# "I'm going to try her birthday": Investigating How Friends Guess Each Other's Smartphone Unlock PINs in the Lab

Elena Korkes
The George Washington University
Washington DC, USA
ekorkes@gwu.edu

Collins W. Munyendo
The George Washington University
Washington DC, USA
cmunyendo@gwu.edu

Alvin Isaac
The George Washington University
Washington DC, USA
aisaac@gwu.edu

Victoria Hennemann
The George Washington University
Washington DC, USA
vrhennemann@gwu.edu

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

## ABSTRACT

Despite the recent popularity of biometrics for smartphone unlocking, knowledge-based authentication schemes (e.g. PINs) remain crucial for smartphone security, and are typically required when the device restarts or the biometric fails. Previous studies on PINs assume an attacker without any personal information about the victim, with many often speculating that an attacker with some personal information of the victim (e.g., a friend) might fare better when guessing their smartphone unlock PINs. However, no study has investigated this yet, despite friends or partners being those most likely to attempt PIN guessing. In this work, we explore how attackers that have some personal information or relationship with the victim guess smartphone unlock credentials by recruiting 9 pairs of participants (n = 18 ) that have some relationship to guess each others' PINs or passwords in an in-person, lab experiment. We find that most participants' initial guessing strategies are birthdays as well as modifications of these birthdays, followed by geometric patterns and repetitions. In contrast, most participants indicated they would try random numbers or common PINs for strangers. While no participant was able to guess another participant's PIN, about half indicated they would not change their PIN or password even if it was guessed by their study partner. We additionally combine participants' guesses to guess PINs selected in a prior study, finding that our participants' guesses perform similarly to the optimized simulated attackers used in previous work. We conclude with takeaways and interesting directions for future research.

**ACM Reference Format:**
Elena Korkes, Collins W. Munyendo, Alvin Isaac, Victoria Hennemann, and Adam J. Aviv. 2024. "I'm going to try her birthday": Investigating How Friends Guess Each Other's Smartphone Unlock PINs in the Lab. In *The 2024 European Symposium on Usable Security (EuroUSEC 2024), September 30-October 1, 2024, Karlstad, Sweden.* ACM, New York, NY, USA, 15 pages. https://doi.org/10.1145/3688459.3688461


*EuroUSEC 2024, September 30-October 1, 2024, Karlstad, Sweden*

ACM ISBN 979-8-4007-1796-3/24/09…$15.00
https://doi.org/10.1145/3688459.3688461

## 1 INTRODUCTION

Smartphones are increasingly playing an important role in our everyday lives. These devices store a lot of personal and sensitive information that must be protected [18]. This includes messages, emails, photos, banking information and accounts, etc. There has been a lot of prior work investigating the security of user-selected 4- and 6-digit PINs for smartphone unlock, finding that most users select memorable PINs, including their birthdays [13] as well as simple PINs including repetitions and geometric patterns [11, 21, 22, 26]. This makes these PINs susceptible to guessing. Other research has additionally shown that longer, human-chosen 6-digit PINs do not necessarily offer meaningful security improvements over 4-digit PINs [21, 22, 26], despite their additional usability burden.

However, most of this research has assumed an attacker that has no prior information about the victim. In fact, most of previous work [21, 22, 26] only speculates that an attacker that knows the victim will utilize this knowledge, e.g. their birthdays, anniversaries etc, to improve their guessing performance. The threat posed by those with knowledge about the victim (e.g., friends and family) is particularly interesting to explore as these are the people who are most likely to have physical access to these devices and attempt guessing. In a recent study conducted by Bailey et al. [11], many participants admitted they had tried to gain unauthorized access to a device belonging to their friend, partner, or other close person.

While targeted, optimized, offline guessing has been explored for passwords more broadly [15, 27, 34], we are the first, to the best of our knowledge, to investigate how attackers with some prior information or knowledge about the victim guess their smartphone unlock PINs via an in-person lab experiment. We primarily seek to answer the following three research questions[1]:

**RQ1**: How do users guess smartphone unlock PINs when they have some personal information about the victim? What strategies do they use? How effective are these strategies?

**RQ2**: How effective are participants' PIN guesses against other user-selected PINs? How do these guesses perform compared to other attackers used in previous work?

**RQ3**: What are users' concerns and perceptions about the security of their smartphone unlock PINs?

[1] A majority of our study participants were using PINs to unlock their devices, and hence our focus on PINs for our research questions.

To answer these research questions, we designed a four-part, in-person study. We recruited nine pairs of participants ($n = 18$) with some sort of relationship with each other e.g., friends, classmates etc, but who did not know each other's PIN, pattern, or password. In the first part, we asked them about their relationship, as well as how long they had known each other. This part of the study was done with both participants together. For the next part of the study, we separated participants into two different rooms, with one researcher present in each room. After asking them basic demographic questions including their age and gender, we next asked them to lock their phones before swapping these devices. Participants then had 10 minutes in total and up to 5 guesses to try and guess their study partner's PIN, pattern, or password. We restricted participant guesses to 5 to prevent the phones from getting locked for long durations of time as a result of many failed unlock attempts. We noted participants' strategies throughout. Afterward, we conducted semi-structured interviews with participants in the third portion of the study to learn more about their strategies for guessing, as well as their perceptions of their smartphones' security. We also showed them the guessing attempts made by their study partner, and inquired how close they were to guessing their PINs. These were all done with participants still separated. Lastly, we debriefed participants in the last part of the study together, informing them whether their PIN had been guessed and steps to follow in updating their PIN, password, or pattern if they chose to.

We find that most participants indeed try to use their study partner's prior knowledge in guessing their PINs, with most of participants' initial guesses being birthdays or some variations of these birthdays, followed by repetitions and geometric patterns on the keypad. Even though most participants admitted to using some variation of their birthdays as their PINs, all participants were surprisingly not able to guess their partner's PIN, with only one participant getting close. The various combinations of birthdays coupled by the throttling implemented on iOS and Android show that it might actually not be that trivial to guess PINs, even for attackers with a relationship or some prior knowledge about the victim. Most participants anticipated that they may fare better against strangers because most people tend to use common PINs. To explore this, we combined all the PIN guesses from participants and used them to guess PINs collected in a recent study by Bailey et al. [11]. We find that these guesses perform similarly to the optimized simulated attackers used in previous work.

Interestingly, about half of participants indicated they would not change their PIN or password even if it had been guessed by their study partner. Often, participants pointed to the trust they have developed with their study partner, or the usability drawbacks of memorizing a new PIN as the reasons for not updating their PINs. While prior work has speculated that knowledge of the victim is likely to increase the guessing success rate for unlock PINs, our results suggest that it may in fact not be straightforward to guess PINs even with prior knowledge of the victim. We discuss our results further and offer promising directions of future work that can further protect end users' smartphone unlock PINs.

## 2 RELATED WORK

There has been significant work aimed at understanding users' attitudes and preferences for locking their smartphones. Throughout this research, participants have provided a range of reasons why they choose (or not) to have extensive security precautions on their smartphones [1, 17]. On one hand, people want privacy, with some concerned about anyone gaining access to their phone; others are only concerned about strangers [17]. At the same time, some participants choose not to lock their smartphones, with the biggest reason for this being convenience [1, 17]. The inconvenience of changing PINs is also a theme we observe in our study.

Research surrounding smartphones' security in general is also prevalent, particularly for Android unlock patterns [5–7, 25, 31], alpha-numeric passwords [24, 30], PINs [14, 21, 22, 26], and LG knock codes [29]. Pattern-based locks, for example, provide hundred of thousands of options. However, so many individuals have been found to frequently use patterns that start from the top left corner and end at the bottom right [4, 7, 20, 25, 31, 33], making them vulnerable to shoulder surfing attacks [8–10, 16, 32] and other guessing attacks. Similarly, while PINs have many possible combinations, users also select them non-uniformly. This means that many user-selected PINs are susceptible to guessing attacks [13, 21, 22, 26].

Researchers have also explored the factors that influence users' PIN selection and the prevalence of PIN reuse [12, 14, 19], finding that most users prioritize convenience over security. In their study, Casimiro et al [14], found that most users draw inspiration for their PINs from dates that are important to them, for instance anniversaries. Furthermore, users frequently reused these PINs across multiple devices and accounts [14]. Similarly, Bonneau et al. [13] found that many users draw inspiration from their birthdays when creating PINs for their banking accounts. Unfortunately, this leaves many users vulnerable when they lose their wallets due to their personal information, including birthdays, often present on other documents contained in the wallet. Using birthdays for PINs is a theme we also observe in our study.

