Where Do You Look When Unlocking Your Phone? A Field Study of Gaze Behavior During Smartphone Unlock

Yasmeen Abdrabou
y.abdrabou@lancaster.ac.uk
Lancaster University
United Kingdom

Tatiana Omelina
t.omelina@campus.lmu.de
LMU Munich
Germany

Felix Dietz
felix.dietz@unibw.de
University of the Bundeswehr Munich
Germany

Mohamed Khamis
mohamed.khamis@glasgow.ac.uk
University of Glasgow
United Kingdom

Florian Alt
florian.alt@unibw.de
University of the Bundeswehr Munich
Germany

Mariam Hassib
hassib@fortiss.org
fortiss Research Institute of the Free State of Bavaria
Germany

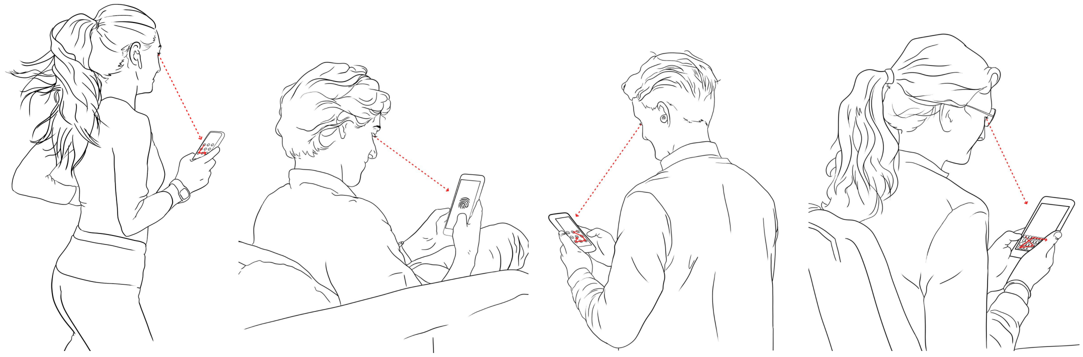

Figure 1: In a field study, we explore users' eye gaze behavior during smartphone unlocking in different environments and different activities. We use our analysis to introduce the concept of leveraging gaze in 2FA/Implicit identification/authentication for enhancing smartphone security and introduce a new threat model induced by continuous gaze tracking.

ABSTRACT

Eye gaze has emerged as a promising avenue for implicit authentication/identification on smartphones, offering the potential for seamless user identification and two-factor authentication. However, a crucial gap exists in understanding eye gaze behaviour specifically during smartphone unlocks. This lack of understanding is magnified by scenarios where users' faces are not fully visible in front cameras, leading to inaccurate gaze estimation. In this work, we conducted a 24-hour in-the-wild study tracking 21 users' eye gaze during smartphone unlocks. Our findings highlight substantial eye gaze behaviour variations influenced by authentication methods, physical activity, and environment. Our findings provide insights to enhance and adapt implicit user identification/authentication systems based on gaze tracking on smartphones taking into consideration different users' behaviour, and environmental effects.

Permission to make digital or hard copies of part or all of this work for personal or classroom use is granted without fee provided that copies are not made or distributed for profit or commercial advantage and that copies bear this notice and the full citation on the first page. Copyrights for third-party components of this work must be honored. For all other uses, contact the owner/author(s).
CHI EA '24, May 11–16, 2024, Honolulu, HI, USA
© 2024 Copyright held by the owner/author(s).
ACM ISBN 979-8-4007-0331-7/24/05
https://doi.org/10.1145/3613905.3651094

CCS CONCEPTS

• **Security and privacy → Human and societal aspects of security and privacy**; • **Human-centered computing → Human computer interaction (HCI)**; **Empirical studies in HCI**.

KEYWORDS

Gaze Behaviour, Authentication, Smartphone, Eye Tracking

ACM Reference Format:
Yasmeen Abdrabou, Tatiana Omelina, Felix Dietz, Mohamed Khamis, Florian Alt, and Mariam Hassib. 2024. Where Do You Look When Unlocking Your Phone? A Field Study of Gaze Behavior During Smartphone Unlock. In *Extended Abstracts of the CHI Conference on Human Factors in Computing Systems (CHI EA '24), May 11–16, 2024, Honolulu, HI, USA.* ACM, New York, NY, USA, 7 pages. https://doi.org/10.1145/3613905.3651094

1 INTRODUCTION

Today, smartphones serve as indispensable companions, storing a lot of personal information ranging from private messages to sensitive financial data. However, this convenience comes with several risks, emphasizing the critical need for robust security measures. Authentication methods and two-factor identification (2FA) play pivotal roles in fortifying smartphone security, serving as the primary gatekeepers to safeguard sensitive content. User identification, combined with stringent password protocols, lays the foundation for a secure smartphone environment. Utilizing eye gaze in (2FA) authentication seen a rise in interest in the research community in the last years [17, 18]. However, the implementation of eye gaze technology on smartphones has primarily focused on explicit authentication, offering protection against attacks like shoulder surfing [18]. Nevertheless, the potential for leveraging eye gaze for implicit authentication and user identification has been introduced but not widely embraced. The primary challenge lies in the need for users to provide supplementary input [17, 34], which often elongates the authentication process.

