsuccessful input activities, 19 clean data sets remained.

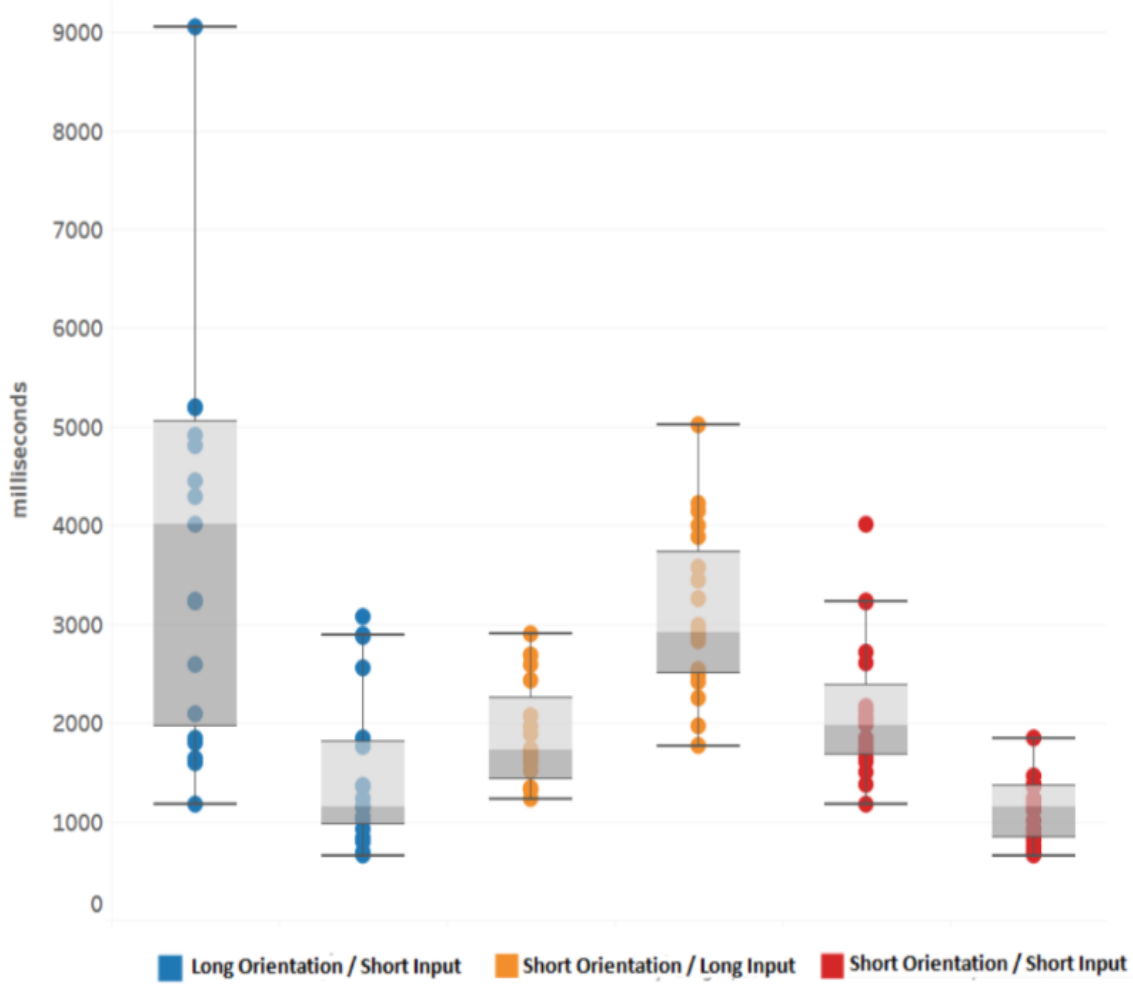
As mentioned earlier, in Section 4.1, the ratio *short/short* was meant to serve as a baseline to the time measurements. If we were to compare it to the two other ratios, we would notice that the average duration of their short *orientation phases* and short *input phases* are very similar to the baseline and that they did not differ substantially (see Figure 5.4).

Although, the ratios *short/long* and *long/short* were designed to have the same overall duration, results show that they had a temporal difference of 1176 ms, on average (see Figure 5.3). The combination *long/short* (6056 ms) had the longest duration, followed by *short/long* (4880 ms) and, lastly, *short/short* (2983 ms). Figure 5.4 shows that, on average, participants needed more time (1094 ms) to finish the long *orientation phase* of *long/short* than they needed for the long *input phase* of *short/long*. If we were to observe the maximum values of both ratios (see Figure 5.4), we would notice that one participant needed a maximum time of 9053 ms for long *orientation*. However, the remaining participants' time for long *orientation* did not exceed 5202 ms. This implies that for the majority of the time, long *orientation* and long *input* did not significantly differ from each other, according to their measurements. In contrast, the ratios *long/short* and *short/long* differed less notably, regarding their "short phases", meaning short *orientation* and short *input*. On average, they differed by 572 ms. Nonetheless, participants needed more time for the short *orientation phase* than they needed for the short *input phase* (see Figure 5.4).

5.4.2 *Users' Perception*

A qualitative evaluation of the ratios *long/short* and *short/long* was assessed through a questionnaire (see Appendix A). In the questionnaire, participants were asked to compare the ratios *short/long* and *long/short* to each other, in order to obtain a precise insight on which of both they generally preferred more. To assure that they had a clear conception of the mentioned ratios, they were given an descriptive illustration as an aid to refer to, as they filled out the questionnaire (see Appendix A.4).

