An Investigation of Shoulder Surfing Attacks on Touch-Based Unlock Events

STEFAN SCHNEEGASS, University of Duisburg-Essen, Germany
ALIA SAAD, University of Duisburg-Essen, Germany
ROMAN HEGER, University of Duisburg-Essen, Germany
SARAH DELGADO, University of the Bundeswehr, Germany
ROMINA POGUNTKE, KUKA Deutschland GmbH, Germany
FLORIAN ALT, University of the Bundeswehr, Germany

Fig. 1. User-centered attacks, such as shoulder surfing, are a common privacy threat. They occur in everyday situations; for example, while one is commuting or sitting in a park. We investigate these attacks using an augmented mobile phone system with a fisheye lens to extend the viewport of the front-facing camera capturing the current situation.

This paper contributes to our understanding of user-centered attacks on smartphones. In particular, we investigate the likelihood of so-called shoulder surfing attacks during touch-based unlock events and provide insights into users' views and perceptions. To do so, we ran a two-week in-the-wild study (N=12) in which we recorded images with a 180-degree field of view lens that was mounted on the smartphone's front-facing camera. In addition, we collected contextual information and allowed participants to assess the situation. We found that only a small fraction of shoulder surfing incidents that occur during authentication are actually perceived as threatening. Furthermore, our findings suggest that our notions of (un)safe places need to be rethought. Our work is complemented by a discussion of implications for future user-centered attack-aware systems. This work can serve as a basis for usable security researchers to better design systems against user-centered attacks.

Authors' addresses: Stefan Schneegass, University of Duisburg-Essen, Schuetzenbahn 70, Essen, Germany, 45127, stefan.schneegass@uni-due.de; Alia Saad, University of Duisburg-Essen, Schuetzenbahn 70, Essen, Germany, 45127, alia.saad@uni-due.de; Roman Heger, University of Duisburg-Essen, Schuetzenbahn 70, Essen, Germany, 45127, roman.heger@uni-due.de; Sarah Delgado, University of the Bundeswehr, Carl-Wery-Str. 20, Munich, Germany, 81739, sarah.delgado@unibw.de; Romina Poguntke, KUKA Deutschland GmbH, Zugspitzstrasse 140, Augsburg, Germany, 86165, Romina.poguntke@hs-kempten.de; Florian Alt, University of the Bundeswehr, Carl-Wery-Str. 20, Munich, Germany, 81739, florian.alt@unibw.de.

2573-0142/2022/9-ART207 $15.00
https://doi.org/10.1145/3546742

CCS Concepts: • **Security and privacy → Usability in security and privacy**; • **Human-centered computing → Empirical studies in HCI**.

Additional Key Words and Phrases: usable security and privacy; user-centered attacks; shoulder surfing; in-the-wild studies.

ACM Reference Format:
Stefan Schneegass, Alia Saad, Roman Heger, Sarah Delgado, Romina Poguntke, and Florian Alt. 2022. An Investigation of Shoulder Surfing Attacks on Touch-Based Unlock Events. *Proc. ACM Hum.-Comput. Interact.* 6, MHCI, Article 207 (September 2022), 14 pages. https://doi.org/10.1145/3546742

1 INTRODUCTION

Smartphones have become an integral part of our everyday life. We not only store sensitive data on our devices, such as photos, but we access sensitive information in the cloud through such devices (e.g., online banking, instant messages, emails). This creates an inherent need to protect smartphones from unauthorized access.

At the same time, authentication schemes commonly used on smartphones (e.g., PINs, lock patterns, and passwords) are susceptible to so-called user-centered attacks. Such attacks include (1) guessing attacks, in which impostors try to identify credentials by trying out all possible combinations (brute force) or by making well-educated guesses (smart guessing attacks), (2) reconstruction attacks, in which adversaries, who get access to a smartphone, try to reconstruct the password from cues left on the screen (e.g., oily or thermal residues), and (3) observation attacks. In observation attacks, adversaries try to observe credentials as users enter them on the smartphone. This attack is particularly popular because no technical means are required and opportunities occur frequently (i.e., during each authentication event).

Prior work has suggested modifications to existing knowledge-based authentication schemes and novel concepts, all of which aim to mitigate the aforementioned threats [9, 14, 15, 22, 26, 27]. However, many solutions tackle attacks in one specific situation, considering one specific threat model. What is still missing is solutions that consider different authentication contexts. Some approaches in this direction exist, for example, mechanisms taking users' location into account [29]. These omit the need for authentication if users are in a presumably safe environment, such as their home. However, the context is usually more complex. Examples for context information that could be considered include the number of people in close proximity, the time of the day, or the current (cognitive) state of the user.

The driving research question behind our work is how often shoulder surfing attacks toward mobile phones occur and how severe users perceive such attacks. To this end, we investigate the user's situation during authentication. To obtain an in-depth understanding of how shoulder surfing influences the security of common authentication schemes, we built a mobile app that obtains contextual information from (a) experience sampling and (b) the sensors of the smartphone. In addition, we record pictures during the authentication process with a modified 180-degree front-facing camera to support participants in a post-hoc assessment of the authentication situation. We then conducted a two-week in-the-wild study with twelve participants using the described app.

Our findings show that the opportunity for shoulder surfing-based observation attacks exists in about 10% of all authentication events. Familiar places (home, workplace) are particularly vulnerable, but incidents are not always perceived as threatening by users. Our results yield implications for the design of mechanisms that are robust against observation attacks and can serve as a basis for the design of more sophisticated context-aware authentication concepts.

Contribution Statement. The contribution of this work is twofold. First, we investigate shoulder surfing attacks during touch-based unlock events and provide insights into users‘ views and perceptions for real world authentication events. Second, we contribute a novel methodology to assess contextual information of potential shoulder surfing situations in-the-wild, providing insights beyond prior field studies employing traditional experience sampling.