In this paper, we investigate users' gaze behavior during smartphone unlocking and the factors affecting it. We introduce the concept of leveraging gaze behavior during the unlock step for gaze-based user identification and two-factor authentication without adding explicit stimuli that may overload the user. Through an in-the-wild study (N = 21), we analyze users' gaze behavior during smartphone unlocking collected over a period of 24 hours. We test the effect of the environment, unlock technique, age, gender, and physical activity on users' eye gaze behavior. Our findings reveal that the environment and physical activity have a significant effect on users' eye gaze behavior, while the unlock technique has an impact on face visibility. These findings not only shed light on critical factors affecting the adoption of eye gaze on smartphones but also pave the way for future research that capitalizes on users' smartphone usage behavior to enhance security measures.

The contribution of our work is twofold. Firstly, through an in-the-wild study, we explore and understand users' eye gaze behavior during smartphone unlocking. Secondly, we use our analysis of gaze behavior during unlock to introduce the concept of leveraging gaze in 2FA and enhancing smartphone security.

2 RELATED WORK

2.1 Users' Smartphone Unlock Behaviour and Its Affecting Factors

In 2014, Harbach et al., found that almost 2.9% of the time of smartphone usage is spent in unlocking[15]. While we have seen a rise to new authentication techniques since then (e.g., facial biometrics or continuous authentication) with the goal of balancing usability and increasing adoption of security measures, it is still estimated that 10% to 35% of users do not use an authentication mechanism mainly due to usability issues [21]. For this, researchers have conducted a multitude of studies to understand user behavior during authentication/unlocking considering factors such as age, gender, and different environments [14, 15, 27, 28]. For example, Mahfouz et al, investigated the error proneness of Android unlocking techniques [23]. In a field study, Harbach et al., compared the usability and security of PINs and patterns[14]. They found that users who unlock using PINs take a longer time to unlock and make fewer errors than pattern users[14]. More recently, Koushki et al., investigated user's uptake and understanding of the Android implicit authentication where they found that users still have trouble understanding its semantics [21].

Researchers found that the environment affects users' overall behaviour such as where they locate themselves in the environment and which actions they perform. For example, a study by Hanle et al. demonstrated variations in people's behaviour and where they locate themselves in public, semipublic, and private spaces [13]— particularly when their actions attract the attention of others [33]. In addition, the familiarity and crowdedness of the environment have been identified as influencing factors on user behaviour [22, 25, 33]. Similar to the environment, users' activity also has a great effect on users' smartphone behaviour where they tend to hold their smartphones in different ways during different activities. For example, a study done by Khamis et al. found that face visibility collected through the smartphone's frontal camera is highly correlated to the activity the user is doing on their phones and their seating position [18, 19]. Similarly, Broh et al. found that users' face visibility on smartphones is much less while running [11, 32] compared to other activities.

2.2 Implicit Gaze Tracking for User Identification and Authentication

While a lot of research focused on building explicit (multimodal) gaze-based authentication schemes (e.g. [3, 20]), implicit gaze-based authentication has a lot of potential in reducing error and increasing the usability of authentication [17, 18]. Katsini et al. provide an extensive overview of the challenges and metrics affecting the success of implicit gaze-based authentication/identification schemes [17]. Song et al., introduced an implicit gaze-based authenication scheme on smartphones using the frontal camera to block illegitimate users if their behavior deviated from legitimate user behavior [30]. Zhang et al. used implicit visual cues from the content of existing applications on head-mounted displays to build an implicit gaze-based continuous authentication system [34]. They found that it is possible to achieve an accuracy comparable to using explicit stimuli [34].

To conclude, implicit user identification from eye gaze behaviour on smartphones has long been introduced, however, to the best of our knowledge, there are no studies that investigate eye gaze in real-world conditions and the factors influencing gaze behaviours. Our work bridges this gap, and introduces the utilisation of the time spent during smartphone unlocking to secure users' phones e.g. implicit gaze-based identification with no extra effort from users.

3 CONCEPT AND EVALUATION

We propose leveraging the time spent unlocking smartphones to collect gaze data implicitly. This gaze data can serve two purposes: firstly, as a second factor for user identification in a 2FA format, thereby enhancing security, and secondly, for implicit user authentication. Our work aims to address two research questions: **RQ1**: How does the unlock technique influence users' gaze behavior? And **RQ2**: How do the environment, user activity, gender, and age impact users' gaze behavior? To explore these questions, we developed an Android background application that records users' unlocks and their gaze data during each unlock. Below, we detail our data collection process and hypotheses. To obtain the data necessary for our analysis we ran a 24-hour in-the-wild user study where we collected users' eye gaze during smartphone unlocks. In the following, we explain the study design, apparatus, and procedure.

3.1 Study Design

To collect ecologically valid data, we conducted an in-the-wild study using a smartphone's front camera for gaze estimation. Our study involved the following *independent variables*: 1) participants' age, 2) gender, 3) environment (private vs public), 4) physical activity (still vs on foot), and 5) unlock technique (PIN, Pattern, Password, and Fingerprint). We investigated a set of 4 *dependent variables* 1) face visibility, 2) authentication duration, 3) eye gaze behavior, and 4) eyes on and out of the screen. The university ethics board approved the study design. To collect this data, we implemented a Hedgehog Android app. The following explains how we collected our data through our app- all data was stored on a University server.