First, participants were asked to evaluate both ratios separately, through five-point Likert scales (see Appendix A.2, questions 12-13). When participants were asked whether they found the searching process (**mental task**) of ratio *long/short* annoying, the answers were split between *agree* (42%) and *disagree* (42%). Three participants (16%) found no difference between the two combinations (see Figure 5.5). Most participants were able to memorize (84%) and enter (89%) the pattern (**practical task**) easily (see Figure 5.5).
In contrast, all participants disagreed that the search process in ratio *short/long* was



Long Orientation / Short Input	Maximum	Q1	Median	Q3	Minimum
Orientation	9053	5052	4011	1966	1174
Input	2892	1801	1149	965	658

Short Orientation / Long Input	Maximum	Q1	Median	Q3	Minimum
Orientation	2900	2250	1721	1425	1231
Input	5020	3729	2917	2505	1769

Short Orientation / Short Input	Maximum	Q1	Median	Q3	Minimum
Orientation	3232	2384	1982	1676	1174
Input	1845	1356	1151	836	658

Figure 5.4: A plotted representation of the time measurements for each ratio, presented in the study: *long/short* (Top); *short/long* (Middle); *short/short* (Bottom).

annoying. Moreover, all agreed that the pattern was easy to enter and 89% agreed that it was easy to memorize (see Figure 5.5).

Next, participants were asked to actively choose which ratio they preferred best in terms of certain given characteristics (see Figure 5.6). This evaluation of the ratios was also assessed through Likert scales (see Appendix A.2, A.3, questions 14-18). The majority of the participants (68%) found that *long/short* required more mental effort, about 16%

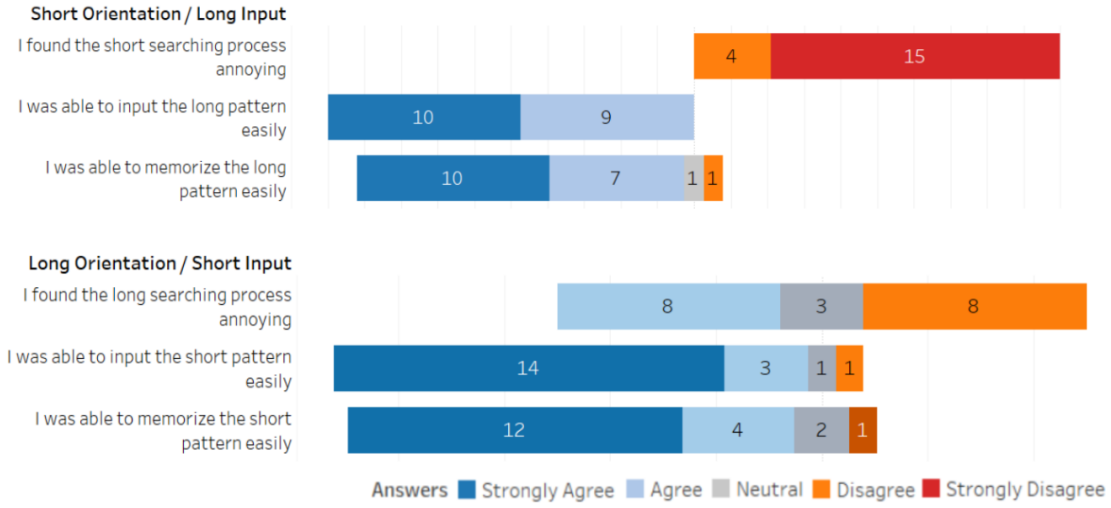


Figure 5.5: A representation of how participants evaluated each ratio separately in terms of this mental and practical task: *long/short* (Top); *short/long* (Bottom).

chose *short/long* and another 16% saw no difference between both ratios (see Figure 5.6). Moreover, about 79% voted for *short/long* as the easiest, followed by a 16% finding *long/short* easier, and 5% who saw no difference between the two (see Figure 5.6). Participants were also asked to chose the ratio, which they found took longer to find. All participants agreed that the pattern for *long/short* took longer to find (see Figure 5.6). In contrast, they were asked which pattern they found took longer to enter. Seventy-four percent chose *short/long*, 26% saw no difference, and no one chose *long/short*. Lastly, they were asked which combination they found was more efficient. The majority (58%) found that *short/long* was more efficient, followed by 26% who chose *long/short*, and 16% who saw no difference (see Figure 5.6).

If we were to compare the participants' estimation, regarding which ratio had the longest duration, to the actual time measurements, we will find that 32% (6) misestimated. In three of the six cases, the duration of *long/short* was falsely considered longer, in one case *short/long* was misestimated as longer and the remaining two participants saw no difference between the two. Nonetheless the majority of the participants (68%) estimated correctly, according to their performance.

Interestingly, only 11% (2) misestimated the ratio, which pattern took longer to find. In both cases *long/short* was chosen, although *short/long* was true. However, 89% estimated correctly. In contrast, 42% (8) misestimated the ratio, which pattern took longer to enter. In five of the eight cases, participants saw no difference between both ratios. In the remaining three cases, *long/short* was chosen, while *short/long* was true.

To get a clearer understanding of the participants' preferences, they were asked to declare which ratio they would prefer for the screen lock on their smartphone. They were advised to elaborate on their choice based on four given reasons to choose from (see Figure A.3, question 21): *It's more efficient / more secure / more difficult / challenging*[4].
Forty-two percent (8) of the participants preferred *long/short* (see Figure 5.7). Most frequent reasons given for choosing *long/short* were that is was *more secure* and *more difficult*.