To nudge users to select more securely, blocklists have been employed where users are not allowed to select certain, common PINs. However, Market et al. [22] discovered that the small blocklist size in use on iOS was not effective, and proposed that the 4-digit PIN blocklist should include 1000 of the most popular PINs in order to be effective. For Android unlock patterns, Munyendo et al. [25] recommend blocking about 100 common patterns for a good balance between security and usability of unlock patterns on Android. Other proposals have suggested the use of 6-digit PINs over 4-digit PINs. However, recent studies have shown that 6-digit PINs offer extremely limited security benefits over 4-digit PINs, despite their additional usability burdens to end-users [21, 22, 26]

Our study is most closely related to work done by Bailey et al. [11]. In their online, survey-based study, Bailey et al. recruited 210 participants via Prolific, with half of them assigned to the 4-digit PIN treatment, and another half assigned to the 6-digit PIN treatment. Participants were first asked to select a secret PIN based on their treatment, then provide five guesses of what they believed other participants in their treatment had chosen. Participants received a monetary bonus if they successfully guessed a PIN selected by another participant in the study. While interesting and useful,

this study focuses on how strangers guess PINs, and does not take into account prior knowledge that close friends or partners might leverage when guessing PINs. This threat model is important to explore as close friends and partners are the ones most likely to have physical access to these devices, and subsequently attempt PIN guessing. In fact, Bailey et al. [11] found that a lot of participants had tried to guess their partner's or friend's PIN at some point. To fill this gap, our study therefore recruits pairs of participants with some relationship with each other for an in-person study to explore the strategies they use in guessing PINs, patterns, or passwords. We also explore their concerns and perceptions of their unlock PINs.

## 3 METHODOLOGY

In this section, we first describe the structure of our experiment, followed by our approach to recruitment and data analysis. Lastly, we detail the limitations and ethical considerations of this work.

### 3.1 Experiment Structure

To explore how people guess smartphone unlock PINs, passwords, or patterns when they have some personal information or relationship with the victim, we designed a four-part experiment where pairs of participants with a personal relationship (e.g. friends, classmates, teammates) attempted to guess each others' PINs, passwords, or patterns. We also inquired about participants' guessing strategies. We describe these four parts below:

*3.1.1 Consent and Knowledge of Each Other.* We started by briefing participants about the study and its purpose, including common terminology we would use during the study. We also informed participants that we would be audio-recording them. Once participants had consented, we asked them how well they knew each other, in what contexts, and for how long (**K1**) [2]. Participants completed this portion of the study together.

*3.1.2 Demographics and Main Experiment.* To ensure research integrity and confidentiality, we separated[3] participants before asking them individual demographic questions including their age, level of education, identified gender, and smartphone type and operating system (**D1** - **D6**). With participants still separated, we proceeded to the main experiment. First, the researchers asked participants to lock their smartphones and hand them to the researcher. The researchers then proceeded to swap the phones such that each of the participants had the other participant's phone. For the experiment, participants had up to five attempts at unlocking their study partner's device by guessing their PIN, pattern, or password. We restricted participant guesses to five to prevent the phones from getting locked for long durations of time as a result of many failed unlock attempts. We based this decision on iOS because at the beginning of the study, iOS devices allowed a user to continue inputting a PIN on the fifth failed attempt. However, these devices begin locking for some extended duration on the 6th failed attempt, i.e., for 1 minute after the 6th failed attempt, and 5 minutes after the 7th failed attempt. In the process of doing the study, however, Apple updated this policy for delays to start occurring after the 4th failed attempt. Hence, a total of 7 participants were only able to make 4 guesses as a result of this. We asked participants to speak and think out loud about their thought process, particularly informing the researchers of any guesses they wanted to make and the reasons for making those guesses throughout. Participants had 10 minutes in total for this task.

*3.1.3 Post-Experiment Interview.* Once participants had exhausted their guessing attempts, we conducted semi-structured interviews individually to learn more about their guessing strategies. We centered our questions around what their main strategy was (**Q1**) and whether they believed that this strategy reflects how others would try to guess their own unlock credentials (**Q2**). We then asked participants about their prior knowledge of their study partner, including birthdays, anniversaries, favorite numbers etc (**Q5**). Our next set of questions inquired about whether participants expected to succeed or fail, and factors that contributed to their expectation (**Q6** - **Q10**). After asking participants whether they would change their unlock PIN, pattern, or password if it was guessed by their partner (**Q13**), we presented them with the attempts made by their study partner and asked how close their study partner was to guessing their PIN, pattern, or password (**Q14**) as well as their perceptions of their PIN, pattern, or password security (**Q15**). Finally, we asked participants about their lock screen settings and their thoughts and feedback on the study (**Q16** - **Q21**).

**Table 1: Demographics of participants. Refer to Table 2 in the Appendix for more fine-grained details of participants.**

| | | No. | % |
|---|---|---|---|
| **Gender** | Female | 10 | 55.6 |
| | Male | 7 | 38.8 |
| | Other | 1 | 5.6 |
| **Age** | 18 - 21 | 8 | 44.4 |
| | 22 - 25 | 8 | 44.4 |
| | Over 25 | 2 | 11.1 |
| **Education** | Some College | 8 | 44.4 |
| | Bachelors | 8 | 44.4 |
| | Masters | 2 | 11.1 |
| **Operating System** | iOS | 17 | 94.4 |
| | Android OS | 1 | 5.6 |

[2] In the interview guide available in the Appendix, **K1** are questions about participants' knowledge of each other, **D1** - **D6** are participants' individual demographic questions, and **Q1** - **Q21** are the main interview questions for the study.

[3] This separation involved moving participants to different physical rooms. For every experiment, we had at least two researchers that conducted this process in parallel with the two participants, swapping phones when needed.

*3.1.4 Study Debrief.* Lastly, we debriefed participants together, informing them whether their study partner had been able to unlock their device. We also provided them with information on how to change their lock screen settings, particularly their password, PIN, or unlock pattern if they so wanted to change them.

## 3.2 Recruitment and Demographics

We recruited participants by placing posters and flyers (see Figure 2 in the Appendix) at various strategic locations in our university (e.g. on elevators, entrances, bulletin boards etc.). We also posted about the study in various Discord and WhatsApp groups as well as on Craiglist. On the recruitment flyers and posters, we required participants to sign up in pairs with someone they knew or had a close relationship with, but did not otherwise know their PIN, pattern, or password. Additionally, we required both participants to be using a PIN, pattern, or password on their smartphone. Participants that signed up and indicated they did not use an unlock scheme, or knew their partner's PIN or password were not eligible. In total, we recruited 9 pairs of participants ($n = 18$). Each participant was compensated $10 via a virtual gift card for completing the 30-minute in person experiment. Our study population comprised primarily younger, female-identifying participants with college education. Seventeen participants were using PINs, with only one participant using an alphanumeric password on their device. Table 1 has the full demographic information of participants.

## 3.3 Data Collection

Prior to conducting the main study, we piloted the experiment with four different pairs of participants, using feedback from these pilots to enhance the script for the main study. For instance, we updated the main interview guide to show participants guesses that their partners had made and then asking them how close their partners were to guessing their PIN, pattern, or password. We begun data collection for the main study in November 2022, continuing through April 2023. The experiment took place in a publicly accessible building in our university, with two rooms always reserved for separating participants for the main part of the study. All interviews were audio-recorded and transcribed by our institutional Zoom accounts. We manually reviewed and fixed any errors in the transcripts. We also took comprehensive notes throughout. We strived to recruit as many participants as we possibly could. However, we note that most participants started gravitating towards the same set of guessing strategies. Therefore, a total of 18 participants was likely sufficient to highlight common guessing strategies.

## 3.4 Data Analysis

To qualitatively analyze the interview transcripts and notes [28], three researchers collaboratively coded two transcripts together to develop a primary codebook. Then, two researchers used this codebook to independently code 10 of the remaining transcripts (55.5% of the data), meeting frequently to resolve differences and make updates to the codebook. The researchers also used these meetings to discuss major themes they noted from the study, following best practices for qualitative research [23]. Once the codebook was consistent, the primary coder finished coding the remainder of the transcripts. Our qualitative results presented in Section 4 are based on the primary codebook available in Appendix B. Since most of our results are qualitative, we caution against drawing any generalizability from these findings. Additionally, we use quantifiers such as most (more than half of participants), several (many participants, but not more than half), and some (a few participants) when reporting our results. We use these quantifiers, rather than counts, to avoid implying generalizability.

## 3.5 Limitations

Our study has several limitations. First, our sample size is relatively small as it was challenging to both recruit and schedule interviews with two participants and two researchers simultaneously. Additionally, our participant population predominantly consisted of younger and well-educated individuals. However, as is typical with qualitative work, we do not make any attempts to generalize our results. At the same time, we argue that our exploratory results highlight some strategies of how people think about and guess PINs, patterns, or passwords when they have some prior information of the victim. While we were interested in how people guess both PINs, patterns, and passwords across various devices, most of our participant devices were iPhones, with PINs the most frequently used authentication mechanism. Thus, future work is needed to explore how people guess passwords and unlock patterns, especially on Android devices. During our study, an Apple update required iPhones to lock after four failed PIN or password attempts, instead of the traditional five attempts. As a result, some of the participants were only able to make four guesses during the experiment portion of the study. Nonetheless, we were still able to learn how these participants guessed the PINs, particularly their most prioritized guessing strategies and attempts.