User Gaze Data: We used the Seeso.io[1] API for gaze estimation, utilizing the smartphone's front camera. The API does not require calibration, which is an important factor in our field study. We know this will affect the accuracy, but in this work, we do not have specific areas of interest to investigate but rather the whole screen. The API also provides timestamped gaze data, categorized as Fixations and Saccades, along with information on face visibility and gaze directed both on and outside of the screen.

Unlock Technique: In the demographics form, we collect the unlocking technique used by users, focusing on four techniques: *PINs*, *Patterns*, *Passwords*, and *Fingerprint*.

User Environment: We analyse eye gaze behavior in two settings: 1) Public Spaces and 2) Private Spaces. Following Jackson's [16] definition, we define *Public Spaces* as *a place accessible to all people for their use and enjoyment*, and *Private Spaces* as *a place open only to those permitted by law or custom* [10]. Our hypothesis is that in private environments, participants will engage in more eye contact with the screen, given the perceived safety and reduced likelihood of shoulder surfing. We also anticipate lower face visibility in private environments due to users' seated posture, e.g., slouching, as noted by previous work [18]. To capture participants' environment, we use an experience sampling pop-up prompt after each unlock, inquiring whether they are currently in a private or public environment.

User Activity: In our study, we examine user activity, detecting states through gyroscope coordinates and estimating activity using the step detector values. User activity is categorised into three groups: 1) Still, 2) Active, and 3) In Vehicle. Our hypothesis suggests limited face visibility and reduced eye contact with the screen in the active state compared to other states.

User Age and Gender: At the beginning of the study, we collected information on users' age and gender. Past studies highlight diverse smartphone usage behaviors across age groups, with younger generations using phones for extended durations [7, 11]. Additionally, females tend to use smartphones for longer periods compared to males [7].

3.2 Recruitment, Participants and Procedure

We recruited 21 participants (11 females, 2 non-binary) through university mailing lists, word of mouth, and social media. Their ages ranged from 18 to 70 ($M = 36.62; SD = 15.57$). The diverse group represented various nationalities and academic backgrounds, including computer science, history, economics, engineering, and medicine. Seven participants wore glasses, and two used contact lenses. None had prior eye-tracking experience (rated 1 on a scale from 1 for novice to 5 for experienced), and their IT security expertise ranged from none to average. Participants received a study link to download our Android application from the university server. They completed the consent and demographics forms, including questions about their unlock technique. The application ran in the background for 24 hours, triggering a popup during each phone unlock to inquire about their environment. Participants were later asked to delete the application and received a 5-euro compensation.

3.3 Limitations

Using the smartphone's front camera for gaze estimation, our study couldn't analyse gaze behavior during FaceID unlock. Additionally, we couldn't prompt users with a swipe-to-unlock technique. We acknowledge unbalanced age and gender datasets, limiting the statistical tests for further data analysis.

4 GAZE BEHAVIOR FEATURES

We derive six gaze behavior characteristics from collected raw data by first calculating saccades and fixations. Fixations involve maintaining gaze on a specific location [29]. Saccades, rapid eye movements shifting the focal point, were defined as in [9]. We identified and used features reported in prior studies [4, 5]:

- **Fixation Count**: This feature provides the number of total fixations in each unlock.
- **Average Fixation Duration**: The average fixation duration per unlock attempt per user.
- **Total Fixation Duration**: The overall duration of gaze fixations on the screen during each unlock.
- **Average Saccadic Duration**: Time between consecutive fixations, providing the average duration per unlock.
- **Average Saccadic Length**: Similarly, the average distance between two fixations per unlock was calculated.
- **Total Gaze Distance Travelled**: Euclidean distance between each pair of fixations during each unlock, illustrating the total distance covered by the gaze.

5 RESULTS

We begin our analysis with an overview and then examine various factors' impact on users' gaze behavior. Given the assumed non-normal distribution of our data, we conducted non-parametric tests and reported mean values (M).

5.1 Data Analysis Overview

Using front cameras for gaze estimation at a sample rate of 30 Hz resulted in an average of 60 samples per user per unlock attempt, varying based on the technique—(min=30 samples for fingerprints, max=120 samples for passwords). This resulted to 46K samples across all participants and techniques. Five participants used PINs, two used passwords, three patterns, and nine used fingerprints. On average, participants took 6.33s for patterns, 5.94s for passwords, 4.51s for PINs, and 4.15s for fingerprints. Participants unlocked their phones an average number of 37.71 times (max=58, min=8).

[1]Seeso.io: https://seeso.io/

Table 1: Results per unlock attempt categorised by age group

Features	Below 40 Years		Above 40 Years	
	Mean	SD	Mean	SD
Unlock Duration	4.79	3	4.92	2.18
Avg Fix Count	53.14	34.70	48.96	32.90
Avg Fix Dur	46.30	13.53	35.70	6.83
Total Fix Dur	2151.65	1264.14	1688.94	1250.95
Avg Sacc Dur	44.41	11.26	34.97	5.92
Avg Sacc Length	154.37	39.99	142.94	41.92
Distance Travelled	6455.90	5197.76	6528.66	5327.46
Face Visibility %	29.27	13.27	53.18	4.69
Avg Gaze On Screen %	53.01	21.97	50.01	20.64

Table 2: Results per unlock attempt categorised by gender.