4 Multiple answers were possible.

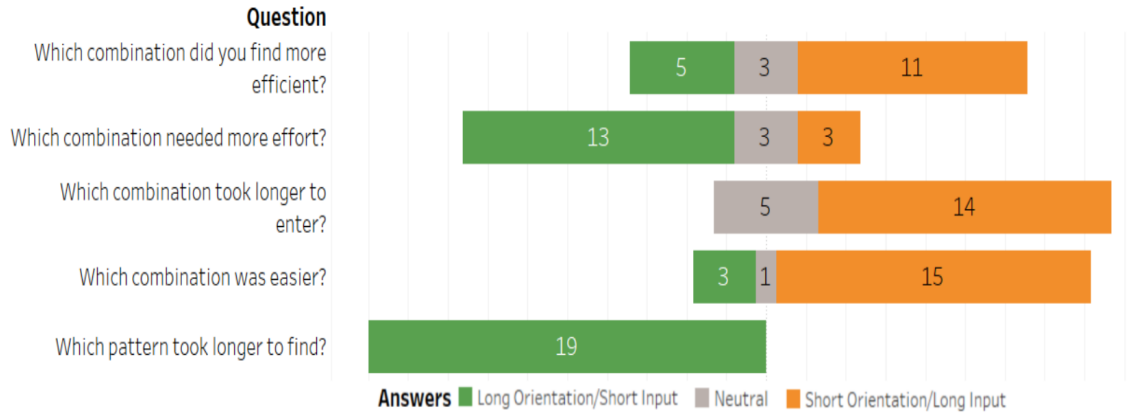


Figure 5.6: Participants were asked to compare the combinations *long/short* and *short/long* to each other by answering the questions above. These questions were answered using Likert scales.

Only one participant found that it was *more efficient* and only two found that it was *challenging*. Interestingly, one participant elaborated further on their choice and wrote that *long/short* also was more comfortable to use.

In contrast, 47% favored the ratio *short/long* and the most frequent reasons given were *more secure* and *more efficient*. The reasons *more difficult* and *challenging* were only given once, each. One participant elaborated that they would choose *short/long* because it is easier, for when they are tired. Eleven percent (2) chose neither of both ratios and elaborated on their choice in the following (see Figure 5.7):

- *"Short/Long is much easier because it's easier to find.*
  It's also much easier to copy => Insecure! I would prefer a mix [of both]."
- *"It don't mind which one, because their use will get easier over time. It really just depends on one's mood."*

As mentioned in Section 4.3.2, a form of *error-recovery* was included into the application with the intention of enhancing its ease-of-use. Although the main focus of our study, was to solely examine certain ratios of *orientation* and *input phases*, it was indispensable to analyze whether the *error-recovery* feature had an impact on the measured and perceived *orientation time*. For that, a question was added to the survey which only had to be answered if a participant encountered the *error recovery* feature during the interaction. Answers were assessed through a Likert-scale (see Figure A.3, question 20). Out of 19 participants, only 6 experienced the *error recovery* (see Figure 5.8)[5]. When asked whether the pop-up window feature helped them find the pattern faster, five of the concerned participants agreed and only one disagreed. Moreover, half of the concerned participants (3) disagreed that the pop-up window elongated the searching process. However, one agreed and two did not notice any difference. Lastly, when asked whether they found the pop-up window annoying, four disagreed, one agreed, and another was

5 We were able to obtain this information during the study, through the database view which was incorporated in the application (see Figure 4.9). If a participant had more than three "search-fails" in one of the levels, it meant that they encountered the *error-recovery* feature.

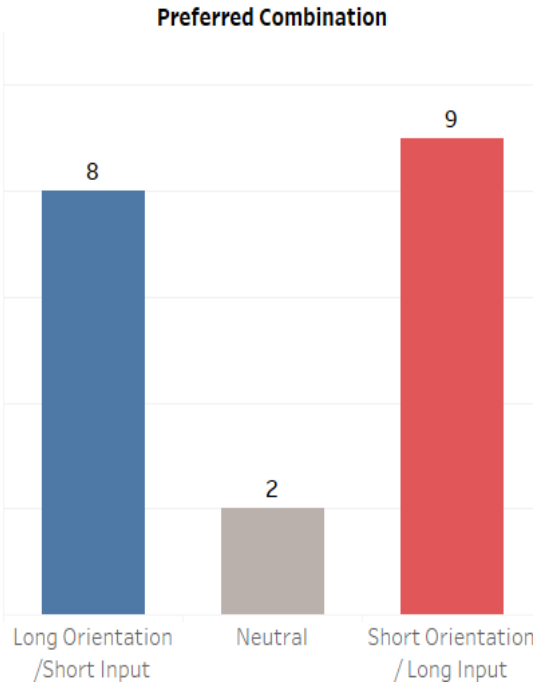


Figure 5.7: A histogram, representing our participants preferences regarding the combinations.