## 3.6 Ethical Considerations

This study was approved by our Institutional Review Board (IRB). Due to the nature of the study, we took several measures to protect participants. Foremost, we fully informed participants about the study and its purpose. We also made them aware that they would be required to hand over their locked device to a researcher who would then hand it over to their study partner. We encouraged participants to opt out if they were not comfortable doing so. Before handing over their locked phones to the researcher, we asked participants to place their devices on airplane mode to limit any harm that may be caused by access of their messages or other sensitive notifications by their study partner during guessing.

When guessing, we asked participants not to exceed five guesses to prevent any harm that might be caused by extended lockout periods on the device (see Section 3.1 for more details). We further instructed participants that in case they were able able to guess their study partners' PIN, password, or pattern, they should immediately hand over the phone to the researcher to avoid accessing their partner's personal information. Before making any guessing attempt, participants had to tell the researcher the guess that they were making, and their reason for making that guess.

We also sought explicit permission from participants to record audio throughout the study. Following the experiment portion of the study, we debriefed participants to inform them if their study partner was able to gain unauthorized access to their device. We

also provided information on how to change their PIN, pattern, or password on both Android and iOS if participants so chose to. Some participants inadvertently disclosed their actual smartphone PINs to us during the experiment portion of the study as they reflected upon their own as well as their partner's guessing strategies. Note, our goal was not to collect participants' actual PINs, but only their offensive PINs. Thus, to minimize any harm that may be caused by unauthorized access to the study data, we removed participants' actual PINs that were disclosed from our study data during transcription.

## 4 EXPERIMENTAL RESULTS (RQ1 & RQ3)

In this section, we first detail participants' authentication mechanisms and their guessing strategies for their partners' locked smartphones, followed by a reflection of how these strategies would change if their study partner was a complete stranger. Afterward, we discuss participants' expectations for success as well as their overall perceptions of their smartphones' security. When presenting participant quotes, every pair of participants are represented by the same participant number. For example, P01A and P01B represent the first two participant pairs, with P01A being the first participant and P01B being the second participant.

### 4.1 Authentication Mechanisms and Guesses

In our study ($n = 18$), most participants were using PINs to unlock their devices, similar to observations from previous work [21, 22, 25, 26]. Out of 18 participants, 17 were using PINs, with only one participant using an alpha-numeric password. Expectedly, no participant was using an Android unlock pattern as a majority were iPhone users. Of the 17 participants that were using a PIN, 10 were using a 6-digit PIN while 7 were using a 4-digit PIN. The popularity of 6-digit PINs is likely because of Apple asking users to select 6-digit PINs by default since iOS 17 [26].

As mentioned in Section 3.1, there was a policy change at Apple in the course of the study that introduced lock delays after the 4th attempt, down from the 5th attempt when we started data collection. As a result, out of the 17 participants using PINs, only 10 made 5 guessing attempts, with 7 participants making only 4 guesses. Nonetheless, this yielded a total of 78 guesses. Unfortunately, one guess was not legible, and hence we ended up with 77 guesses in total. We discuss the strategies behind these guesses next.

### 4.2 Strategies for Guessing

There are many different ways in which individuals may attempt to gain unauthorized access to a locked smartphone. We closely looked at participants' guessing strategies during the experiment and asked them to further explain these strategies during the post-experiment interview.

*4.2.1 Guessing Strategies Against Friends.* Throughout the experiment, participants frequently sought to leverage their knowledge of their study partner and any accessible information on the phone to enhance their attempts at gaining access to their partner's device. During the post-experiment interview, we asked participants to elaborate on their main guessing strategy when attempting to unlock their partner's device (**Q1**).

Among the various guessing strategies employed by friends or partners, *birthdays* were the most common strategy, followed by *geometric patterns*, *repetitions*, and *usability*. When we looked at the individual guesses, 34/77 of the guesses followed some variation of what participants believed was their study partner's birthday. Often, participants indicated that they had used similar techniques when selecting their own PINs. For example, P02A said that the:

> "first thing I will try to do is basically, try to assemble the password with his date of birth. And this is because mine is kind of related to my date of birth, so I expect everyone to have a similar pattern."

Following the same strategy, P04A said that they "think majority of the people, they will be keeping their birthdays or their friends' birthdays." When making their first guess, P07B stated that they were "going to try her birthday." Similarly, P06B said that they "know her birthday is July 8th 2000. So I'm gonna try *070800*." Overall, we find that participants frequently relied on prior knowledge of their partners' birthdays when guessing their PINs.

At the same time, some participants did not know their partners' birthdays and attempted to find this information in several ways. For instance, some participants looked through cards such as driver's licenses that people often carry on the back of their phones as elaborated by P06B:

> "[I will] look at the cards on the back of her phone. I got a credit card. So credit card, license, and a [university] ID. I think I might go onto the license and try something there."

Participants also attempted to guess unlock PINs by following geometric patterns; this approach was used in 16/77 guessing attempts, as explained by P06A:

> "I feel like most people tend towards like patterns and dates that they remember because those are all memorable numbers. And then I also have like family members and stuff who just do like patterns."

Often, participants mentioned trying patterns that can be made when entering PINs. P07A elaborated this as follows: "I mean like *2468* makes kind of like a diamond shape, which is kind of cool. So maybe I'll just try that." This was also the case for passwords, with P07B stating:

> "I feel like people, like, when you're making phones' [password], like, assume it'll be like the middle like, go down the middle row, or something like that."

After patterns, repetition were the third most common strategy, with 12/77 guesses being repetitions. Most participants that used repetitions indicated having observed other people use such strategies for their PINs. For instance, P01A stated that "I see some people just put one number. So I just tried that, but it did not work." P05A added that "my first attempt is obviously *0000* because, as far as it is the most common password, people will keep in their phones."

Lastly, the fourth most common strategy that participants employed was usability, i.e., a PIN that is easy to enter; this accounted for 11/77 guesses made by participants. For instance, P03A said that "I'll go in a straight line down the middle, because I feel like some people like easy access." Echoing this, P09B indicated that their study partner "is just a simple person. I don't think she will

use a complicated number. So, I will do one until 6." In other words, this participant's guess was *123456*.

Other strategies that were mentioned by several participants included *other important numbers*, *favorite numbers*, and *colors*. For example, P06B knew that their study partner "graduated college in 2022. I'm gonna try *070822*." P07A, on the other hand, tried a religious clue: "maybe it's Christmas. I know that she's Catholic."

In **Q4** and **Q5**, we additionally asked participants if any other information, including anniversaries as well as other important dates and numbers, had aided their strategy, and why this was or was not helpful. Several participants indicated that they either tried, or considered using other important dates, numbers, patterns, anniversaries, and smudges. Some participants indicated that they had observed their partners entering their PINs, but not closely enough to see the PIN. Some also tried to gain access using apps. However, these strategies proved unsuccessful for various reasons. In the case of smudges for example, several participants said the smudges were all over, as elaborated by P08B:

> "So the first thing is, I'm gonna look for fingerprints anywhere. See if there was any indication it is to a pattern that's used a lot. But it's all just like swipes in the middle, so probably TikTok, if I had to guess."

P06A tried to gain unauthorized access through the photos app, but this was not successful:

> "I was going in the photos, because sometimes I know there used to be a glitch before they updated it where if you clicked on photos, it would go in …It's not there [anymore]."

P08A tried to get additional information about their partner through their notifications, but this was not helpful:

> "I'm gonna kind of look through all the notifications as a first thing. The problem is that unlike my phone where I have like previews, he doesn't have previews. He only has like the actual notifications, so I can't really get any information from that."

*4.2.2 Guessing Strategies Against Strangers.* Beyond their guessing strategies against their partner during the experiment, we next asked participants to indicate how their strategies would change if their study partner was a complete stranger (**Q3**a). The most common strategies mentioned were random numbers and common passwords or PINs. Although trivial or common passwords or PINs can leave users' devices vulnerable, several participants indicated that they have seen other people using them nonetheless. For instance, P06A stated:

> "The first thing I would try to guess is those sequences or really common, like I would try *000000* or *123456* or the ones like all the way down. I feel like a lot of people have that."

Similarly, P02A said they would try common passcodes since they would not have any prior information of a stranger:

> "If I had a total stranger next to me, my options would be using trivial passcodes from one to six or six zero[s] or six eights. I would try something like that for example. I don't feel like my partner put such passcodes because they are too easy to get, but if I had to do it with a total stranger I would use this kind of stuff."

P05B indicated they would opt for a random combination of numbers due to the lack of personal information:

> "That would be actually difficult because I don't really know that person, so I won't be able to make attempts. If I would be trying to make certain attempts, I would be just …guessing out of the blue."

P01B, on the other hand, doubted they would succeed:

> "Well, I wouldn't know their birthday, so it'd be pretty hard for me to use that to try to lock their phone. And so my strategy wouldn't work because I don't have anything. I don't have that personal information."