2 BACKGROUND AND RELATED WORK

Observation attacks, such as shoulder surfing, are commonly referred to as user-centered attacks. These attacks refer to the observation of an individual entering their password by an attacker, without the individual's knowledge [5]. Such attacks – in contrast to malware [3, 18] – do not necessarily require malicious software to be installed on the device. Besides the physical observation, other means to conduct such attacks includes cameras placed in the environment or directly exploiting the mobile's camera to infer the password from interpreting the user's eye movement while entering a password [28] or inferring from the user's hand movement to the actual password [23]. As will be outlined below, this type of attack received considerable attention from the research community. Two aspects of previous work are of particular interest to our research. Firstly, we review approaches to mitigate observation attacks. Secondly, we summarize work that contributes to our understanding of observation attacks.

2.1 Mitigating Observation Attacks

Both the modification of existing and the development of novel authentication schemes were proposed to mitigate observation attacks. Papadopoulos et al. used a hybrid keypad to mislead the attacker from observing the correct PIN [17]. SwiPIN [26] requires users to enter the PIN according to a direction assigned to each digit, thus making input difficult for an adversary to observe. Similarly, Holz et al. [12, 13, 25] combine PIN and vibration.

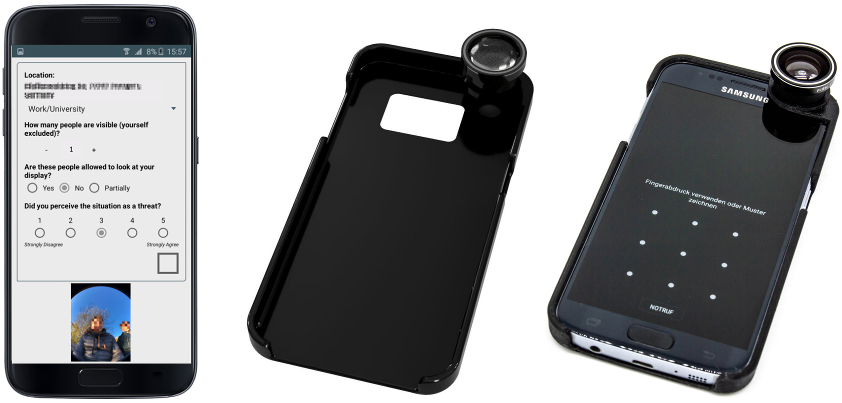
Further approaches focused on using other modalities, such as gaze [6, 14]. Gaze input makes shoulder surfing more difficult, since eye movements and input can hardly be perceived in parallel. Khamis et al. improved this approach by combining gaze and touch for PIN entry [9, 11]. This makes shoulder surfing also difficult for multiple attackers [10].

Summary. From this review we learn that a considerable amount of work is put into mitigating observation attacks. At the same time, the vast number of approaches did not yet find their way onto off-the-shelf smartphones. The reason might be that there is no universally viable solution yet and most approaches generate an overhead for the user. We believe that a better understanding of observational attacks – in particular an assessment of how users perceive the situation – could pave the way towards mechanisms that provide a more holistic protection against such attacks.

2.2 Understanding Observation Attacks

In contrast to mitigating observation attacks, little is known on the actual context of user-centered attacks. Harbach et al. were among the first to explore shoulder surfing as the most common type of user centered attack [8]. In a field study, they logged all authentication events and applied experience sampling to gain additional information on a subset of these events. Additionally, they used Amazon Mechanical Turk to conduct a survey on shoulder surfing. Results show that in about 25% of cases, smartphone users consider authentication as unnecessary. In addition, participants considered less than 1% of situation in which they were asked as risky. In contrast to our work, however, users neither gained information on whether and how many potential shoulder surfers were in their vicinity at the specific moment they unlocked the phone nor were supported in recalling a situation – which we do by providing a picture.

Eiband et al. [7] conducted a survey study, collecting user stories of shoulder surfing situations. The focus was on shoulder surfing in general. They found that the majority of shoulder surfing



8% 15:57

Location:

[redacted]

Work/University

How many people are visible (yourself excluded)?

- 1 +

Are these people allowed to look at your display?

○ Yes ● No ○ Partially

Did you perceive the situation as a threat?

1	2	3	4	5
○	○	●	○	○

Strongly Disagree *Strongly Agree*

□

Fig. 2. The rating application (left) and the smartphone enclosure including, fish-eye lens (center: rendered design, right: prototype).

incidents is opportunistic and most attackers focus on instant messaging and social networks. Using a 360° video displayed on a head mounted device, Saad et al. explored gaze behavior in shoulder surfing situations in a controlled lab experiment [20] showing that all users gazed on the phone. Simiarly, Abdrabou et al. investigate shoulder surfing in virtual reality [1] and aim at understanding how such attacks happen [2]. They identify three different stages including idle, approach, and attack. In a lab study, Bace et al. showed that viewing distance and angle influences the shoulder surfing feasibility [4]. In contrast, we assesses real world shoulder surfing incidents, bridging the gap between VR studies and survey based approaches.

Summary. We extend prior knowledge on user-centered attacks and contribute to state-of-the-art methodology. In particular, we employ a novel method that allows users to reflect on specific situations by means of images, hence increasing the ecologic validity of the insights.

3 INVESTIGATING USER-CENTERED ATTACKS

Prior work focused on designing countermeasures to shoulder-surfing attacks. At the same time, little work has been done to understand such attacks in real life settings. To close this gap, we (a) contribute an approach that assesses parts of the user's context while unlocking and (b) conducted an in-the-wild study employing the approach with the goal of obtaining an in-depth understanding of shoulder surfing attacks.