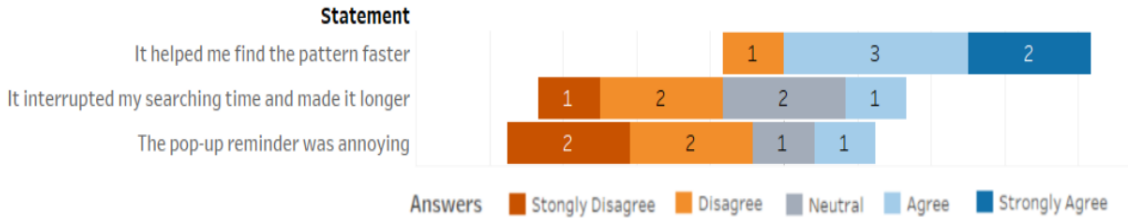


Figure 5.8: A representation of how participants evaluated the *error-recovery* feature of the application.

indecisive (see Figure 5.8). In order to see whether *error-recovery* had an impact on the concerned participants' performance, their quantitative data was examined. Luckily, the concerned participants never encountered *error-recovery* during the third level of each phase[6], which implies that the feature had no impact of their measured time. Nonetheless, the examination of the feature's effect still provided information on whether it's design was well accepted by participants, which is true for the majority of the participants.

6 As mentioned earlier, the first and second level of each phase in the application, were considered an exercise. Only the third levels of each phase were involved in the quantitative evaluation.

6 DISCUSSION AND LIMITATIONS

In this chapter, we will review and analyze the main results of the study (see Chapter 5), in relation to the recommendations proposed in Section 3.2.2. Based on these results, we will discuss the universality of Zezschwitz et al.'s [1] approach. Last, the limitations, which were faced during the design and procedure of the study, will be presented.

Analogous to Zezschwitz et al. [1], the main phases (*orientation* and *input*) were measured in the study. An improved approach was taken towards enhancing the accuracy of the time measurements, specifically those of *orientation time*. Thus one of the limitations of their approach was the inaccuracy of the *orientation time* measurements. The concept **FiPa** was specially designed to to prevent this issue.
Based on a further recommendation, the measurement of perceived efficiency was taken into consideration for the design of this study. Participants' perception of efficiency, regarding the ratios, was measured and assessed through a questionnaire. They were asked to directly compare the two main ratios *short/long* and *long/short* to each other, in terms of certain characteristics like mental effort, efficiency, preference, length of input, length of search and so on.

As explained earlier, the contrasting ratios *short/long* and *long/short* were designed to be asymmetrical in terms of their phase lengths[1]. The quantitative results showed that, on average, their overall length differed by 1176 ms. Thereby, *long/short* had the longest average duration of 6056 ms. Nonetheless, in the worst case, both ratios were relatively similar, regarding their long phases and their short phases. This shows that the design of the concept and the implementation of the ratios were suitable and successful for the purpose of this study. We were, therefore, able to prove our assumptions and observations (see Chapter 3), thus our used method and the resulting quantitative data, were similar to how we had desired for them to be.

In terms of perceived efficiency, participants were first asked to evaluate the **mental** and **practical tasks** of each ratio, separately. They were asked to rate the annoyance of each ratio's *orientation* and the simplicity to memorize, as well as input its corresponding pattern. Interestingly, the majority of the participants found, both, short and long pattern easy to memorize and to input (see Figure 5.5). However, the difference between both ratios was notable regarding the annoyance of their *orientation times*. While all participants disagreed that *short orientation* was annoying, the average opinion regarding the annoyance of *long orientation* was "neutral". Even if participants did not strongly incline towards a positive or negative opinion regarding the annoyance of *long orientation*, the results show a greater acceptance of *short orientation*. This observation indicates that participants had a greater acceptance for short *orientation time*.

1 Meaning "long orientation" had to have the same length as "long input" and "short orientation" had to have the same length as "short input".

As mentioned earlier, participants were asked to compare both ratios, based on certain characteristics. The majority of the participants (68%) found that *long/short* required more mental effort than *short/long* (only 16%). This implies that, although both ratios contained a complicated task[2], complicated **mental tasks** (long *orientation times*) seem to have stressed participants more than complicated **practical tasks** (long *input times*). Consequently, most participants (79%) agreed that the implementation of *short/long* was easier than *long/short* (only 16%). In addition, when participants were asked which of both ratios took longer to find and enter, the results indicated that participants were more sensitive towards the complexity of long *orientation phases* than they were towards *long input phases*. While all nineteen participants agreed that the pattern in *long/short* took longer to find than in *short/long*, only 74% agreed that the pattern in *short/long* took longer to enter. Through comparing participants' time estimates to the measured data, it was notable to see that they were right 89% of the time regarding the ratio which had the longest *orientation time*. However, less participants (57%) estimated correctly, regarding the ratio which had the longest *input time*. This shows that participants were more sensitive towards the time and mental effort needed to undergo the *orientation phase*. Thus less of them were able to distinguish between the length of short and long *input time*. Participants incline towards the ratio *short/long* was more notable when they were asked which ratio implementation they found to be more efficient. The majority leaned towards *short/long* (58%) and only 26% found *long/short* to be more efficient.