*4.2.3 Strategy Comparison.* After evaluating how their guessing strategies would change if they had a stranger as their study partner, we next asked participants if they felt they would be at an advantage, disadvantage, or similarly situated with a stranger as their study partner (**Q3**b). Most participants stated that they would be at a disadvantage. For instance, P02B stated they would be at:

> "a disadvantage because I would have to chose random numbers instead of doing the birthday strategy which might work with some other people."

This was echoed by P02A: "I'm more at an advantage than if trying to guess the password of a friend." P09B similarly added that "I think it's gonna be a disadvantage because it's less information from them, rather a friend."

Three participants mentioned they would be similarly situated, with P06A pointing to the many different possible 6-digit PIN combinations as a big challenge:

> "I don't know, I feel like probably the same like, especially with 6 numbers. There are so many complications, just like mathematically. So I probably feel it would have been the same. I was making educated guesses, but I don't think it doesn't really improve my chances that much I don't think."

Interestingly, P01A believed that they would have more of an advantage with a stranger as their study partner "since they may have probably used patterns."

*4.2.4 Strategy Reflection.* We asked participants to reflect on their guessing strategies but also think about how others would try to unlock their own device (**Q2**). Most participants said their strategies reflect how they believe their friends would attempt to access their device. A majority further said it reflects how strangers would attempt to unlock their devices. For example P03A said that they "think your phone password is relevant to you and something, maybe only you or potentially close people to you would know." Reiterating this, P03B added that "I think, in order to be able to do this the way I did it for P03A, you have to know the person." Some participants further mentioned that they had indeed seen people using memorable passwords as elaborated by P05B:

> "I have seen people keeping just the easiest passwords that they can remember …Birthday of themselves, or like, or someone they love like mom or girlfriend."

P04A similarly noted that "I've seen one of her best friends keeping his birthday and his friend's birthday along with it. So . . . for the majority of people, they will follow this strategy."

A few participants said that they do not believe that their strategies reflect the strategies others would use. For instance, P08A stated that they "believe other people would try to search information about them other than rely on the person's phone, the lock screen which is not meant to help you."

*4.2.5 Strategy Summary.* Overall, most participants leveraged some variation of birthdays when making guessing attempts against their study partner's device. On the other hand, common passwords or patterns and random numbers were the strategies participants indicated they would use against strangers. Further, the majority of participants felt that having a stranger as a study partner would place them at a disadvantage. They additionally felt that their chosen guessing strategies reflect how they believe others would attempt to gain unauthorized access to their own devices.

## 4.3 Perceptions of Smartphone Security

To explore users' perceptions of their smartphone security, we asked them how close their study partners' guesses were to their actual PIN or password (**Q14**), and their overall perception of their smartphone's security (**Q15**).

*4.3.1 Closeness to Guessing Success.* All participants were unable to guess their study partner's PIN or password, with most not even close, according to their partners. Out of the 18 participants, 13 said that their study partner was far from guessing their PIN or password. Only five participants were close or somewhat close to guessing successfully.

While we did not collect the participants' actual PINs or passwords that they use on the smartphones, some participants provided additional information on how they created their PINs. For instance, P01B acknowledged that "its my birthday, but you know my birthday its the only way you could figure it out." Of the five participants that said their study partner was close or somewhat close to guessing their PIN or password, three of them believed it was due to using their birthdays. For example, P09A said that "it's really close, because she use my dates of birthday. I love 23, but the wrong number is the first one." In other words, their study partner was close to guessing their PIN, and only got a single digit wrong.

P08B explained that while their study partner was not close to guessing their current PIN or password, they mentioned that,"one of my old ones is on here. That's funny." While P08A's PIN was not guessed, they still believed that it's simple and could be easily guessed: "I will be honest, my passcode is very simple, I'm too lazy to choose a complicated one, so there's actually a good chance he may figure it out." Some participants inadvertently disclosed their actual PINs to us. After the experiment concluded, we removed these PINs from our dataset to protect the participants.

*4.3.2 User Perceptions.* When asked whether their PINs or passwords are secure (**Q15**), most participants were affirmative. For instance, P09B stated:

> "I'm confident about my security, and even though it's like [a] simple number. But it's not something that people can guess easily, because you feel that you just don't think that I will be that kind of person that will use that."

However, P05A noted the potential of a brute-force attack being successful on their device:

> "I realized that it's just what it is anyone can guess, probably if they try long and hard enough."

While P03B's PIN was close to being guessed by their study partner, they were not worried: "I know it's not very secure, because it's just my birthday. I just don't really care."

*4.3.3 Updates to PINs, Passwords, or Patterns.* We also asked participants if they would change their PIN, pattern, or password if their study partner was able to successfully gain access to their device (**Q13**). While half of participants would change their PIN if guessed, another half indicated they would not. For example, P02B believed that "it would have been a lucky break". Other participants did not want to memorize more information, as elaborated by P01B: "I already like this. I don't know I just, it's more numbers I have to memorize. So I'm like, I probably just not."

At the same time, about half of participants mentioned that they would be comfortable with their study partner having access to their device, and thus would not change their PIN even if it was guessed by their study partner. For example, P04B said that "I wouldn't, because even if he did that's because he knew something about my information that strangers wouldn't know." P06B added that "I wouldn't really care about P06A having access to it, but I would be kind of concerned someone could guess it."

On the contrary, P08A indicated that "the only person that should know my passcode is me." Echoing this sentiment, P05A indicated that "I think it's a good way to keep yourself . . . away from so many hacks." P09A further noted that:

> "phone[s] especially have like a lot of private information about one person, because I put everything in my phone like my card, my email, my message, my everything, the numbers. So I will like definitely change the password."

Similarly, P04A emphasized that they would change their PIN because "I don't want her to open my phone and check my messages. For my privacy."

*4.3.4 Lock Screen Settings.* We further asked participants if they knew how to access their lock screen settings, and if they had ever made any changes to these settings. (**Q16** - **Q17**). The majority of participants expressed that they knew how to access the various lock screen settings. Around half of the participants mentioned making changes to their lock screen settings. However, when asked to elaborate, participants mostly referenced times where they changed their the actual PIN or password. For example, P08A stated that "I changed my lock screen settings, from 4-digits to 6-digits. So I feel like that was a pretty big change." With most participants mostly talking about updates to their PIN, participants may have in fact misinterpreted this question. Therefore, we leave further exploration of lockscreen settings to future work.

*4.3.5 Perceptions Summary.* In summary, the majority of the participants were not close to guessing their study partners' PIN or password and generally felt secure about their chosen authentication method. In the scenario that their study partner was able to gain unauthorized access, half of the participants would change their PIN or password and half would not.

## 4.4 Success Expectations

During our post-experiment interview, we further asked participants to evaluate the effectiveness of their strategy, as well as factors that led to their success or failure (**Q6** - **Q11**).

*4.4.1 Success Expectations For Friends.* When asked if they expected to succeed at gaining unauthorized access (**Q9**) to their study partner's device, 13/18 participants indicated they did not expect to succeed. Participants cited different reasons for not being able to succeed, one being a limited number of attempts. For instance, P05B said that they "didn't have much hope that I would succeed, because I don't really know, like I had only 5 attempts." Echoing this sentiment, P06B pointed to "cryptography and the fact that there are so many combinations." Similarly, P06A stated:

> "Mathematically, it's so impossible to like get into someone's phone, I think, with like PIN security. Yeah, I think it would have a better chance if there was like like 3 numbers like, basically if it was like less combinations."

*4.4.2 Success Expectations For Strangers.* Interestingly, when we asked participants if their strategy would be effective at gaining unauthorized access to another person's device (**Q12**), 16/18 participants said they expected to succeed. This is a slight contradiction to their earlier sentiments in Section 4.2.3 where most participants said they would be at a disadvantage when guessing unlock credentials of strangers. Nonetheless, P04B noted that "I've [seen] some people using that geometric pattern so it might succeed." This was also echoed by P05A who believed that "people do keep common passwords on their phone." This was also the case for P09B who stated that "other people tend to have a simple way, especially if they are like older. They tend to forget some simple codes."

Some participants indicated that they would succeed on strangers' devices if they gained access to some personal information about them, as elaborated by P04A: "It could have been if I knew their birthday or some information about them." This was also echoed by P02A:

> "My personal experience tells me that usually passcodes are related to birth dates for some reason. This is my case, my friend's case, my family's case, so I believe if I was trying to get my friends password, the close ones, the ones where I am sure about; also how they think, and if they will do it related to their age, because I know the previous password to also help for you to try to predict the new password."

*4.4.3 Success Expectations Summary.* Overall, a majority of participants did not expect to succeed at gaining unauthorized access to their study partner's smartphone by gussing their PIN or password. The main failure reason cited was a limited number of guessing attempts thanks to the throttling implemented across both iOS and Android. However, most participants felt that their guessing strategy would be successful on another person's device because of a belief that other people might be using common PINs. In Section 5, we aggregate participants' guesses and use them to guess PINs selected by strangers from a different study to explore this.