Features	Females		Males		Non-binary	
	Mean	SD	Mean	SD	Mean	SD
Unlock Duration	5.45	2.3	4.82	3.13	1.34	4.03
Avg Fix Count	55.99	39.03	56.54	23.88	11.31	0.73
Avg Fix Dur	44.08	16.75	40.17	6.53	51.21	12.88
Total Fix Dur	2121.85	1282.76	2251.35	1132.94	528.62	48.45
Avg Sacc Dur	42.15	14.12	39.66	6.11	47.53	7.93
Avg Sacc Length	155.44	47.32	134.97	19.88	191.8	6.49
Distance Travelled	7530.16	6473.68	6161.76	2672.77	1942.32	347.46
Face Visibility %	8.95	7.62	12.03	16.12	17.77	11.22
Gaze On Screen %	45.35	17.94	38.53	20.99	76.70	21.584

5.2 Effect of Age and Gender on Gaze behavior

We studied the impact of age and gender on users' gaze behavior during phone unlock attempts. For age analysis, we divided participants into two groups: those above and below 40 years old as research found that millennials stand out for their technology use compared to older generations [31]. Among the participants, 15 were below 40, and 6 were above 40. Findings showed that participants over 40 took a bit longer ($M = 4.92; SD = 2.18$) to unlock their phones than those below 40 ($M = 4.79; SD = 3$). Table 1 displays the average results of dependent variables by age groups. Participants above 40 generally had less gaze data, indicating less eye contact with the screen during unlocks compared to those under 40. However, participants over 40 scanned wider areas on the screen.For gender effects, among our participants (11 females, 8 males, and 2 non-binary), females took longer to unlock their smartphones ($M = 5.45; SD = 2.3$ seconds) compared to males ($M = 4.82; SD = 3.13$) and non-binary participants ($M = 1.36; SD = 4.03$). (cf., Table 2). Females had longer fixations and saccades, scanning wider areas despite a lower face visibility percentage. For both age and results, due to imbalanced gender samples, statistical tests were not conducted.

5.3 Effect of Unlock Technique on Gaze Behavior

In our participant pool, five used PINs, two opted for passwords, three used patterns, and nine relied on fingerprints for unlocking. Due to dataset imbalance, we grouped these techniques into:

- **Attentive Unlock Techniques** - sensitive to inattentive interaction, including PINs, Patterns, and Passwords.
- **Inattentive Unlock Techniques** - Less affected by inattentive interaction, exemplified by Fingerprints.

Table 3: Mann-Whitney test for the different authentication techniques, (Significant results in bold, P <.05)

Features	Inattentive Techniques		Attentive Techniques		Mann Whitney U Test	
	Mean	SD	Mean	SD	U	P
Unlock Duration	4.15	3.11	5.43	2.33	31	.091
Avg Fix Count	**39.87**	**40.22**	**62.91**	**23.52**	**18**	**.009**
Avg Fix Dur	46.29	17.41	40.52	7.59	44	.439
Total Fix Dur	**1558.01**	**1375.27**	**2438.92**	**966.71**	**17**	**.007**
Avg Sacc Dur	43.67	14.54	39.93	6.66	51	.778
Avg Sacc Length	158.57	52.47	144.30	22.247	50	.725
Distance Travelled	**6068.78**	**7245.50**	**6847.51**	**2183.61**	**25**	**.035**
Face Visibility %	13.29	14.86	8.85	7.62	49	.673
Gaze On Screen %	**23.53**	**23.87**	**83.33**	**18.94**	**45**	**.011**

Table 4: Wilcoxon signed rank test across the different activities, (Significant results in bold, P <.05)

Features	Still-state		Active-state		Wilcoxon Signed Rank Test	
	Mean	SD	Mean	SD	Z	P
Unlock Duration	5.58	3.63	3.96	3.07	-2.37	.018
Avg Fix Count	**44.58**	**28.78**	**37.07**	**36.70**	**-2.01**	**.04**
Avg Fix Dur	43.94	14.75	37.50	11.38	-1.81	.07
Total Fix Dur	**2121.59**	**1166.25**	**1588.04**	**1430.41**	**-2.25**	**.02**
Avg Sacc Dur	40.19	6.66	38.92	5.34	-0.52	.60
Avg Sacc Length	141.30	48.90	136.53	51.11	-0.52	.60
Distance Travelled	6193.56	5332.68	5292.91	3695.10	-0.20	.84
Face Visibility %	**26.47**	**7.18**	**9.24**	**3.17**	**-1.87**	**.046**
Gaze on Screen %	**34.25**	**4.67**	**18.13**	**5.7**	**-3.8**	**.042**

Conducting a Mann-Whitney test on independent samples, we found that, although inattentive unlocks were shorter as expected ($M = 4.15; SD = 3.11$) compared to attentive ones ($M = 5.43; SD = 2.33$), no statistically significant differences were observed ($P > .05$). However, the higher standard deviation in inattentive unlocks was due to a reported high failure unlock rate, also reported in literature [8]. Regarding gaze features, we identified statistically significant effects of the unlock technique on average fixation count ($U = 18, P = .009$), total fixation duration ($U = 17, P = .007$), and overall gaze traveled distance on the screen ($U = 25, P = .035$), suggesting increased attention to the screen. A statistically significant effect on gaze percentage on the screen was noted ($U = 45$, $P = .011$), with attentive techniques having more gaze on the screen ($M = 83.33; SD = 18.94$) than inattentive ($M = 23.53; SD = 23.87$), (cf., Table 3).