Based on these analyzed results, one might expect that, in general, participants would have had a greater incline towards *short/long* than towards *long/short*. However, when asked to chose one ratio implementation as a screen lock for their smartphone, this was not the case. Although 47% chose the ratio *short/long* for their screen lock, still 42% chose *long/short*. It is clear to see that there is not a significant difference regarding the preference of both ratios. However, we assume that participants who chose *long/short*, made their choice with regard to the potential security aspects of the ratio design, as the most frequently given reasons for *long/short* were "more secure" and "more difficult". Nonetheless, most participants chose *short/long* for their screen lock. The most frequent reasons given were "more secure", as well as "more efficient". These reasons imply a higher user-acceptance and preference for *short/long*, in terms of usability. The remaining 11% (2) did not choose either of both ratios, yet they gave interesting reasons why. One participant said that they preferred *short/long*, as it is easier. Yet, because it would be less secure, they would much rather prefer a combination of both ratios for their screen lock. This implies they would favor a concept that is not only easier to use, but that also assures to be secure enough to protect their smartphone. Another participant stated that it did not matter to them which one they chose, as they would get used to either ratio, with time. They added that the choice would depend, more specifically on one's mood. This opinion indicates that, for some, the usability of a concept is not only dependent of its design and implementation, yet could also be determined by the user himself and by the specific needs and preferences they might have in a particular situation. It would be interesting to thoroughly analyze this observation in the future.

To see whether there was a correlation between participants' ratio preferences and their personal screen lock choice, they were asked to share the type of authentication

2 The "long phases" of each ratio were meant to represent complicated tasks.

mechanism which they used and the length or complexity of their secret. We assumed that participants who used short and simple secrets, would choose *short/long*, and the ones who used longer secrets would choose the latter. However, we could not find any notable behavioral patterns.

All in all, the conducted study has shown that by "measuring all stages", it was possible to receive a more accurate conception of the ratios' measured performance. Combined with "measuring perceived speed" qualitatively, participants' perceptions and opinion appeared more comprehensible and justifiable during the evaluation [1]. By comparing participants' perception on the implementation of *long/short* and *short/long*, it was noticeable that the majority of participants favored the concept design, where *orientation time* did not exceed *input time*. Although *long/short* had a simple **practical task**, results showed that it did not compensate for complicated **mental task** which it presented [1]. This validates previous observations in the project which indicated that "*orientation time* should be kept as low as possible" for better user-acceptance [1].

The fact that more participants found *long orientation* to be longer than *long input*, validates that phase ratios should be "in favor" of the input phase. Reason being that users are less bothered by the required effort for accomplishing a complicated **practical tasks**, than they are of complicated **mental tasks**. Especially when mental tasks are randomized, as each one represents a unique challenge, which can not be simplified over time, through the strength of muscle memory (as with memorizing long secrets). In the concept **FiPa**, each grid differed from the other in all ratio implementations, yet the factor of randomization was more noticeable for *long/short*. The *traps*, which were uniquely set, complicated the search process even more. This is also a reason why participants had a stronger incline towards the orientation of *short/long*. This means that the inclusion of randomization in authentication concept designs is disliked by users, as it causes for longer *orientation times*. For that, it should be avoided or minimized as much as possible, as suggested by Zezschwitz et al. [1].

6.1 LIMITATIONS

Although **FiPa** was designed to emulate an authentication process in a lab setting, it is not clear whether participants' evaluation of the ratios might have differed if they had interacted with the concept in real-life scenarios[3]. As the concept was only used for a short period of time, there is a chance that participants' preferences and the study results might have differed.

Unfortunately, the study had to be conducted twice. The first study involved a wider and more versatile demographic, however, its quantitative results were not usable, by cause of an error in the implementation of the time measurements of the application. Sadly, the error was detected, afterwards, during the evaluation of the results. Consequently, an additional study had to be conducted and a new set of participants had to be recruited because the former participants were already familiar with the contents of the study and would have caused a bias in the results. The majority of the newly recruited participants were computer science students, as they had to be collected on short notice.

3 Meaning if the participants had used the implementation of the concept as an authentication mechanism for a certain period of time (similar to the study design of Zezschwitz et al. [1]).

This is another reason why the results of this study cannot be fully generalized, as most of the participants had an IT-background and were also familiar with the importance of smartphone security. The outcome of the study would have been more interesting and convincing, if our participants had a wider demographic and did not use screen locks on their smartphone. In combination with a longitude study, it would have been possible to obtain more detailed information on the perceived efficiency and the user-acceptance of the main ratios, represented in the concept. As mentioned in Chapter 2, the primary reason why smartphone users persist not to use a screen lock is due to their perceived inconvenience. It would have been interesting to find out, which of the ratio implementation had the potential of motivating users to use authentication mechanisms on their smartphone and improve their smartphone security behavior. Depending on their preference regarding the ratios it would have been possible to derive the true effect of *orientation time* and perceived efficiency. As a result a standard could be developed, to guarantee a enhanced user-acceptance and a higher perceived efficiency for future authentication concept propositions.

In the study, the questionnaire included a semantic differential with the intent to evaluate the aesthetics of the application. The intention was to examine how participants perceived the aesthetics of the application and to see whether their performance and preference was positively or negatively influenced by it. However, during the evaluation it was noted that these observations would exceed the scope of this thesis and distract from its true focus, namely the effect of orientation time on the perceived efficiency of authentication mechanisms.

We would like to note that our choice to measure the times for every third level of each phase, in the application, was not based on a study. Instead, we examined the quantitative data and calculated the amount of input errors made amongst all participants, for each level separately. We found that, in total, only 4 input errors were made in the first level, followed by 6 input errors in the second level and only 2 input errors in the third.

Lastly, we would like to mention that there remains one recommendation, which we were not able to validate. That is, "Optimize Context Switches" (see Section 3.2.2). Although the **mental** and **practical tasks** in **FiPa** were designed to be coherent and were intended complement each other, we did not lay focus on letting participants evaluate this feature of the concept.