# 5 GUESSABILITY ANALYSIS (RQ2)

As discussed, several participants believed that their guesses would fare better when guessing PINs selected by others outside the study. To evaluate this, we combined the offensive 4- and 6-digit PINs selected by participants and used them to guess PINs selected in a recent study by Bailey et al. [11]. In their study, Bailey et al. asked participants to select one of a 4- or 6-digit secret PIN, as well as provide 5 guesses of the same PIN length of what they believed other participants in the study had selected. Participants received a reward if they succeeded in guessing another participant's PIN.

In this section, we compare how our participants' guesses fare in guessing PINs selected in Bailey et al.'s study. We also compare our participants' performance to (a) that of Bailey et al.'s participants and (b) that of datasets e.g., RockYou and Amitay that have been widely used in the literature [11, 21, 22, 26] for guessing.

## 5.1 Datasets

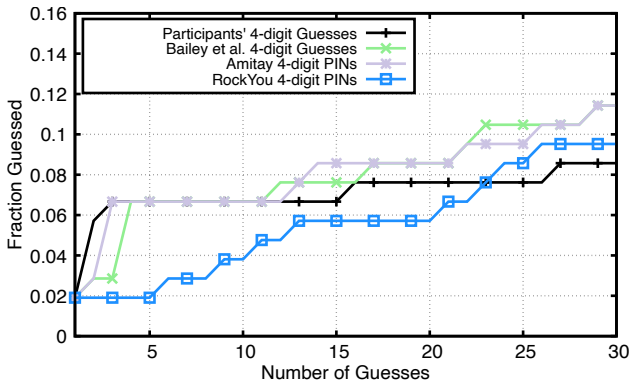
For this analysis, we are interested in guessing both the secret 4- and 6-digit PINs selected by participants in Bailey et al. [11]'s study. To perform this guessing, we leveraged various datasets. First, we aggregated the offensive 4- and 6-digit PINs provided by participants in our study. For comparison purposes, we also used offensive 4- and 6-digit PINs that were collected by Bailey et al. [11], as well as 4- and 6-digit PINs extracted from numeric sequences in the RockYou password leak. Extracting PINs from RockYou is an approach that other researchers have previously employed [13, 21, 22, 35]. For 4-digit PINs, we also used a 4-digit PIN dataset collected by Daniel Amitay [3] that has been particularly noted to perform well when guessing 4-digit PINs.

## 5.2 Guessing Strategy

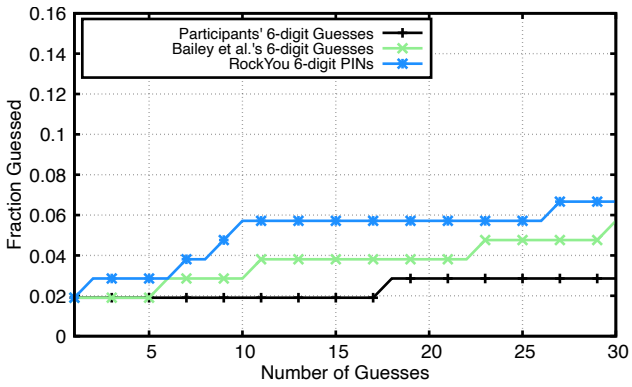
To perform the guessing, we first ordered the offensive PINs, either 4- or 6-digit, in descending order of frequency. Afterward, we guessed the most frequent PIN first, and then the next most frequent PIN, all the way to 30 guesses. Similar to previous work [21, 22, 25, 26], we primarily consider a throttled attacker (which is the most relevant for mobile authentication) and thus limit our guesses to 30 as an attacker will typically have 10–30 guesses before significant delays and lockouts start to occur across iOS and Android.

## 5.3 Guessing Results

We find that the aggregated guesses from participants in our study performed surprisingly well against the secret PINs selected in Bailey et al's study (see Figure 1). In the case of 4-digit PINs, our participants' guesses performed similarly to Bailey et al's offensive PINs and Amitay, but outperformed RockYou, particularly when making just five guesses. After five guesses, both our participants' PINs as well as Bailey et al's and Amitay can guess 6.7% of 4-digit PINs. In contrast, only 2.9% of 4-digit PINs are guessed when using 4-digit PINs from RockYou to guess. This is also the case after 10




(a) Guessing performance of 4-digit PINs.




(b) Guessing performance of 6-digit PINs.

**Figure 1: Guessing performance of participants' offensive PINs against secret PINs collected by Bailey et al. [11]**

guesses. However, when making 30 guesses, our participants' 4-digit PINs can only guess 8.6% of PINs. In contrast, RockYou guesses 9.5%, while both Bailey et al's offensive PINs and Amitay guess 11.4% of the secret PINs. In summary, both Bailey et al's as well as Amitay and our participants' offensive 4-digit PINs perform better than RockYou, particularly when making up to 10 guesses.

When guessing 6-digit PINs, the RockYou dataset seems to perform better than both Bailey et al's offensive PINs, as well as our participants' PINs. After five guesses, both our participants' and Bailey's offensive 6-digit PINs can guess 1.9% of PINs. On the other hand, the RockYou PINs guesses 2.9% of PINs. After 10 guesses, our participants' offensive PINs are still only able to guess 1.9% of PINs. In contrast, Bailey et al' offensive 6-digit PINs can guess 2.9%, while RockYou can guess 5.7%. When making 30 guesses, our participants' PINs guess 2.9% of 6-digit PINs, Bailey et al's PINs guess 5.7% of PINs, while RockYou guesses 6.7% of PINs. In summary, RockYou 6-digit PINs perform better than both Bailey et al's and our participants' offensive 6-digit PINs.

## 5.4 Guessability Summary

Overall, our results confirm that the RockYou 4-digit PIN dataset is possibly not the best dataset to use when guessing 4-digit PINs. Rather, user-selected 4-digit PINs might provide a more effective alternative, with offensive 4-digit PINs selected both in our study as well as in Bailey et al's study performing surprisingly well. On the other hand, 6-digit PINs from RockYou seem to perform better than user-provided offensive PINs when guessing 6-digit PINs. Given that some of Bailey et al's participants indicated that they use some of the secret PINs they selected in that study on their smartphones, our participants may not have been wrong in stating that their offensive PINs would be successful against strangers' PINs.

# 6 DISCUSSION AND CONCLUSION

In this paper, we analyze participants' attempts to guess smartphone PINs, patterns, or passwords when knowing some personal information about the victim. We also explore participants' concerns and perceptions about the security of their smartphones, specifically regarding their passwords, PINs, or patterns. We find that when participants attempt to unlock their friend's phone, the most common technique is guessing birthdays, followed by geometric patterns and repetitions.

In the rest of this section, we discuss our results further as well as their implications on smartphone security.

*Birthdays are most common guessing technique for those with prior knowledge of the victim.* Throughout the course of our study, we observed that birthdays were the most common guessing strategy among participants that know each other. Even though no participant was able to successfully guess their study partner's PIN, several participants actually admitted to using some variations of their birthdays for their PINs. This is inline with prior work [13] that has found birthdays to be a common strategy for selecting PINs. One participant was one digit away from guessing their partner's PIN, while another one guessed a PIN that was previously used by their partner. There are indeed several variations of birthdays that people could use for their PINs. In the case of 4-digit PINs, this could be *yyyy*, *mmyy*, *yymm*, *ddmm*, *ddyy*, *ddmm*, etc. For 6-digit PINs, this could be *mmyyyy*, *yyyymm*, *ddmmyy*, *mmddyy*, etc. These combinations could also be regional, with the date format in the US for example being different compared to the rest of the world. While there is a risk that PINs based on birthdays could be susceptible to guessing if people gain access to some personal information about the victim, there are also very many different variations of birthdays that people could use. This, coupled with the throttling implemented by both Android and iOS, makes it challenging for guessing attacks to be successful, especially for casual guessers who may have access to the device for only a short period of time. Thus, while previous studies [21, 22, 26] have speculated that knowledge of the victim might improve guessing performance for smartphone unlock PINs, we find that it is not straightfoward to guess PINs, even with previous knowledge of the victim.

*About half of participants would not change PINs even if they are guessed.* Interestingly, about half of the participants in our study indicated that they would not change their PIN, pattern, or password even if it was guessed by their study partner. Often, participants pointed to trusting their study partner or not wanting to memorize

a new PIN. On one hand, this could be a confirmation of the privacy paradox where people are sometimes concerned about privacy but at the same time do not take any protective measures to protect their privacy. On the other hand, participants were probably weighing the security versus usability tradeoffs of updating their PINs, and prioritizing usability. Either way, smartphones hold a lot of crucial information, and people's digital and financial lives can be severely impacted when their PINs are guessed and their devices accessed. A promising future area of research is to explore whether fear appeals — especially with regards to the damage that can be done on peoples' digital lives when their PINs are guessed – can nudge users to select more secure choices. Prior work by Albayram et al. [2] has particularly found that fear appeals can encourage users to enable an unlock scheme on their device. Alerting users about failed unlock attempts on their devices is another promising direction that could possibly encourage users to select or change their PIN to a more stronger one (if they do not have one already).