5.4 Effect of User Activity on Gaze behavior

To analyze users' gaze across activities, we used accelerometer and gyroscope data to categorize activities into two states:

- **Still-state** - almost no difference in acceleration and velocity.
- **Active-state** - differences in acceleration and velocity, further divided into on-foot and in-vehicle conditions (no incidents recorded in the in-vehicle condition).

Four participants lacked incidents for unlock in motion active-state, so they were excluded from activity data analysis. Most unlocks occurred in a still state ($M = 23.38; SD = 14.97$) compared to an active state ($M = 12.76; SD = 10.96$). A Wilcoxon signed-rank test revealed a statistically significant effect of users' activity on unlock duration ($Z = -2.37, P = .018$). Contrary to expectations,

Table 5: Wilcoxon signed rank test for gaze features across the different environments, (Significant results bold, P <.05)

Features	Public Environment		Private Environment		Wilcoxon Signed Rank Test	
	Mean	SD	Mean	SD	Z	P
Unlock Duration	4.88	2.54	4.27	2.34	-0.83	.27
Avg Fix Count	**42.87**	**39.06**	**52.81**	**28.34**	**-1.1**	**.022**
Avg Fix Dur	46.76	26.48	42.58	8.61	-0.93	.34
Total Fix Dur	2102.17	1377.56	2125.49	1230.86	-0.76	.44
Avg Sacc Dur	**39.57**	**5.70**	**40.40**	**6.88**	**-1.98**	**.048**
Avg Sacc Length	146.44	42.70	151.42	40.23	-0.02	.98
Distance Travelled	6341.35	3104.57	6841.06	5879.95	-1.15	.24
Face Visibility %	29.83	3.2	30.52	4.1	0.1	.776
Gaze on Screen %	**54.13**	**10.2**	**63.49**	**7.98**	**1.4**	**.029**

active states induce shorter unlock duration ($M = 3.96; SD = 3.07$) compared to still-states ($M = 5.58; SD = 3.63$), suggesting a more pronounced impact of the unlock technique on the unlock duration. For gaze data, a Wilcoxon signed-rank test showed a statistically significant effect of user activity on gaze. Users had more fixations while unlocking in a still state ($M = 44.58; SD = 28.78$) compared to an active state ($M = 37.07; SD = 36.70$) ($Z = -2.02, P = .044$). A significant effect of activity on total fixation duration was observed, with participants maintaining longer gaze durations in a still state ($M = 2121.59; SD = 1166.25$) compared to an active state ($M = 1588.04; SD = 1430.41$) ($Z = -2.25, P = .024$). Moreover, users' activity significantly affected face visibility ($Z = -1.87; P = .046$) and gaze on-screen percentage ($Z = -3.8; P = .042$), with active states resulting in lower face visibility and reduced gaze on-screen percentage (cf., Table 4).

5.5 Effect of Environment on Gaze Behavior

We categorized responses to the experience sampling pop-up into Public and Private environments. Four participants were excluded due to not having any unlock in public environments. Most unlocks occurred in private environments ($M = 26; SD = 17.15$) compared to public ones ($M = 9; SD = 9.43$). While unlocking took longer in public environments ($M = 4.88; SD = 2.54$) than in private ones ($M = 4.27; SD = 2.34$), the difference was statistically insignificant. The environment had a significant effect on fixation count ($Z = -1.1, P = .022$), with more fixations in private environments ($M = 52.81; SD = 28.34$) than in public ($M = 42.87; SD = 39.06$). A significant effect of the environment on saccadic duration was observed ($Z = -1.98, P = .048$), with longer saccades in private environments ($M = 40.40; SD = 6.88$) compared to public ($M = 39.57; SD = 5.70$). This suggests increased engagement and attention to the screen during unlocking in private environments. Participants demonstrated significantly more eye contact with the screen in private environments ($M = 63.49; SD = 7.98$) than in public ones ($M = 54.13; SD = 10.2$) ($Z = 1.4, P = .029$), Table 5.

Summary

Our findings highlight that age influences users' smartphone unlock behavior, particularly affecting face visibility and eye contact. Females in our sample exhibit limited face visibility but cover more screen areas with their gaze during unlocking. The unlocking techniques significantly impact users' eye contact with the screen and gaze behavior, reflected in fixation count and screen distance traveled. Moreover, user activity, specifically in a still state, has better face visibility and increases eye contact with the screen, leading to more fixations. Environmental factors also contribute to behavior variations, where unlocking in private environments was found to be associated with more fixations and eye contact with the screens.

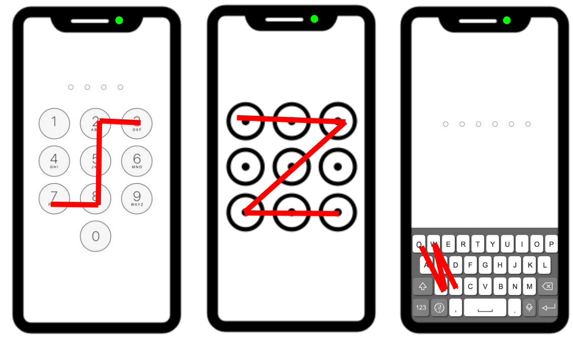

Figure 2: Arbitrary visualization of gaze behavior from participants across different unlock techniques.