7

CONCLUSION AND FUTURE WORK

The aim of this thesis, was to analyze how far the effects of certain factors, more specifically those of *orientation time*, might influence the perceived efficiency, and therefore the usability of smartphone authentication concepts. We based our assumptions and hypotheses on the ongoing study which was presented in Chapter 3. We took into consideration, a selection of improvements and approaches to provide proof for the observations and recommendations made by Zezschwitz et al. [1]. One of the improvements, was to represent all studied phase ratios in a single concept. The intention, behind this approach, was to obtain more precise and authentic opinions on the ratios, without having the representative concepts be an influencing factor on participants' preferences. Moreover, we decided to observe a pair of contrasting ratios (*long/short* and *short/long*) to observe the true effect that *orientation time* has on the user-acceptance of a concept, with regard to its *input time*. A quantitative evaluation of the times for each ratio, allowed us to assure that the ratio implementations were suitable for the purpose of our study. Measurements showed that both contrasting ratios were close to the baseline and that, in the worst case, their contrasting phases did not substantially differ in length. This aspect granted us the possibility to compare participants' perception of both examined phases: *orientation* and *input*. A qualitative evaluation showed that participants were more sensitive towards the length of *orientation time* than they were towards the length of input time. Therefore, they were able to estimate the duration of *orientation* more correctly than the duration of *input*. In summary, it could be said that *short/long* was rated more positively than *long/short*, as the majority of the participants agreed that it was more easy, efficient and that it required less mental effort. Our findings imply that, in general, users are less aggravated by long *input times* than they are by long *orientation times*. Moreover, they show that pairing short *input phase* with long *orientation phases* does not equalize the amount of mental effort needed for the ratio. Therefore, it is true that authentication concepts should consist of *orientation times* which exceed the length of their corresponding *input times*. This means that *orientation times* should truly be kept as short as possible. As the implementation of our concept **FiPa** contained a randomization feature[1], which was especially noticeable in the ratio *long/short*, it caused for longer orientation times. For that, randomization should be reduced as much as possible, to contribute towards increasing the perceived efficiency of an authentication concept. However, as randomization is generally used as a measure to increase the security mechanisms, this means that newer countermeasures are called for which, simultaneously, agree with the usability of a concept and also enhance its security feature. Moreover, we were able to confirm that users generally prefer short *orientation times* and that they are less bothered by longer *input times*, by discovering that the majority of our participants favored to use the ratio *short/long* for the smartphone's screen lock.

1 Thus overall, all grids in the application differed from each other, and mental tasks were complicated through uniquely set *traps* (see Section 4.2.2.3).

All in all, it is safe to say that our findings and the outcomes of our study represent further steps towards understanding how users understand and perceive the efficiency of authentication mechanisms. In addition, our discoveries have taken us one step closer towards creating a standard for the design of more efficient authentication mechanisms, as users' general likes and dislikes have been confirmed. In fact, our study has also drawn attention towards certain aspects which could also be considered in future research contributions. For instance, although we have found that users, generally prefer long *input times*, we can not conclude that they are completely satisfied with them, regardless their length and complexity. As mentioned in Chapter 2, the correct and secure use of password authentication mechanisms still remains an issue that has not yet been solved. Therefore the true limits of what users consider efficient, regarding *input time* should be specifically examined and, if necessary, alternative solutions should be considered. Furthermore, in order to thoroughly assess the universality of our observations, it would be interesting to conduct a longitude study, using a similar design approach to ours, with participants who do not use a screen lock on their smartphone. That way, one could examine whether our complementary findings remain true over longer periods of use and whether they have the ability of improving the security behaviours and habits of users. Depending on the outcomes of this proposed study, it would then be possible to even create a provisional design standard for authentication mechanisms. That way, current and newly developed authentication concepts could be compared and evaluated with more certainty and validity. Consequently, one could observe whether preset and improved design standards of authentication mechanisms successfully apply in all real-life situations and cases. Thus our results indicated that users' preference of a particular concept might depend on their current mood.

BIBLIOGRAPHY

[1] Designing efficient authentication mechanisms: There is more to efficiency than input speed.

[2] *Imagery, Memory and Cognition (PLE: Memory) - Essays in Honor of Allan Paivio*. Psychology Press, London, 2014.

[3] Anne Adams, Angela Sasse, and Peter Lunt. Making passwords secure and usable. 12 1999.

[4] Anne Adams and Martina Angela Sasse. Users are not the enemy. *Commun. ACM*, 42(12):40–46, December 1999.

[5] Khalid Airowaily and Majed Alrubaian. Oily residuals security threat on smart phones. In *Proceedings of the 2011 First International Conference on Robot, Vision and Signal Processing*, RVSP '11, pages 300–302, Washington, DC, USA, 2011. IEEE Computer Society.

[6] Yusuf Albayram, Mohammad Maifi Hasan Khan, Theodore Jensen, and Nhan Nguyen. "...better to use a lock screen than to worry about saving a few seconds of time": Effect of fear appeal in the context of smartphone locking behavior. In *Proceedings of the Thirteenth USENIX Conference on Usable Privacy and Security*, SOUPS '17, pages 49–63, Berkeley, CA, USA, 2017. USENIX Association.

[7] Mansour Alsaleh, Noura Alomar, and Abdulrahman Alarifi. Smartphone users: Understanding how security mechanisms are perceived and new persuasive methods. *PLoS ONE*, 12, 03 2017.

[8] Andreas Butz and Antonio Krüger. *Mensch-Maschine-Interaktion* -. Walter de Gruyter GmbH & Co KG, Berlin, 1. aufl. edition, 2014.