*User-provided guesses perform surprisingly well when guessing PINs selected by others from a previous study.* Most previous work on mobile authentication has leveraged the Amitay dataset when guessing 4-digit PINs and the RockYou dataset when guessing 6-digit PINs. The Amitay dataset was collected from PINs selected by users on a screen imitating the iOS lockscreen [3] by Daniel Amitay. Since such a dataset does not exist for 6-digit PINs, researchers have mostly used 6-digit sequences extracted from the RockYou password leak when guessing 6-digit PINs. In using the offensive 4- and 6-digit PINs provided by participants in our study to guess 4- and 6-digit PINs collected from a different study by Bailey et al. [11], we find these PINs to perform similarly to the Amitay dataset when making up to 10 guesses for 4-digit PINs, and even better than the RockYou dataset. However, the RockYou dataset performs well on 6-digit PINs. Since our dataset was relatively small, we suggest future work to collect a bigger dataset of 6-digit PINs from users. This will provide an opportunity to better explore the guessability and distribution of human-chosen 6-digit PINs.

*Exploring awareness and perceptions of lockscreen settings is an interesting direction for future research.* Lockscreen settings, including the display of sensitive notifications on the screen when the device is locked, duration before the device is locked, among others are crucial for privacy. During our study, we asked participants about these settings, including whether they had recently changed them. It appears that most participants only think about and change their PIN, password, or unlock pattern, and not other lockscreen settings, including sensitive information from notifications getting displayed when the device is locked for example. Therefore, it might be interesting to explore more deeply whether users are aware of the various lockscreen settings on their devices, as well as willingness to update them. This could potentially be done with two groups of participants where one group is made aware about the risks posed by certain settings, while the control group is not. The goal would be to explore whether increasing awareness about the risks posed by exposure of certain information on the lockscreen can nudge participants to update these settings.

## ACKNOWLEDGMENTS

We thank Miles Grant and James Levy for their help, as well as all the anonymous reviewers for their insightful comments and feedback. We also thank all our participants for their time and invaluable insights. This material is based upon work supported by the US National Science Foundation under Grant No. 1845300.

## REFERENCES

[1] Yomna Abdelrahman, Mohamed Khamis, Stefan Schneegass, and Florian Alt. 2017. Stay Cool! Understanding Thermal Attacks on Mobile-Based User Authentication. In *ACM Conference on Human Factors in Computing Systems (CHI '17)*. ACM, Denver, Colorado, USA, 3751–3763.

[2] Yusuf Albayram, Mohammad Maifi Hasan Khan, Theodore Jensen, and Nhan Nguyen. 2017. "...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 *Symposium on Usable Privacy and Security (SOUPS '17)*. USENIX, Santa Clara, California, USA, 49–63.

[3] Daniel Amitay. 2011. Most Common iPhone Passcodes. http://danielamitay.com/blog/2011/6/13/most-common-iphone-passcodes, as of August 20, 2024.

[4] Panagiotis Andriotis, George Oikonomou, Alexios Mylonas, and Theo Tryfonas. 2016. A Study on Usability and Security Features of the Android Pattern Lock Screen. *Information and Computer Security* 24, 1 (March 2016), 53–72.

[5] Panagiotis Andriotis, Theo Tryfonas, and George Oikonomou. 2014. Complexity Metrics and User Strength Perceptions of the Pattern-Lock Graphical Authentication Method. In *Conference on Human Aspects of Information Security, Privacy and Trust (HAS '14)*. Springer, Heraklion, Crete, Greece, 115–126.

[6] Panagiotis Andriotis, Theo Tryfonas, George Oikonomou, and Can Yildiz. 2013. A Pilot Study on the Security of Pattern Screen-Lock Methods and Soft Side Channel Attacks. In *ACM Conference on Security and Privacy in Wireless and Mobile Networks (WiSec '13)*. ACM, Budapest, Hungary, 1–6.

[7] Adam J. Aviv, Devon Budzitowski, and Ravi Kuber. 2015. Is Bigger Better? Comparing User-Generated Passwords on 3x3 vs. 4x4 Grid Sizes for Android's Pattern Unlock. In *Annual Computer Security Applications Conference (ACSAC '15)*. ACM, Los Angeles, California, USA, 301–310.

[8] Adam J. Aviv, John T. Davin, Flynn Wolf, and Ravi Kuber. 2017. Towards Baselines for Shoulder Surfing on Mobile Authentication. In *Annual Conference on Computer Security Applications (ACSAC '17)*. ACM, Orlando, Florida, USA, 486–498.

[9] Adam J. Aviv, Katherine Gibson, Evan Mossop, Matt Blaze, and Jonathan M. Smith. 2010. Smudge Attacks on Smartphone Touch Screens. In *USENIX Workshop on Offensive Technologies (WOOT '10)*. USENIX, Washington, District of Columbia, USA, 1–7.

[10] Adam J. Aviv, Flynn Wolf, and Ravi Kuber. 2018. Comparing Video Based Shoulder Surfing with Live Simulation and Towards Baselines for Shoulder Surfing on Mobile Authentication. In *Annual Conference on Computer Security Applications (ACSAC '18)*. ACM, San Juan, Puerto Rico, USA, 453–466.

[11] Daniel V Bailey, Collins W Munyendo, Hunter A Dyer, Miles Grant, Philipp Markert, and Adam J Aviv. 2023. "Someone Definitely Used 0000"': Strategies, Performance, and User Perception of Novice Smartphone-Unlock PIN-Guessers. In *Proc. EuroUSEC*.

[12] Joseph Bonneau, Cormac Herley, Paul C Van Oorschot, and Frank Stajano. 2015. Passwords and the evolution of imperfect authentication. *Commun. ACM* 58, 7, 78–87.

[13] Joseph Bonneau, Sören Preibusch, and Ross Anderson. 2012. A Birthday Present Every Eleven Wallets? The Security of Customer-Chosen Banking PINs. In *Financial Cryptography and Data Security (FC '12)*. Springer, Kralendijk, Bonaire, 25–40.

[14] Maria Casimiro, Joe Segel, Lewei Li, Yigeng Wang, and Lorrie Faith Cranor. 2020. A Quest for Inspiration: How Users Create and Reuse PINs. In *Who Are You?! Adventures in Authentication Workshop (WAY '20)*. Virtual Conference, 1–7.

[15] Anupam Das, Joseph Bonneau, Matthew Caesar, Nikita Borisov, and XiaoFeng Wang. 2014. The Tangled Web of Password Reuse. In *Symposium on Network and Distributed System Security (NDSS '14)*. ISOC, San Diego, California, USA.

[16] Alexander De Luca, Marian Harbach, Emanuel von Zezschwitz, Max-Emanuel Maurer, Bernhard Ewald Slawik, Heinrich Hussmann, and Matthew Smith. 2014. Now You See Me, Now You Don't: Protecting Smartphone Authentication from Shoulder Surfers. In *ACM Conference on Human Factors in Computing Systems (CHI '14)*. ACM, Toronto, Ontario, Canada, 2937–2946.

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

[18] Federal Trade Commission. 2022. How to Protect Your Phone from Hackers. https://consumer.ftc.gov/articles/how-protect-your-phone-hackers

[19] Małgorzata Figurska, Maciej Stańczyk, and Kamil Kulesza. 2008. Humans cannot consciously generate random numbers sequences: Polemic study. *Medical*