3.1 UCA Log Tool

We built a tool, supporting the assessment of contextual information of user-centered attacks (UCA log tool). It consists of two parts: a custom made mobile phone enclosure and an Android logging application (cf., Figure 2).

3.1.1 Mobile Phone Enclosure. We designed a custom enclosure for each participant in the study reported later in this paper, so that participants were able to use their own phone (cf., Figure 2). The mobile phone enclosure was 3D printed using a flexible TPU material and looked similar to off-the-shelf mobile phone protection cases. It includes notches for cameras, buttons, and ports. The enclosure also includes a fish-eye lens placed on the front facing camera. The lens extends the field of view of the camera from a range of 60 to 80 degrees to 180 degrees.

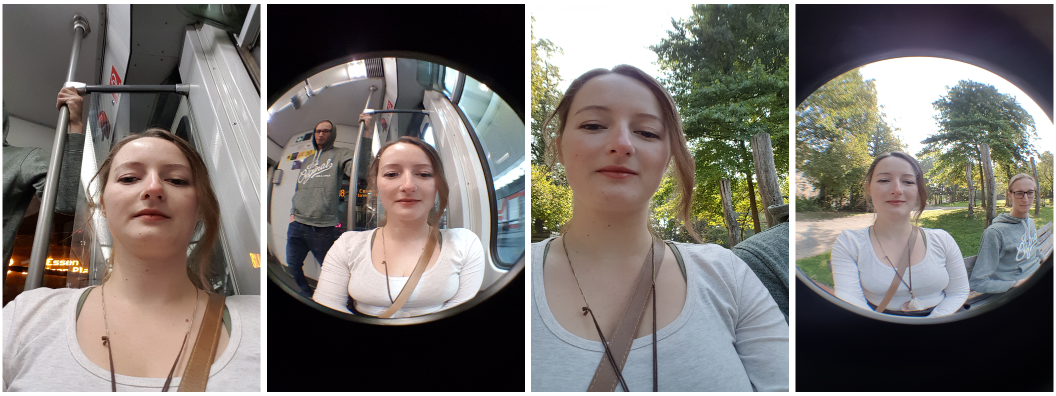


Fig. 3. Different fields of view of a mobile phone enclosure using a fish-eye lens, extending the front facing camera. Two staged situations in a train (left) and in a park (right).

3.1.2 Android Logging Application. The Android application consists of a logging service and a rating user interface.

Logging Service The service logs sensor data that help in understanding the context of each authentication event. Note, that at no point in the study credentials or characteristics thereof (e.g., password length) were logged. First, the service automatically takes a picture with the front facing camera at the moment the mobile phone is unlocked (i.e., the Android intent *USER_PRESENT* is received through a broadcast receiver). This picture – taken through the fish-eye lens – shows the surroundings of the participant and people potentially looking at the display during authenticating (Figure 3). We apply face detection using the Google Mobile Vision API[1], to extract the number of faces. This information is used by the rating interface (see below) to make a recommendation and, hence, ease the task of reporting the number of faces in the image by participants. In addition, we also record the timestamp and current GPS location of the smartphone, the latter of which is used to support the recall and assessment of the situation by the participant.

Rating Interface The interface allows participants to provide details on each authentication event (Figure 2). It shows a list of the pictures taken during all new authentication events (i.e., the ones not yet rated). Users can explicitly access the rating interface through the app. We also built a mechanism, reminding participants to rate the authentication events. We triggered a notification as soon as the user did not rate an event within two days.

As soon as participants select an authentication event, they can provide details. First, they can select the category of the current *location*. Categories are derived from Eiband et al. [7] and include home, public transport, theater or lecture hall, work or university, cafe or restaurant or bar, crowded place, public space, and others. Besides the image, we presented the address, extracted from the GPS coordinates, at the moment of unlock to support the assessment. Next, participant can select the *number of people* visible in the image. We pre-select this value using the result of the face detection to ease input. As soon as more than one person is detected (i.e., someone in addition to the participant), we add two additional questions, namely, if these people are *allowed to look at the screen* (yes, no, partly) and whether the participant perceived this situation as a *threat* (Likert item;

[1] Google Mobile Vision API: https://developers.google.com/vision/android/face-tracker-tutorial. A comparison of public cloud computer vision services showed that out of 450 human faces, the Google Mobile Vision API detected close to 100% correctly [24]. Actual numbers were determined by participants.

1=strongly disagree to 5=strongly agree). Last, a check-box indicates that everything is filled in properly. As the box is checked, the app shows the next unrated event.

The user interface also allows sharing data with researchers. Since authentication events happen in various situations in which automatically taking pictures might be inappropriate, we only stored images locally and did not upload them at any point. Rather, the interface generates a text file out of the logged data (excluding the images) and the user's rating. Next, the application triggers an Android intent that allows transmitting the data (e.g., through e-mail or instant messenger). We deliberately use this method to protect participants' privacy, that is (a) participants have full control over what is sent and when and (b) they can verify this (as opposed to, e.g., uploading to a server in the background).

3.2 In-the-Wild Study

We conducted a two week in-the-wild study in 2018. During this study, we logged all authentication events, that is when users entered their credentials to log into the smartphone, and let participants rate these events.

3.2.1 Recruiting and Demographics . We recruited 13 participants (8 female, 5 male; 12 right-handed, 1 left-handed) aged between 20 and 29 years ($M = 24.60, SD = 2.84$) via University mailing lists. The majority of participants hold a Bachelor's degree (7), A-level (3), or Master's degree (3).