[9] Serge Egelman, Sakshi Jain, Rebecca S. Portnoff, Kerwell Liao, Sunny Consolvo, and David Wagner. Are you ready to lock? In *Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security*, CCS '14, pages 750–761, New York, NY, USA, 2014. ACM.

[10] Adrian Frutiger. *Signs and Symbols - Their Design and Meaning*. Watson-Guptill Publications, reprint edition, 1998.

[11] Marian Harbach, Alexander De Luca, and Serge Egelman. The anatomy of smartphone unlocking: A field study of android lock screens. In *Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems*, CHI '16, pages 4806–4817, New York, NY, USA, 2016. ACM.

[12] Marian Harbach, Alexander De Luca, Nathan Malkin, and Serge Egelman. Keep on lockin' in the free world: A multi-national comparison of smartphone locking. In *Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems*, CHI '16, pages 4823–4827, New York, NY, USA, 2016. ACM.

[13] 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 *10th Symposium On Usable Privacy and Security (SOUPS 2014)*, pages 213–230, Menlo Park, CA, 2014. USENIX Association.

[14] Taekyoung Kwon and Sarang Na. Tinylock: Affordable defense against smudge attacks on smartphone pattern lock systems. *Computers & Security*, 42, 11 2013.

[15] Douglas Nelson, Valerie Reed, and John Walling. Pictorial superiority effect. *Journal of experimental psychology. Human learning and memory*, 2:523–8, 10 1976.

[16] L. O'Gorman. Comparing passwords, tokens, and biometrics for user authentication. *Proceedings of the IEEE*, 91(12):2021–2040, Dec 2003.

[17] Bryan Payne and W. Edwards. A brief introduction to usable security. *Internet Computing, IEEE*, 12:13–21, 06 2008.

[18] Paulo Realpe-Muñoz, César A. Collazos, Toni Granollers, Jaime Muñoz Arteaga, and Eduardo B. Fernandez. Design process for usable security and authentication using a user-centered approach. In *Proceedings of the XVIII International Conference on Human Computer Interaction*, Interaccion '17, pages 42:1–42:8, New York, NY, USA, 2017. ACM.

[19] Angela Sasse and I Flechais. *Usable Security: Why Do We Need It? How Do We Get It?* 01 2005.

[20] Roland Schlöglhofer and Johannes Sametinger. Secure and usable authentication on mobile devices. *ACM International Conference Proceeding Series*, 12 2012.

[21] Symantec. Risks and potentials of graphical and gesture-based authentication for touchscreen mobile devices. 2012.

[22] Emanuel von Zezschwitz. Risks and potentials of graphical and gesture-based authentication for touchscreen mobile devices. November 2016.

[23] Emanuel von Zezschwitz, Alexander De Luca, Bruno Brunkow, and Heinrich Hussmann. Swipin: Fast and secure pin-entry on smartphones. In *Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems*, CHI '15, pages 1403–1406, New York, NY, USA, 2015. ACM.

[24] Emanuel von Zezschwitz, Alexander De Luca, Bruno Brunkow, and Heinrich Hussmann. Swipin: Fast and secure pin-entry on smartphones. In *Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems*, CHI '15, pages 1403–1406, New York, NY, USA, 2015. ACM.

[25] Emanuel von Zezschwitz, Paul Dunphy, and Alexander De Luca. Patterns in the wild: A field study of the usability of pattern and pin-based authentication on mobile devices. In *Proceedings of the 15th International Conference on Human-computer Interaction with Mobile Devices and Services*, MobileHCI '13, pages 261–270, New York, NY, USA, 2013. ACM.

[26] Emanuel von Zezschwitz, Anton Koslow, Alexander De Luca, and Heinrich Hussmann. Making graphic-based authentication secure against smudge attacks. In *Proceedings of the 2013 International Conference on Intelligent User Interfaces*, IUI '13, pages 277–286, New York, NY, USA, 2013. ACM.

[27] Dan Zakay and Richard Block. Prospective and retrospective duration judgments: An executive-control perspective. *Acta neurobiologiae experimentalis*, 64:319–28, 02 2004.

A APPENDIX

A.1 QUESTIONNAIRE

Questionnaire

User - ID _____

1. What is your gender? _____
2. What is your age? _____
3. What is your Profession/Job? _____
4. Do you have an IT-related background?
   - ☐ Yes
   - ☐ No
5. Do you currently own a Smartphone?
   - ☐ Yes
   - ☐ No
6. Do you currently use a screen lock for your Smartphone?
   - ☐ Yes
   - ☐ No

   Please give a reason for using/not using a screen lock.

   _____
7. What do you like and dislike about screen locks in general?

   _____

   _____
8. Please select the form of security that you are currently using for your Smartphone? (If you use biometric authentication, please select your fallback method)
   - ☐ PIN
   - ☐ Password
   - ☐ Android Pattern Lock
   - ☐ None of the above, but:_____
   - ☐ I have none
9. **If you use the Android Pattern Lock.**
   How many nodes does your current pattern consist of? _____
10. **If you use a Password Lock.**
    How many characters does your current password consist of? _____

    What type of characters does your current password consist of? (Multiple answers possible)
    - ☐ upper case letters *("ABC…")*
    - ☐ lower case letter *("abc…")*
    - ☐ numbers *("123…")*
    - ☐ special characters *(" (,), -, _ , !, ?, …")*
    - ☐ blank spaces *(" ")*
    - ☐ emojis

Figure A.1: Questionnaire to our study, page 1.