*hypotheses* 70, 1 (2008), 182–185.
[20] Marte Løge, Markus Dürmuth, and Lillian Røstad. 2016. On User Choice for Android Unlock Patterns. In *European Workshop on Usable Security (EuroUSEC '16)*. ISOC, Darmstadt, Germany.
[21] Philipp Markert, Daniel V. Bailey, Maximilian Golla, Markus Dürmuth, and Adam J. Aviv. 2020. This PIN Can Be Easily Guessed: Analyzing the Security of Smartphone Unlock PINs. In *IEEE Symposium on Security and Privacy (SP '20)*. IEEE, San Francisco, California, USA, 286–303.
[22] Philipp Markert, Daniel V. Bailey, Maximilian Golla, Markus Dürmuth, and Adam J. Aviv. 2021. On the Security of Smartphone Unlock PINs. *ACM Transactions on Privacy and Security* 24, 4 (Nov. 2021), 30:1–30:36.
[23] Nora McDonald, Sarita Schoenebeck, and Andrea Forte. 2019. Reliability and Inter-Rater Reliability in Qualitative Research: Norms and Guidelines for CSCW and HCI Practice. *Proc. ACM Hum.-Comput. Interact.*, Article 72 (2019), 23 pages.
[24] William Melicher, Darya Kurilova, Sean M. Segreti, Pranshu Kalvani, Richard Shay, Blase Ur, Lujo Bauer, Nicolas Christin, Lorrie Faith Cranor, and Michelle L. Mazurek. 2016. Usability and Security of Text Passwords on Mobile Devices. In *ACM Conference on Human Factors in Computing Systems (CHI '16)*. ACM, San Jose, California, USA, 527–539.
[25] Collins W. Munyendo, Miles Grant, Philipp Markert, Timothy J. Forman, and Adam J. Aviv. 2021. Using a Blocklist to Improve the Security of User Selection of Android Patterns. In *Symposium on Usable Privacy and Security (SOUPS '21)*. USENIX, Virtual Conference, 37–56.
[26] Collins W. Munyendo, Philipp Markert, Alexandra Nisenoff, Miles Grant, Elena Korkes, Blase Ur, and Adam J. Aviv. 2022. "The Same PIN, Just Longer": On the (In)Security of Upgrading PINs from 4 to 6 Digits. In *USENIX Security Symposium (SSYM '22)*. USENIX, Boston, Massachusetts, USA.
[27] Bijeeta Pal, Tal Daniel, Rahul Chatterjee, and Thomas Ristenpart. 2019. Beyond Credential Stuffing: Password Similarity Models using Neural Networks. In *IEEE Symposium on Security and Privacy (SP '19)*. IEEE, San Francisco, California, USA, 866–883.
[28] Kathryn Roulston. 2014. *Analysing interviews.* The SAGE handbook of qualitative data analysis.
[29] Raina Samuel, Philipp Markert, Adam J. Aviv, and Iulian Neamtiu. 2020. Knock, Knock. Who's There? On the Security of LG's Knock Codes. In *Symposium on Usable Privacy and Security (SOUPS '20)*. ACM, Virtual Conference, 37–59.
[30] Florian Schaub, Ruben Deyhle, and Michael Weber. 2012. Password Entry Usability and Shoulder Surfing Susceptibility on Different Smartphone Platforms. In *International Conference on Mobile and Ubiquitous Multimedia (MUM '12)*. ACM, Ulm, Germany, 13:1–13:10.
[31] Sebastian Uellenbeck, Markus Dürmuth, Christopher Wolf, and Thorsten Holz. 2013. Quantifying the Security of Graphical Passwords: The Case of Android Unlock Patterns. In *ACM Conference on Computer and Communications Security (CCS '13)*. ACM, Berlin, Germany, 161–172.
[32] Emanuel von Zezschwitz, Alexander De Luca, Philipp Janssen, and Heinrich Hussmann. 2015. Easy to Draw, but Hard to Trace?: On the Observability of Grid-based (Un)Lock Patterns. In *ACM Conference on Human Factors in Computing Systems (CHI '15)*. ACM, Seoul, Republic of Korea, 2339–2342.
[33] Emanuel von Zezschwitz, Malin Eiband, Daniel Buschek, Sascha Oberhuber, Alexander De Luca, Florian Alt, and Heinrich Hussmann. 2016. On Quantifying the Effective Passsword Space of Grid-Based Unlock Gestures. In *Conference on Mobile and Ubiquitous Multimedia (MUM '16)*. ACM, Rovaniemi, Finland, 201–212.
[34] Chun Wang, Steve T.K. Jan, Hang Hu, Douglas Bossart, and Gang Wang. 2018. The Next Domino to Fall: Empirical Analysis of User Passwords across Online Services. In *ACM Conference on Data and Application Security and Privacy (CODASPY '18)*. ACM, Tempe, Arizona, USA, 196–203.
[35] Ding Wang, Qianchen Gu, Xinyi Huang, and Ping Wang. 2017. Understanding Human-Chosen PINs: Characteristics, Distribution and Security. In *ACM Asia Conference on Computer and Communications Security (ASIA CCS '17)*. ACM, Abu Dhabi, United Arab Emirates, 372–385.

# APPENDIX

## A EXPERIMENT

### Descriptions and Instructions

*Read these instructions to the participants:*
This study has 4 major parts to it. Part 1 consists of basic demographics questions about you and your study partner. Part 2 is the experiment itself. As you read in the informed consent document, this is where you and your study partner will swap locked phones and attempt to gain access to each other's phones. Part 3 is a post-experiment interview. In part 4, we will debrief you about the study as well as provide information that can improve the security of your phone. All parts occur in chronological order. The study should take around 30-35 minutes.

*Read the following briefing to the participants. Pause occasionally and ask for questions:*
First, a phone can be either locked or unlocked. A locked phone would require you to enter a PIN, pattern, or password to unlock it to access apps, photos, emails, etc. You can also unlock your phone using a biometric, such as a fingerprint or face, but we are going to focus on how you use PINs, patterns, or passwords in this study. As part of the study you will attempt to unlock your study partner's phone using a PIN, pattern or password. If you do so successfully, we'll call that an unauthorized access.
Do you have any questions about the terminology?
While you attempt to unlock your study partner's phone, we also ask that you keep in mind the strategy you are using. We will ask you about it later.

*Conclude by saying:*
Is there anything you would like me to explain again? We will now move into some group demographics questions. As a reminder, we will be audio-recording to transcribe the information later.
Are you comfortable being audio-recorded?

*Start the audio recording, and get verbal consent:*
To confirm again, do you wish to continue with the study?

**Knowledge of Each Other (Group)**

**K1** How well do you know each other?
- (a) Can you describe your relationship with your study partner? For example, are you friends, colleagues, strangers, etc.?
- (b) How long have you known each other?
- (c) Have you ever traveled together on a trip outside of this area?
- (d) How often did you spend time together in the last month?

*Explain that participants will now be separated by saying:*
We will now be separating you from your partner. This portion of the study is done individually in order to preserve privacy and research integrity.

*Pause the audio recording. At this point the researchers will separate the participants into individual groups as each part of the study must be done independently. This also adds privacy for demographics and interview question.*

We will now be starting the individual demographics portion of the study.

*Ask the below demographics questions about the individual. Ask subparts of questions if they are not mentioned. Remind participants that you will resume recording before recording.*

**Demographic Questions (Individual)**

**D1** What is your age?
**D2** What is your highest level of education?

(a) What is your area of focus in education such as (major or trade school focus)?
**D3** What is your profession?
**D4** What is your identified gender?
**D5** What is your smartphone's operating system?
(a) For example, do you have an iPhone or an Android phone? Most likely, if you don't have an iPhone you have an Android phone. If you don't know, we can look for you.
**D6** What is the model of your phone, if you know it?
(a) For example, an iPhone 8, or a Samsung Galaxy, or a Google Pixel 3. If you don't know, we can help you find out.

*Ask participants to put their phones in airplane mode, lock the device (and confirm) then give their phone to the researcher. Both researchers will now exchange phones. Pause the audio recording.*

**Final Instructions**
*Resume the audio recording and read the following instructions to the participant:*

- During this experiment you will have up to 5 attempts at unlocking your study partner's phone by entering in a PIN, pattern, or password.
- You will have 10 minutes total for the task.
- Before and while entering PINs, patterns, or passwords, you are allowed to explore anything that is available from your study partner's locked phone.
- Be sure to speak/think out loud while you complete this task by describing any strategies or thought process or information you find in trying to unlock your partner's phone. We will be using audio recording equipment.
- You will also be provided a pen-and-paper that you can take notes during the study. We will review these notes later.
- Importantly, you should pause before any attempt to enter a PIN, pattern or password by letting the researcher know you're doing so, describing what PIN, pattern or password you're entering, and why you've chosen that PIN, pattern or password. Do you understand these instructions?
- If you succeed on an attempt, put down the phone and give it to the researcher. You should repeat what you did to unlock the phone.
- After your 5th attempt, put down the phone and give it to the researcher. Please do not make more than 5 attempts.
- Do you have any questions before we begin?

*Give the participant the phone and tell them "you may start now." Start a timer for 10 minutes. Follow the instructions given to the participant and take notes on anything they do and say. If the timer goes off, or they succeed, or use all 5 attempts, take the phone and tell the participant this portion of the study is over.*

**Post-Experiment Interview (Individual)**
That concluded the experiment portion of the study. We will now begin the interview portion of this study. Please answer all these questions honestly and to the best of your ability.

*Read the following questions in order as a semi-structured interview. Ask the sub-bullet questions if they did not directly answer them in the main questions. Take notes on all answers.*

**Q1** What was your main strategy to unlock the phone and why?
**Q2** Did your strategies reflect how you believe others would try to unlock your phone?
(a) Why do you think so or not? Or why do you think they vary?
(b) Do you think this is true of both your friends and strangers?
**Q3** Suppose that your study partner was a complete stranger. Answer the next question with this in mind.
(a) How does having a stranger as your study partner, instead of someone you know, affect the strategies you would use in an attempt to unlock and access the phone?
(b) Do you think you would have gained an advantage, disadvantage, or stayed the same in the experiment?
**Q4** Did any information help guide your strategy?
*For each additional information they offer, ask the below additional questions about it:*
(a) What was the particular information?
(b) Can you explain how you learned the info?
(c) Did it turn out to be useful for your strategy or not? Please explain.
*Only ask for each subpart if they didn't mention above*
**Q5** Did you know any of the following about your study partner before this study?
(a) Birthday.
(b) Anniversary.
(c) Other important dates
(d) Other important numbers?
(e) Have you observed them entering their PIN, pattern, or password before?
*Ask below questions if they were **successful** in gaining unauthorized access:*
**Q6** Why do you think your strategy succeeded?
**Q7** Are there other strategies you thought about trying? *Only ask for each subpart if they didn't mention above*
(a) Smudges, fingerprints, other residue on the phone.
(b) Voice assistants
(c) Using data gathered from widgets
(d) Geometric patterns
(e) Trying to enter via the use of an application
**Q8** Do you think you would be able to replicate your success on a stranger's phone?
(a) If so why, if not, why not?
*Ask this set of questions if they **failed** in gaining unauthorized access:*

**Q9** Did you expect to succeed?
(a) Why?
**Q10** What factors do you think led to your failure?
**Q11** Are there other strategies you thought about trying? Did you consider any of the following?
(a) Smudges, fingerprints, other residue on the phone.