6 DISCUSSION AND FUTURE WORK

6.1 User Authentication and Identification During Smartphone Unlock:

Our primary objective was to understand gaze behavior during smartphone unlocking to enhance security. We observed that users make more eye contact with their smartphone screens during attentive unlock techniques, we propose the integration of gaze as an additional factor for 2FA. This approach leverages users' natural tendency to follow their touch input during attentive unlocking, utilizing both touch and gaze inputs for a more robust security measure. Future research should investigate the uniqueness of user gaze behavior during the unlocking step as an opportunity for implicit identification and authentication. Recent research has explored variations in gaze behavior when users view images, suggesting its potential as an identification step before device unlocking [1]. Conversely, in the case of inattentive unlock techniques, users' eyes are relatively free, suggesting the possibility of implementing two-factor authentication by prompting users to provide a different eye input, enhancing security. Finally, future work could also look into splitting the unlock step into before, during, and after unlock and investigate each step individually, similar to Abdrabou et al. [4]. Then investigate the previously mentioned mechanisms and their suitability in each stage.

6.2 Gaze-Calibration During Phone Unlock

By visualizing participants' gaze paths on screens, we noticed a consistent pattern of following their fingers, particularly in attentive unlock techniques. This aligns with existing literature [3], where a study investigated visual angles across Android lock patterns.

Given our finding that users' gaze behaviors are significantly influenced by their chosen unlock technique, especially when following touch input for attentive unlocks, we recognize an opportunity to leverage this step for eye tracker calibration. Considering the growing prevalence of eye tracking in handheld devices and the time-consuming nature of eye tracking calibration, which interrupts users' primary activities, we propose using the unlock step for eye calibration. This would enhance the overall usability of eye tracking on smartphones [26]. Further research should explore how the unlock step can effectively calibrate eye trackers.

6.3 Gaze-Based Threat Models

The majority of our participants' gaze followed their touch input, particularly in attentive techniques. While acknowledging that our results are not validated by the participants since we did not collect their authentication data, distinctive gaze patterns emerged, notably during the entry of patterns, PINs, and passwords. This revelation unveils a novel threat model associated with continuous gaze tracking, wherein an adversary could potentially extract users' PINs, Patterns, and passwords from their gaze data if collecting raw gaze data and timestamps. Due to ethical considerations, we refrain from presenting specific gaze paths; however, a closely mimicked representation is depicted in Figure **??**, demonstrating similar gaze paths to those observed in our data analysis. It's essential to note that background elements were added for visualization purposes, as we lack certainty about specific locations on the screen. Nevertheless, the potential leakage of such data poses a significant risk to users. Even if it doesn't directly reveal their actual unlock method, it could narrow down possibilities for a brute force attack. This finding is particularly intriguing since, until now, eye gaze has primarily been utilized as a secure input technique protecting users from various attacks such as shoulder surfing [2, 12], thermal attacks [24], and smudge attacks [20], but it has not been explored as a potential threat model in its own right.

6.4 Challenges in Conducting Smartphone Gaze-behavior Studies

Throughout our work, we have seen participants are reluctant to take part in studies that collect user eye gaze. Similar to new forms of authentication or interaction (e.g. implicit authentication [21]), users have a limited understanding of what gaze data actually means. We have seen this during our recruitment phase, in the number of downloads of the app (85 link downloads) versus the final number of study participants who actually installed it and took part in the study ($n = 21$). Users need more transparency to be able to understand gaze data [6], and hence build more trust in such systems. This directs future research to explore different ways of communicating gaze data collection and its severity.

7 CONCLUSION

The paper introduces a novel approach by investigating users' gaze behavior during smartphone unlocking for potential gaze-based user identification and two-factor authentication. In a 24-hour in-the-wild study with 21 participants, the research explores the impact of environment, unlock technique, age, gender, and physical activity on users' eye gaze behavior. Findings highlight the significant influence of environment and physical activity on gaze behavior, with the unlock technique affecting face visibility. These insights deepen our understanding of factors shaping eye gaze adoption on smartphones and suggest directions for future research.

ACKNOWLEDGMENTS

This work was supported by the European Research Council (ERC) under the European Union's Horizon 2020 research and innovation programme (Grant No. 101021229, GEMINI: Gaze and Eye Movement in Interaction). It was also funded by dtec.bw – Digitalization and Technology Research Center of the Bundeswehr (Voice of Wisdom). dtec.bw is funded by the European Union – NextGenerationEU.