11. Please rate the app on the following traits.

Unstructured	○	○	○	○	○	Structured
Playful	○	○	○	○	○	Boring
Annoying	○	○	○	○	○	Pleasing
Fascinating	○	○	○	○	○	Banal
Understandable	○	○	○	○	○	Confusing
Nice	○	○	○	○	○	Ugly

12. Please rate "Short search / Long Pattern" according to the following statements.

	Strongly disagree	Disagree	Neutral	Agree	Strongly agree
I was able to memorize the long pattern easily					
I found the short searching process difficult					
I was able to input the long pattern easily					

13. Please rate "Long search / Short Pattern" according to the following statements.

	Strongly disagree	Disagree	Neutral	Agree	Strongly agree
I was able to memorize the short pattern easily					
I found the long searching process difficult					
I was able to input the short pattern easily					

14. Which combination was easier?

	Strongly agree	Agree	Neutral	Agree	Strongly agree	
Long search / Short pattern	○	○	○	○	○	Short search / Long pattern

15. Which combination was more efficient?

	Strongly agree	Agree	Neutral	Agree	Strongly agree	
Long search / Short pattern	○	○	○	○	○	Short search / Long pattern

16. Which combination needed more mental effort?

	Strongly agree	Agree	Neutral	Agree	Strongly agree	
Long search / Short pattern	○	○	○	○	○	Short search / Long pattern

Figure A.2: Questionnaire to our study, page 2. In the survey ratios were referred to as "combinations" for easier understanding. Refer to figure A.4 to understand the used descriptions of for each ratio.

17. Which pattern took longer to find?

	Strongly agree	Agree	Neutral	Agree	Strongly agree	
Long search / Short pattern	○	○	○	○	○	Short search / Long pattern

18. Which pattern took longer to enter?

	Strongly agree	Agree	Neutral	Agree	Strongly agree	
Long search / Short pattern	○	○	○	○	○	Short search / Long pattern

19. Which combination took longer in general?

	Strongly agree	Agree	Neutral	Agree	Strongly agree	
Long search / Short pattern	○	○	○	○	○	Short search / Long pattern

20. [Please, answer this question, only if it applies to you.]

	Strongly disagree	Disagree	Neutral	Agree	Strongly agree
I found the pop-up was annoying					
It interrupted my searching time and made it longer					
It made me find the pattern faster					

21. Imagine you had to choose one of the combinations as your screen lock. Which one would you choose?

	Strongly agree	Agree	Neutral	Agree	Strongly agree	
Long search / Short pattern	○	○	○	○	○	Short search / Long pattern

Please give a reason for your choice. (Multiple answers possible)

- ☐ It's more secure
- ☐ It's more efficient
- ☐ It's more difficult
- ☐ It's challenging
- ☐ other: _____

22. Let us know what you **liked / disliked** about the study and/or the app. Feel free to add any suggestions/comments, **thank you**.

Figure A.3: Questionnaire to our study, page 3. In the survey ratios were referred to as "combinations" for easier understanding. Refer to figure A.4 to understand the used descriptions of for each ratio.

A.2 ILLUSTRATION

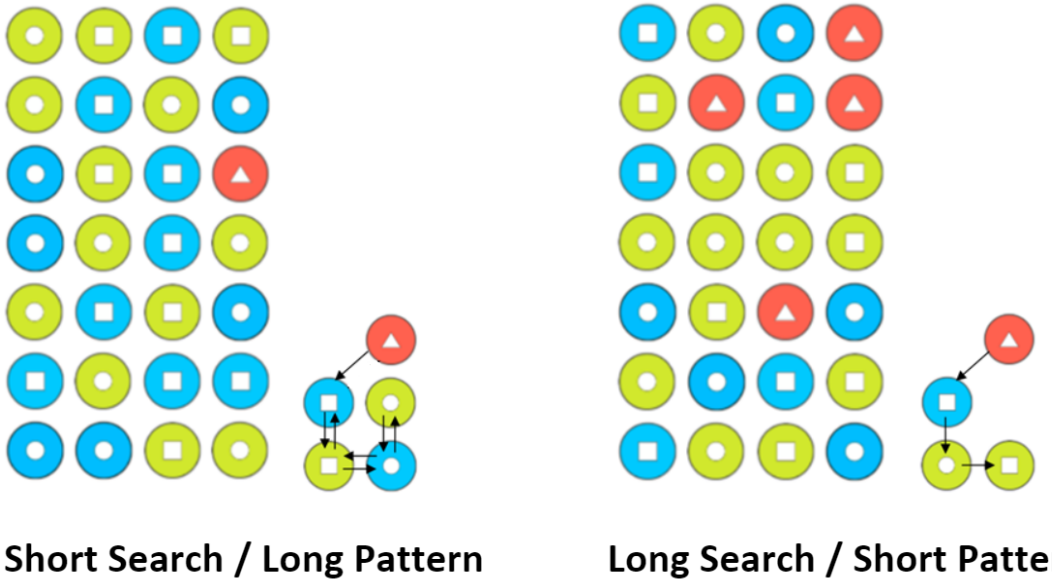


Figure A.4: This is an illustration which was given to the participants as an aid to help them remember the contrasting ratios, as they filled out the questionnaires. The description of the ratios was simplified for easier understanding: *short orientation/long input* (Left), *long orientation/short input* (Right).