3.2.2 Procedure. After participants arrived at our lab, we explained the purpose of the study, asked them to provide written informed consent to participate, and fill in a demographic questionnaire. Next, we asked participants whether they are familiar with the term shoulder surfing and, in case they were not, provided an explanation of this kind of attack (i.e., people who should not be allowed to look at the screen look at the screen). We then explained how the apparatus works and that it automatically takes pictures from the front facing camera to which we have no access at any time. Note that due to taking pictures automatically, people not being participants might have been captured in the pictures. As pictures were only temporarily stored on participants' phones and neither made available to researchers or the public, this is compliant with national privacy regulations of our country. The study received clearance from the <removed for anonymity> ethics board. Participants did not voice any concerns. Next, we equipped their phone with a specific enclosure and installed the Android app. If we did not have a fitting enclosure, we 3D printed one and provided it the next day. We also asked them to lock and unlock their phone so that we could briefly explain the app's interface.

After the study, participants returned to the lab to give back the enclosure. In case their phone still contained log data they had not yet shared we asked them to do so. Afterwards, we de-installed the app from their phones. At this point, any data collection ended. We remunerated each participant with € 10 plus € 1 for each day they rated all authentication events. If they rated all authentication events throughout the two weeks they received an additional € 10.

4 RESULTS

Our results are based on the data from 12 participants. We removed data from one participant as her phone broke during the study and, thus, we could not access the log file. On average, participants rated the situations within $Med = 9.4$ hours ($IQR = 1.9 - 25.9$ hours).

4.1 Unlock Events

First, we analyzed unlock events. Participants unlocked their phone in total 9145 times ($M = 54$/day, $SD = 34$) during the study. Each participant on average performed 754 events ($Min = 214$, $Max = 1793$, $SD = 437$) . We categorized authentication events based on location (Figure 4–left).

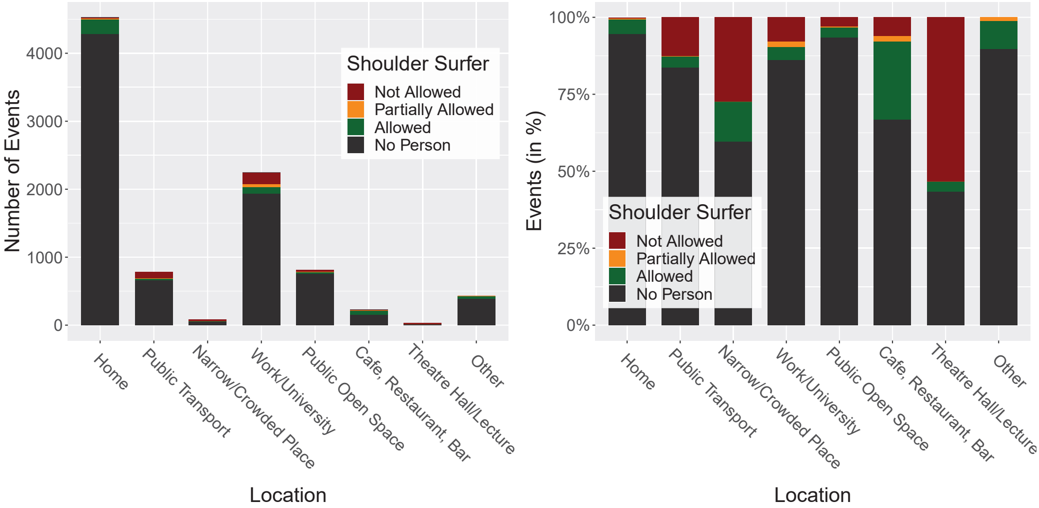


Fig. 4. Left: Distribution of authentication events based location. Login events mainly occurred at home and at work. Shoulder surfing events also occurred more often in these locations, compared to public locations. Notably, the majority of shoulder surfers at home were allowed to do so. Right: Percentage of authentication events per location. The likelihood of a shoulder surfing event to be done by a person not allowed to look at the phone is highest for lecture halls/theatres, narrow and crowded space, and in public transport. They are less likely at work/university, in cafes, restaurants and bars, as well as in open public spaces.

We thereby use the same categories as Eiband et al. [7]. Most unlock events occurred at home (50%), followed by participants' workplace or, in the case of students, at University (about 25%). Authentication in public space only contributes about 9% of unlock events.

4.2 Shoulder Surfing

Next, we looked at how often *opportunities for shoulder surfing* occurred and how they were distributed across events (see Figure 4; green, yellow, red bars). We found that in 918 ($M = 77$ per Person, $SD = 68$) out of the 9145 events, an additional person was visible (about 10%). Overall 1268 ($M = 106$ per Person, $SD = 122$) additional persons were visible. Thus, on average 1.4 additional persons are visible per shoulder surfed authentication event. When looking at the distribution of shoulder surfing events per location, we found that events occur most often in theatre halls / lectures, followed by narrow and crowded places, cafes, restaurants, and bars, and in public transport (see Figure 5–left).

Investigating whether shoulder surfers are *allowed to look at the user's display* (cf. Figure 5–left), users disagreed in 372 events, where only a single person was visible (not allowed – red) and in 65 events, where multiple people were visible (partially allowed – yellow). Events were classified as 'partially allowed' in cases where out of all people visible in the image there was at least one person for whom users disagreed that they were allowed to look at the display. Hence, in 437 cases out of 918 (48%) people were not allowed to look at the phone. We found that overall, shoulder surfing events mainly occurred at work / University, followed by at home and in public transport.

When looking at the percentages, for most shoulder surfing events at home or in cafes, restaurants and bars, people were allowed to look at the screen. In contrast, for shoulder surfing events in theatre halls / lectures, public transport, work / University and narrow / crowded places, a high percentage of people in the image were not allowed to look at the screen (cf. Figure 5–right).