REFERENCES

[1] Yasmeen Abdrabou, Mariam Hassib, Shuqin Hu, Ken Pfeuffer, Mohamed Khamis, Andreas Bulling, and Florian Alt. 2024. EyeSeeIdentity: Exploring Natural Gaze Behaviour for Implicit User Identification during Photo Viewing. In *Proceedings of the Usable Security Mini Conference.*

[2] Yasmeen Abdrabou, Mohamed Khamis, Rana Mohamed Eisa, Sherif Ismail, and Amrl Elmougy. 2019. Just gaze and wave: exploring the use of gaze and gestures for shoulder-surfing resilient authentication. In *Proceedings of the 11th ACM Symposium on Eye Tracking Research & Applications* (Denver, Colorado) *(ETRA '19)*. Association for Computing Machinery, New York, NY, USA, Article 29, 10 pages. https://doi.org/10.1145/3314111.3319837

[3] Yasmeen Abdrabou, Ken Pfeuffer, Mohamed Khamis, and Florian Alt. 2020. GazeLockPatterns: Comparing Authentication Using Gaze and Touch for Entering Lock Patterns. In *ACM Symposium on Eye Tracking Research and Applications* (Stuttgart, Germany) *(ETRA '20 Short Papers)*. Association for Computing Machinery, New York, NY, USA, Article 29, 6 pages. https://doi.org/10.1145/3379156.3391371

[4] Yasmeen Abdrabou, Johannes Schütte, Ahmed Shams, Ken Pfeuffer, Daniel Buschek, Mohamed Khamis, and Florian Alt. 2022. "Your Eyes Tell You Have Used This Password Before": Identifying Password Reuse from Gaze and Keystroke Dynamics. In *Proceedings of the 2022 CHI Conference on Human Factors in Computing Systems* (New Orleans, LA, USA) *(CHI '22)*. Association for Computing Machinery, New York, NY, USA, Article 400, 16 pages. https://doi.org/10.1145/3491102.3517531

[5] Yasmeen Abdrabou, Ahmed Shams, Mohamed Omar Mantawy, Anam Ahmad Khan, Mohamed Khamis, Florian Alt, and Yomna Abdelrahman. 2021. GazeMeter: Exploring the Usage of Gaze Behaviour to Enhance Password Assessments. In *ACM Symposium on Eye Tracking Research and Applications* (Virtual Event, Germany) *(ETRA '21 Full Papers)*. Association for Computing Machinery, New York, NY, USA, Article 9, 12 pages. https://doi.org/10.1145/3448017.3457384

[6] Noora Alsakar, Yasmeen Abdrabou, Simone Stumpf, and Mohamed Khamis. 2023. Investigating Privacy Perceptions and Subjective Acceptance of Eye Tracking on Handheld Mobile Devices. *Proceedings of the ACM on Human-Computer Interaction* 7, ETRA (2023), 1–16.

[7] Ionut Andone, Konrad Błaszkiewicz, Mark Eibes, Boris Trendafilov, Christian Montag, and Alexander Markowetz. 2016. How age and gender affect smartphone usage. In *Proceedings of the 2016 ACM International Joint Conference on Pervasive and Ubiquitous Computing: Adjunct* (Heidelberg, Germany) *(UbiComp '16)*. Association for Computing Machinery, New York, NY, USA, 9–12. https://doi.org/10.1145/2968219.2971451

[8] Manuel Barbosa, Thierry Brouard, Stéphane Cauchie, and Simão Melo de Sousa. 2008. Secure Biometric Authentication with Improved Accuracy. In *Information Security and Privacy*, Yi Mu, Willy Susilo, and Jennifer Seberry (Eds.). Springer Berlin Heidelberg, Berlin, Heidelberg, 21–36.

[9] Marc D. Binder, Nobutaka Hirokawa, and Uwe Windhorst (Eds.). 2009. *Saccade, Saccadic Eye Movement.* Springer Berlin Heidelberg, Berlin, Heidelberg, 3557–3557. https://doi.org/10.1007/978-3-540-29678-2_5190

[10] Eugenie L. Birch. 2007. *Public and Private Space in Urban Areas: House, Neighborhood, and City.* Springer US, Boston, MA, 118–128. https://doi.org/10.1007/978-0-387-32933-8_8

[11] Christina Bröhl, Alexander Mertens, and Martina Ziefle. 2017. How Do Users Interact with Mobile Devices? An Analysis of Handheld Positions for Different Technology Generations. In *Human Aspects of IT for the Aged Population. Applications, Services and Contexts*, Jia Zhou and Gavriel Salvendy (Eds.). Springer International Publishing, Cham, 3–16.

[12] Alexander De Luca, Martin Denzel, and Heinrich Hussmann. 2009. Look into my eyes! can you guess my password?. In *Proceedings of the 5th Symposium on Usable Privacy and Security* (Mountain View, California, USA) *(SOUPS '09)*.

Association for Computing Machinery, New York, NY, USA, Article 7, 12 pages. https://doi.org/10.1145/1572532.1572542

[13] Małgorzata Hanzl and Slawomir Ledwon. 2017. Analyses of human behaviour in public spaces. *ISOCARP, Portland, Oregon, USA* (2017).

[14] Marian Harbach, Alexander De Luca, and Serge Egelman. 2016. 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*. 4806–4817.

[15] Marian Harbach, Emanuel Von Zezschwitz, Andreas Fichtner, Alexander De Luca, and Matthew Smith. 2014. {It's} a hard lock life: A field study of smartphone ({Un) Locking} behavior and risk perception. In *10th symposium on usable privacy and security (SOUPS 2014)*. 213–230.

[16] John B Jackson. 2018. The American public space. In *Classic Readings in Urban Planning*. Routledge, 300–307.

[17] Christina Katsini, Yasmeen Abdrabou, George E Raptis, Mohamed Khamis, and Florian Alt. 2020. The role of eye gaze in security and privacy applications: Survey and future HCI research directions. In *Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems*. 1–21.