(b) Voice assistants.
(c) Using data gathered from widgets.
(d) Geometric patterns.
(e) Trying to enter via the use of an application.

**Q12** Do you think your strategy might have succeeded on someone else's phone?
(a) If so who and why, if not, why not?

Suppose your study partner was able to gain unauthorized access to your phone. This may not be the case, but pretend that it is.

**Q13** Would you change your password or PIN or pattern?
(a) Why?
(b) What would you change about it?

Note, that during debriefing, we will inform you if in fact your study partner was able to gain unauthorized access to your phone. After which you can choose to change your password/PIN/pattern. Please wait a moment while we exchange mobile phones.

*Pause the recording. Researchers leave their rooms, and exchange mobile phones so that each participant has their own phone back in their possession. Researchers exchange information on if the phone had been accessed successfully or not as well as guesses made. Then, resume recording again.*

**Lock Screen Questions (Individual)**
*If the participant's PIN/pattern/password was not guessed, show them the guesses made and say:*

**Q14** From these guesses that were made by your partner, how close was your PIN/pattern/password to being guessed?
**Q15** Overall, how do you feel about the security of your PIN, pattern, or password?
**Q16** Do you know how to access settings on your phone for your lock screen?
**Q17** Have you ever changed your lock screen settings?
(a) If so, when and how?
**Q18** Can we see your current lock screen settings? We will also be taking a picture of these settings so that we may transcribe them later.

*While the participant is doing this, the researcher times how long it takes for them to find this information, as well as notes any misclicks or false. If the participant can't find this information, we help them find it.*

**Final Questions (Individual)**

**Q19** Have you ever been in a situation like this where someone else had your phone?
(a) Who had your phone?
(b) What concerns did you have, if any?
**Q20** Overall, what did you think of the study?
**Q21** Is there any other feedback or information you would like to share?

This concludes the interview portion of the experiment. Thank you for answering our questions.

*Stop audio recording, and get the study participants back together for a final debrief.*

**Debrief (Group)**
Thank you for participating in our study. We will now take you through the final debriefing. First of all, we find it important to let you know if either of your phones was susceptible to unauthorized access. Please note that even if your PIN was not guessed, it does not necessarily mean that it's secure.
*Tell them whose phone was unlocked and how.*

- Your study partner was able to unlock your phone using the PIN/password/pattern XXXX. We will not record this PINpassword/pattern as part of the study, but you will now have the opportunity to change your PIN/password/pattern on your phone, if you so choose.
- Your student partner was not able to unlock your phone. This does not mean your PIN/password/pattern is secure from other attacks. Following, we will provide information for changing your PIN/password/pattern, if you choose to do so.
- In case you want to change any of your lock screen settings, or your password. This is how you would do so.
- Do you have any additional questions about our study? Once again, thank you for completing this study.
- If you can please provide your email address so we may provide you with a digital Amazon gift card. Your email address will never be linked to the data.

# B QUALITATIVE CODES

- **strategies-partners (112)**
  **birthdays (42):** *friends-birthday (3), related-to-personal-pattern (3), previous-observations (2)*
  **geometric-patterns (19):** *previous-observations (2), smudges (1)*
  **repetitions (16):** *previous-observations (3), siblings (1)*
  **usability (15):** *previous-observations (3), related-to-personal-pattern (1)*
  *other-important-numbers (5), favorite-number (3), extra-curricular-activities (3), even-numbers (2), letter (2), other-important-dates (1), random-numbers (1), home-state-info (1), music-interest (1), odd-numbers (1)*
- **strategies-strangers (25)**
  **random-numbers (8):** *no-personal-info (3)*
  **common-passwords (6):** *no-personal-info (1)*
  **usability (3):** *no-personal-info (1)*
  **birthday (2):** *license (1)*
  *no-personal-info (2), no-idea (1), find-information (1), smudges (1), phone-number (1)*
- **strategies-reflection (43)**
  **yes (37):** *friends (13), strangers (11)*
  **no (6):** *stranger (1)*
  **unsure (1)**


**Figure 2: Anonymized recruitment flyer.**

- **failure-reason (13)**
  *combinations (4), six-digits (2), bad-memory (2), lack-of-personal-info (2), not-simple-code (1), focus-on-birthday (1), open-ended (1)*
- **stranger-advantage (24)**
  **stayed-same (4):** *combinations (1)*
  **yes (3):** *patterns (1)*
  **no (17):** *no-personal-info (4)*
- **additional-info-for-strategy (50)**
  *observed-them-entering (5), other-important-dates (5), smudges (5), other-important-numbers (4), birthdays (4), patterns (4), using-app (4), letters (3), voice-assistants (3), anniversaries (3), capitalization (2), other-important-info (2), notifications (2), memorability (1), phone-wallet-cards (1), parents-birthday (1), boyfriends-birthday (1)*
- **success-expectation-for-partner (32)**
  **no (23):** *limited-attempts (7), no-personal-info (2), word (1)*
  **yes (9):** *birthday (3), time-of-friendship (1)*
- **success-expectation-for-other-person (37)**
  **yes (33):** *birthday (5), common-passwords (4), previous-observation (3), smudges (2), personal-information (2), android-pattern (1)*
  **no (4):** *combinations (1), unpredictable (1)*
- **change-PIN? (36)**
  **yes (16):** *concern (6), easy-to-guess (1)*
  **no (11):** *difficult-to-guess (1), luck (1), memorability (1) access-for-friend (9)*
- **change-PIN-how (6)**
  *change-password (3), less-personal (1), familiar-to-old (1), add-digits (1)*
- **closeness-to-guessing (19)**
  **far (14):** *changed-logic (1)*
  **close (3)**
  **middle (2)**
- **PIN-security-perceptions (18)**
  *secure (13), not-secure (3), moderate (2)*
- **changed-lockscreen (30)**
  **yes (22):** *password (3), 1-2 years (2), one-month (2), wallpaper (1), 4-to-6 (1), control-center (1), face-id (1), patterned-code (1), 6 years (1)*
  **no (7)**
  **unsure (1)**
- **actual-PIN (8)**
  **birthday (5):** *combo-parent-child-birthday (1)*
  *license-plate (1), boyfriend-phone-number (1), double-tap (1)*

**Table 2: Detailed demographics of participants. Every pair of participants are represented by the same participant number. For example, P01A and P01B represent the first two participant pairs, with P01A being the first participant and P01B being the second.**

| Participant | Gender | Age | Level of Education | Major | Phone OS | Phone Model | Relationship to Partner |
|---|---|---|---|---|---|---|---|
| P01A | Female | 22 | High school | - | iOS | iPhone | Classmates and friends |
| P01B | Non-binary | 21 | High school | Chemistry | iOS | iPhone | Classmates and friends |
| P02A | Male | 24 | Masters | Transportation engineering | iOS | iPhone | Classmates |
| P02B | Male | 22 | Masters | Autonomous vehicles | iOS | iPhone | Classmates |
| P03A | Female | 20 | High school | Cognitive neuroscience | iOS | iPhone | Friends and teammates |
| P03B | Female | 22 | High school | Political communication | iOS | iPhone | Friends and teammates |
| P04A | Male | 21 | Bachelors | Data science | iOS | iPhone | Friends |
| P04B | Female | 22 | Bachelors | Computer science | Android | - | Friends |
| P05A | Male | 24 | Bachelors | Computer science | iOS | iPhone | Classmates and friends |
| P05B | Female | 23 | Bachelors | Data science | iOS | iPhone | Classmates and friends |
| P06A | Female | 22 | Bachelors | International affairs | iOS | iPhone | Classmates and friends |
| P06B | Male | 22 | Bachelors | International relations | iOS | iPhone | Classmates and friends |
| P07A | Female | 19 | High school | Computer science | iOS | iPhone | Friends |
| P07B | Female | 19 | High school | Computer science | iOS | iPhone | Friends |
| P08A | Male | 18 | High school | Computer science | iOS | iPhone | Friends |
| P08B | Male | 18 | High school | Computer science | iOS | iPhone | Friends |
| P09A | Female | 29 | Bachelors | Global health | iOS | iPhone | Friends |
| P09B | Female | 28 | Bachelors | Law | iOS | iPhone | Friends |