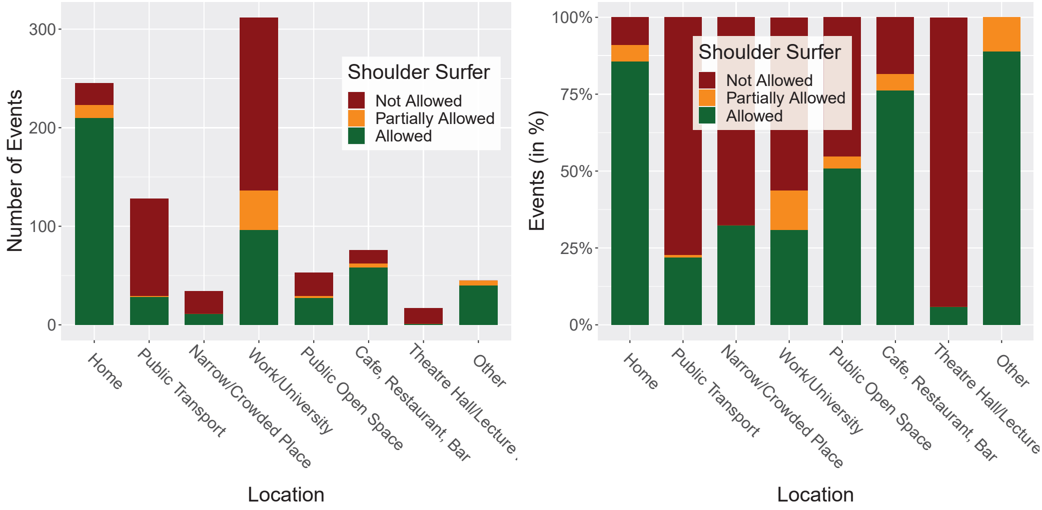


Fig. 5. Left: Distribution of shoulder surfing events per location and allowance to look at the phone. Shoulder surfing events mainly occurred at work/university, at home, and in public transport. Right: Percentage of shoulder surfing events per location. While a large number of shoulder surfing events occurred at home, users stated for most cases, that shoulder surfer were allowed to look at the phone. Also in cafes, restaurants and bars, the percentage of "allowed" shoulder surfers was rather high. In contrast, in theatre halls/lectures, in public transport, at work/university, and in narrow/crowded places the majority of shoulder surfers was not allowed to look at the screen.

4.3 Threats

Out of the 437 shoulder surfing events, the users rated 11 as a *threat* (i.e., ratings of "*Agree*" or "*Strongly Agree*" – cf., Figure 6). Most shoulder surfing events by people who were not allowed to look at the screen occurred at work / University and in public transport (Figure 6–left). Our findings are in line with findings from Harbach et al. that less than 1% of incidents are considered a threat [8]. When looking at which percentage of these were perceived as a threat (Figure 6–right), we found that this was rarely the case for events at work / University as well as in narrow/crowded places, and in theatre halls and lectures. In contrast, a large high percentage of events was perceived as a threat at home, in public transport and in public open space. We discuss these findings in the following section.

4.4 Times of the Day

The unlock events as well as the shoulder surfing incidents over time are depicted in Figure 7. We found that incidents are more likely to happen between 9 pm and 12 am (15.7%) and 9 am and 12 pm (12.9%) than between 5 pm and 8 pm (7.9%) and 6 am and 9 am (4.3%).

4.5 Limitations

We acknowledge the following limitations. The insights gained in this work are based on the results of 12 rather young participants (i.e. students). This might increase the number of events logged in the system given that younger people are more tech savvy (i.e., using the smart phone more often) and in general more likely to be active, travel using public transport (i.e., having more situations with strangers in their vicinity), and live more often in shared apartments.

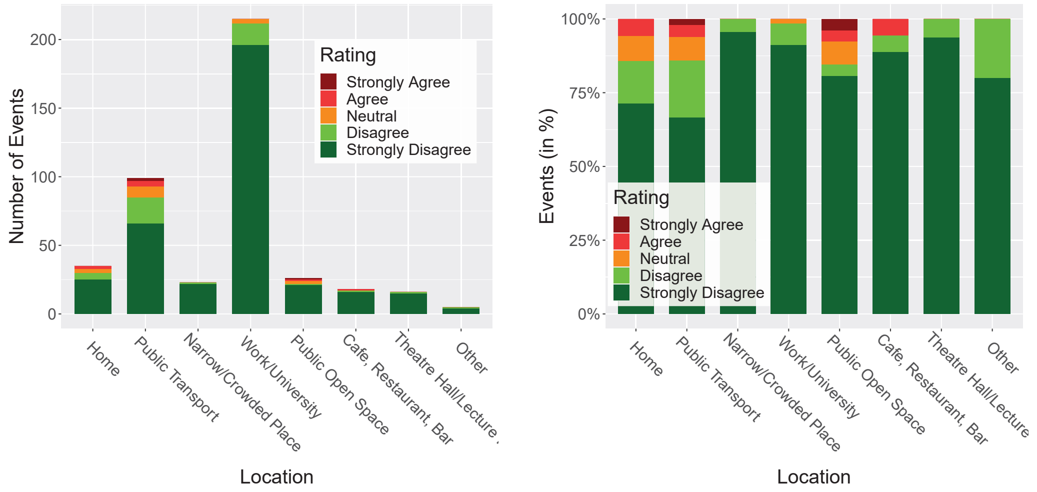


Fig. 6. Left: Distribution of shoulder surfing events by people who were not allowed to look at the screen and how much of a threat they were rated by users per location. Most situations occurred at work/university as well as in public transport. Right: Shoulder surfing events by people who were not allowed to look at the screen and how how much of a threat they were rated by users per location. While a high number of people who were not allowed looked at the screen of users at work/at University, the number of cases where this was perceived as threat was low. In contrast, a rather high percentage of shoulder surfing events at home, in public transport, and in public open spaces was considered a threat.