[18] Mohamed Khamis, Florian Alt, and Andreas Bulling. 2018. The past, present, and future of gaze-enabled handheld mobile devices: survey and lessons learned. In *Proceedings of the 20th International Conference on Human-Computer Interaction with Mobile Devices and Services* (Barcelona, Spain) *(MobileHCI '18)*. Association for Computing Machinery, New York, NY, USA, Article 38, 17 pages. https://doi.org/10.1145/3229434.3229452

[19] Mohamed Khamis, Anita Baier, Niels Henze, Florian Alt, and Andreas Bulling. 2018. Understanding Face and Eye Visibility in Front-Facing Cameras of Smartphones used in the Wild. In *Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems* (<conf-loc>, <city>Montreal QC</city>, <country>Canada</country>, </conf-loc>) *(CHI '18)*. Association for Computing Machinery, New York, NY, USA, 1–12. https://doi.org/10.1145/3173574.3173854

[20] Mohamed Khamis, Mariam Hassib, Emanuel von Zezschwitz, Andreas Bulling, and Florian Alt. 2017. GazeTouchPIN: protecting sensitive data on mobile devices using secure multimodal authentication. In *Proceedings of the 19th ACM International Conference on Multimodal Interaction* (Glasgow, UK) *(ICMI '17)*. Association for Computing Machinery, New York, NY, USA, 446–450. https://doi.org/10.1145/3136755.3136809

[21] Masoud Mehrabi Koushki, Borke Obada-Obieh, Jun Ho Huh, and Konstantin Beznosov. 2021. On smartphone users' difficulty with understanding implicit authentication. In *Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems*. 1–14.

[22] Ahreum Maeng, Robin J Tanner, and Dilip Soman. 2013. Conservative when crowded: Social crowding and consumer choice. *Journal of Marketing Research* 50, 6 (2013), 739–752.

[23] Ahmed Mahfouz, Ildar Muslukhov, and Konstantin Beznosov. 2016. Android users in the wild: Their authentication and usage behavior. *Pervasive and Mobile Computing* 32 (2016), 50–61.

[24] Karola Marky, Shaun Macdonald, Yasmeen Abdrabou, and Mohamed Khamis. 2023. In the Quest to Protect Users from Side-Channel Attacks–A User-Centred Design Space to Mitigate Thermal Attacks on Public Payment Terminals. (2023).

[25] Veronica Muffato and Chiara Meneghetti. 2020. Knowledge of familiar environments: Assessing modalities and individual visuo-spatial factors. *Journal of Environmental Psychology* 67 (2020), 101387. https://doi.org/10.1016/j.jenvp.2020.101387

[26] Ken Pfeuffer, Melodie Vidal, Jayson Turner, Andreas Bulling, and Hans Gellersen. 2013. Pursuit calibration: making gaze calibration less tedious and more flexible. In *Proceedings of the 26th Annual ACM Symposium on User Interface Software and Technology* (St. Andrews, Scotland, United Kingdom) *(UIST '13)*. Association for Computing Machinery, New York, NY, USA, 261–270. https://doi.org/10.1145/2501988.2501998

[27] Lina Qiu, Alexander De Luca, Ildar Muslukhov, and Konstantin Beznosov. 2019. Towards understanding the link between age and smartphone authentication. In *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems*. 1–10.

[28] Lina Qiu, Ildar Muslukhov, and Konstantin Beznosov. 2016. Advancing the understanding of android unlocking and usage. In *Twelfth Symposium on Usable Privacy and Security (SOUPS 2016)*.

[29] Michele Rucci and Martina Poletti. 2015. Control and Functions of Fixational Eye Movements. *Annual Review of Vision Science* 1, 1 (2015), 499–518. https://doi.org/10.1146/annurev-vision-082114-035742 arXiv:https://doi.org/10.1146/annurev-vision-082114-035742 PMID: 27795997.

[30] Chen Song, Aosen Wang, Kui Ren, and Wenyao Xu. 2016. Eyeveri: A secure and usable approach for smartphone user authentication. In *IEEE INFOCOM 2016-The 35th Annual IEEE International Conference on Computer Communications*. IEEE, 1–9.

[31] Emily A Vogels. 2019. Millennials stand out for their technology use, but older generations also embrace digital life. (2019).

[32] Raphael Wimmer. 2010. Grasp sensing for human-computer interaction. In *Proceedings of the Fifth International Conference on Tangible, Embedded, and Embodied Interaction* (Funchal, Portugal) *(TEI '11)*. Association for Computing Machinery, New York, NY, USA, 221–228. https://doi.org/10.1145/1935701.1935745

[33] Niels Wouters, John Downs, Mitchell Harrop, Travis Cox, Eduardo Oliveira, Sarah Webber, Frank Vetere, and Andrew Vande Moere. 2016. Uncovering the Honeypot Effect: How Audiences Engage with Public Interactive Systems. In *Proceedings of the 2016 ACM Conference on Designing Interactive Systems* (Brisbane, QLD, Australia) *(DIS '16)*. Association for Computing Machinery, New York, NY, USA, 5–16. https://doi.org/10.1145/2901790.2901796

[34] Yongtuo Zhang, Wen Hu, Weitao Xu, Chun Tung Chou, and Jiankun Hu. 2018. Continuous authentication using eye movement response of implicit visual stimuli. *Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies* 1, 4 (2018), 1–22.