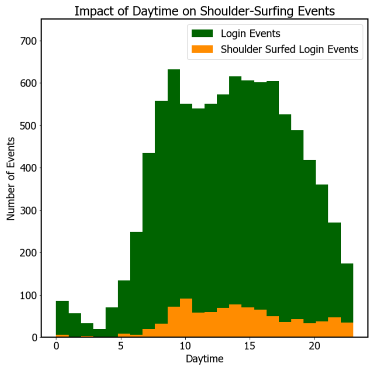


Fig. 7. Distribution of authentication events based on daytime. Login events peak in the morning and late afternoon. Shoulder surfing events occur more often in the morning and evening.

We only capture parts of the user's context. For example, we do not capture users' state of mind, tiredness, mood, or current task. Furthermore, the picture only provide a view of the scenery behind the user and not in front.

Given the nature of the in-the-wild study, we could not control the moment when participants rated the incidents. On average, participants rated the situations within $Med = 9.4$ hours and we additionally reminded them after 2 days. Within that time, participants might have forgotten details of the situation. Although we provided an image as memory aid, this could have affected their rating of the situation.

Another limitation concerns factors that influence the frequency of shoulder surfing events. Firstly, the additional enclosure, including the fish-eye lens, might have attracted additional attention, although we designed the enclosure to be as unobtrusive as possible. Secondly, since this was an in-the-wild study, we had no control over the fact that parts of the screen / the content might have been covered by participants' hands (i.e., hiding the PIN or password from attacker or not). Thirdly, the characteristics of participants' credentials (e.g., password length) could have affected attention towards the screen. Since we did not log this information for privacy reasons, we cannot rule out any effect.

We also do not know the exact times participants spend at each location. We did not continuously capture participants' location so as to not violate participants' privacy.

Finally, participants might have a different perception of which situations pose a threat to their phone. While we explained to participants what we mean by shoulder surfing during the briefing for the study, this perception could still be influenced by many factors. This could include users' general affinity to security / privacy, how well they recalled the situation they rated, or how they feel about security in the place in which the picture was taken. We might have captured several images or even a video during the authentication process to further help participants assess the situation – yet this could have raised further privacy concerns and added substantial effort for participants. Furthermore, the time between the unlock event and the users' rating ($Med = 9.4$ hours) might have influenced users' perception of the situation and, thus, the rating.

5 DISCUSSION

In the following, we discuss the implications of our work – in particular with regard to the design of mechanisms with the objective to mitigate user-centered attacks.

5.1 Cost-Benefit of User-Centered Attack-Aware Systems

Shoulder surfing has been perceived as a threat to the privacy of users' authentication credentials. At the same time, the number of shoulder surfing events perceived as threat is rather low – 11 out of 9145 authentication events have been rated as a threat. This confirms findings from prior work [8] and is in line with research showing that authentication is only one among many other targets of shoulder surfing [7]. This implies that designers of future approaches to mitigate user-centered attacks need to take into account the effort solutions generate for the user. In particular solutions that negatively influence usability or require user intervention should be applied with great care. For example, Schaub et al. found that keyboards with lower usability are harder to shoulder surf [21]. At the same time, users might not want to trade usability for security, in particular, since the number of shoulder surfing events perceived as threat is low.

Our findings contribute some insights here. For example, we found that for our participant group shoulder surfing occurs more frequently during particular times of day. Future approaches – specifically those requiring interventions – could account for this, for example, by being active in those contexts.

5.2 (Un)Safe Places and Contexts

We found that some users considered their home a potentially unsafe place, since a considerable number of the incidents they rated as threats occurred at home. There may be different reasons for this. More situations that are perceived as a threat to privacy might occur in shared flats or student dorms as opposed to situations in which users live together with their family. At the same time, prior research showed that social insider attacks, i.e. cases in which people snoop on others' smartphones, occur frequently in situations in which victim and attacker have a close relationship [16].

This suggests that previously introduced 'simplistic' contextual authentication mechanisms where, for example, a smartphone is automatically unlocked as it assumes the user is at home, may need to be rethought. We extended the knowledge about the context in our work. Yet, there are further contextual factors that could be investigated. Future research could also look more closely into when a place in particular or a context in general is considered safe or unsafe. Furthermore, the influence of the user's cognitive, emotional, or physical state could be considered. This might be useful, for example, for the design of mitigation strategies (i.e., a tired user might require more visible interventions). Subsequently, authentication concepts need to be re-designed to account for this.

5.3 UCA Awareness and other Apps

Knowledge of the smartphone about the risk caused by user-centered attacks has also implications beyond authentication mechanisms. Applications could directly benefit from this information. If the smartphone provided information on shoulder-surfing currently being possible, applications could directly respond to this, for example, by removing sensitive information or closing the app. However, doing so requires again an understanding of when users consider a threat important enough to do so. This is not obvious: note, we found very few cases in our study, in which the presence of others was considered a threat to smartphone authentication. One reason for this might have been that to really be an issue for the user, adversaries would need to get hold of the smartphone in addition to the credentials. For privacy-sensitive content, this is different, because in this case it is enough for the adversary to perceive the content (e.g., confidential information or compromising images).

6 FUTURE WORK: TOWARDS USER-CENTERED ATTACK-AWARE SYSTEMS

In the following we discuss aspects that, according to our findings, are relevant as we are designing novel concepts that are aware of user-centered attacks. We consider knowledge-based authentication as one important use case despite biometric approaches having gained popularity. Our findings are also relevant as shoulder surfing attacks are not only targeting authentication but various types of content and interaction [7].

6.1 Communicating Threats to the User

As the front-facing camera captures information on the user's current context, one question is, how to process this information. Several approaches have been proposed so far to communicate this information to the user [19]. However, the low number of shoulder surfing events perceived as threat in our study suggests that notifying the user each time shoulder surfing is possible is likely to become annoying quickly. Hence, a focus of future research could be how to *narrow down the number of events in which a threat is apparent* and only communicate these to the user. For example, a system could learn contexts in which shoulder surfing is ok (e.g., when friends or spouse are visible in the image).

6.2 Modifications to the Smartphone

One of the key tools for our study was the usage of a fish-eye lens to capture the environment behind the user. Having such a lens embedded in the next generation of smartphones, would be beneficial in combating observation attacks, as shoulder-surfing incidents could be identified in real-time. Adding such a camera would align with the current trend of augmenting smartphones with more and more cameras, both on the back and on the front of the phone. While the current purpose is to enhance image quality, enable stereo-vision and add artificial depth, improving security might be an interesting and beneficial new feature.

6.3 Opportunistic vs. Intentional Shoulder Surfing

In this work, we measured how often bystanders had the opportunity to look at the user's phone. While – from a security perspective – this should be considered as a potential attack, we do not have any insights whether or not the potential attacker (a) looked indeed at the phone and (b) had malicious intentions. Bystanders could have simply looked around or looked at the phone out of curiosity or boredom. Future work could investigate how malicious intent could be inferred from gaze data, for example, through the time gaze is directed at the phone or by assessing whether the same users repeatedly looks at the phone.

7 CONCLUSION

We presented our findings from a study that investigated user-centered attacks. In particular, we assessed information on the user's context while unlocking the smartphone by recording the scene from the front-facing camera. We also recorded the current location and used experience sampling to allow the users to further describe the situation. On the one hand, our findings provide specific recommendations with regard to how authentication concepts can be improved to be more robust against user-centered attacks. On the other hand, our findings suggest that some of the assumptions we make about the security (and perception thereof) need further investigation. Hence, our work should be of interest for designers of future shoulder surfing-aware concepts.

ACKNOWLEDGMENTS

This project is funded by the Deutsche Forschungsgemeinschaft (DFG, German Research Foundation – 425869382) and is part of Priority Program SPP2199 Scalable Interaction Paradigms for Pervasive Computing Environments. We further thank Sophie Ogando for her work on the initial prototype of the UCA Log Tool.

REFERENCES

[1] Yasmeen Abdrabou, Radiah Rivu, Tarek Ammar, Jonathan Liebers, Alia Saad, Carina Liebers, Uwe Gruenefeld, Pascal Knierim, Mohamed Khamis, Ville Mäkelä, Stefan Schneegass, and Florian Alt. 2022. Understanding Shoulder Surfer Behavior Using Virtual Reality. In *2022 IEEE Conference on Virtual Reality and 3D User Interfaces Abstracts and Workshops (VRW)*. 576–577. https://doi.org/10.1109/VRW55335.2022.00139

[2] Yasmeen Abdrabou, Sheikh Radiah Rivu, Tarek Ammar, Jonathan Liebers, Alia Saad, Carina Liebers, Uwe Gruenefeld, Pascal Knierim, Mohamed Khamis, Ville Makela, Stefan Schneegass, and Florian Alt. 2022. Understanding Shoulder Surfer Behavior and Attack Patterns Using Virtual Reality. In *Proceedings of the 2022 International Conference on Advanced Visual Interfaces* (Frascati, Rome, Italy) *(AVI 2022)*. ACM, New York, NY, USA, Article 15, 9 pages. https://doi.org/10.1145/3531073.3531106

[3] Milad Taleby Ahvanooey, Qianmu Li, Mahdi Rabbani, and Ahmed Raza Rajput. 2020. A Survey on Smartphones Security: Software Vulnerabilities, Malware, and Attacks. *CoRR* abs/2001.09406 (2020). arXiv:2001.09406 https://arxiv.org/abs/2001.09406

[4] Mihai Bace, Alia Saad, Mohamed Khamis, Stefan Schneegass, and Andreas Bulling. 2022. PrivacyScout: Assessing Vulnerability to Shoulder Surfing on Mobile Devices. In *Proceedings on Privacy Enhancing Technologies*, Vol. 1. 576–577.

[5] VA Brennen. 2005. Cryptography Dictionary.

[6] Heiko Drewes, Alexander De Luca, and Albrecht Schmidt. 2007. Eye-gaze Interaction for Mobile Phones. In *Proceedings of the 4th International Conference on Mobile Technology, Applications, and Systems and the 1st International Symposium on Computer Human Interaction in Mobile Technology* (Singapore) *(Mobility '07)*. ACM, New York, NY, USA, 364–371. https://doi.org/10.1145/1378063.1378122

[7] Malin Eiband, Mohamed Khamis, Emanuel Von Zezschwitz, Heinrich Hussmann, and Florian Alt. 2017. Understanding shoulder surfing in the wild: Stories from users and observers. In *Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems*. ACM, 4254–4265.

[8] Marian Harbach, Emanuel Von Zezschwitz, Andreas Fichtner, Alexander De Luca, and Matthew Smith. 2014. It's a hard lock life: A field study of smartphone (un) locking behavior and risk perception. In *Symposium on usable privacy and security (SOUPS)*. 213–230.

[9] Mohamed Khamis, Florian Alt, Mariam Hassib, Emanuel von Zezschwitz, Regina Hasholzner, and Andreas Bulling. 2016. Gazetouchpass: Multimodal authentication using gaze and touch on mobile devices. In *Proceedings of the 2016 CHI Conference Extended Abstracts on Human Factors in Computing Systems*. ACM, 2156–2164.

[10] Mohamed Khamis, Linda Bandelow, Stina Schick, Dario Casadevall, Andreas Bulling, and Florian Alt. 2017. They are all after you: Investigating the Viability of a Threat Model that involves Multiple Shoulder Surfers. In *Proceedings of the 16th International Conference on Mobile and Ubiquitous Multimedia*. ACM, 31–35.

[11] 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*. ACM, 446–450.

[12] Katharina Krombholz, Thomas Hupperich, and Thorsten Holz. 2016. Use the force: Evaluating force-sensitive authentication for mobile devices. In *Symposium on Usable Privacy and Security (SOUPS)*. 207–219.

[13] K. Krombholz, T. Hupperich, and T. Holz. 2017. May the Force Be with You: The Future of Force-Sensitive Authentication. *IEEE Internet Computing* 21, 3 (May 2017), 64–69. https://doi.org/10.1109/MIC.2017.78

[14] Manu Kumar, Tal Garfinkel, Dan Boneh, and Terry Winograd. 2007. Reducing shoulder-surfing by using gaze-based password entry. In *Proceedings of the 3rd symposium on Usable privacy and security*. ACM, 13–19.

[15] Taekyoung Kwon and Sarang Na. 2014. TinyLock: Affordable defense against smudge attacks on smartphone pattern lock systems. *computers & security* 42 (2014), 137–150.

[16] Diogo Marques, Ildar Muslukhov, Tiago Guerreiro, Luís Carriço, and Konstantin Beznosov. 2016. Snooping on Mobile Phones: Prevalence and Trends. In *Twelfth Symposium on Usable Privacy and Security (SOUPS 2016)*. USENIX Association, Denver, CO, 159–174. https://www.usenix.org/conference/soups2016/technical-sessions/presentation/marques

[17] A. Papadopoulos, T. Nguyen, E. Durmus, and N. Memon. 2017. IllusionPIN: Shoulder-Surfing Resistant Authentication Using Hybrid Images. *IEEE Transactions on Information Forensics and Security* 12, 12 (Dec 2017), 2875–2889. https://doi.org/10.1109/TIFS.2017.2725199

[18] Attia Qamar, Ahmad Karim, and Victor Chang. 2019. Mobile malware attacks: Review, taxonomy & future directions. *Future Generation Computer Systems* 97 (2019), 887–909. https://doi.org/10.1016/j.future.2019.03.007

[19] Alia Saad, Michael Chukwu, and Stefan Schneegass. 2018. Communicating Shoulder Surfing Attacks to Users. In *Proceedings of the 17th International Conference on Mobile and Ubiquitous Multimedia* (Cairo, Egypt) *(MUM 2018)*. ACM, New York, NY, USA, 147–152. https://doi.org/10.1145/3282894.3282919

[20] Alia Saad, Jonathan Liebers, Uwe Gruenefeld, Florian Alt, and Stefan Schneegass. 2021. Understanding Bystanders' Tendency to Shoulder Surf Smartphones Using 360-degree Videos in Virtual Reality. In *Proceedings of the 23rd International Conference on Human-Computer Interaction with Mobile Devices and Services* (Toulouse, France) *(MobileHCI '21)*. ACM, New York, NY, USA. https://dx.doi.org/10.1145/3447526.3472058

[21] Florian Schaub, Ruben Deyhle, and Michael Weber. 2012. Password Entry Usability and Shoulder Surfing Susceptibility on Different Smartphone Platforms. In *Proceedings of the 11th International Conference on Mobile and Ubiquitous Multimedia* (Ulm, Germany) *(MUM '12)*. ACM, New York, NY, USA, Article 13, 10 pages. https://doi.org/10.1145/2406367.2406384

[22] Stefan Schneegass, Frank Steimle, Andreas Bulling, Florian Alt, and Albrecht Schmidt. 2014. SmudgeSafe: Geometric Image Transformations for Smudge-resistant User Authentication. In *Proceedings of the 2014 ACM International Joint Conference on Pervasive and Ubiquitous Computing* (Seattle, Washington) *(UbiComp '14)*. ACM, New York, NY, USA, 775–786. https://doi.org/10.1145/2632048.2636090

[23] Diksha Shukla and Vir V. Phoha. 2019. Stealing Passwords by Observing Hands Movement. *IEEE Transactions on Information Forensics and Security* 14, 12 (2019), 3086–3101. https://doi.org/10.1109/TIFS.2019.2911171

[24] Jake Singh, Jackson Wheeler, Nicholas Fong, and Sanjeev Chaudhary. 2019. A Comparison of Public Cloud Computer Vision Services.

[25] Sebastian Uellenbeck, Thomas Hupperich, Christopher Wolf, and Thorsten Holz. 2015. Tactile One-Time Pad: Leakage-Resilient Authentication for Smartphones. In *Financial Cryptography and Data Security*, Rainer Böhme and Tatsuaki Okamoto (Eds.). Springer Berlin Heidelberg, Berlin, Heidelberg, 237–253.

[26] Emanuel Von Zezschwitz, Alexander De Luca, Bruno Brunkow, and Heinrich Hussmann. 2015. Swipin: Fast and secure pin-entry on smartphones. In *Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems*. ACM, 1403–1406.

[27] Susan Wiedenbeck, Jim Waters, Leonardo Sobrado, and Jean-Camille Birget. 2006. Design and evaluation of a shoulder-surfing resistant graphical password scheme. In *Proceedings of the working conference on Advanced visual interfaces*. ACM, 177–184.

[28] Longfei Wu, Xiaojiang Du, and Xinwen Fu. 2014. Security threats to mobile multimedia applications: Camera-based attacks on mobile phones. *IEEE Communications Magazine* 52, 3 (2014), 80–87. https://doi.org/10.1109/MCOM.2014.6766089

[29] Feng Zhang, Aron Kondoro, and Sead Muftic. 2012. Location-based authentication and authorization using smart phones. In *2012 IEEE 11th International Conference on Trust, Security and Privacy in Computing and Communications*. IEEE, 1285–1292.

Received February 2022; revised May 2022; accepted June 2022