Communicating Shoulder Surfing Attacks to Users

Alia Saad[1,2], **Michael Chukwu**[2], **Stefan Schneegass**[2]
[1]German University in Cairo, Cairo, Egypt, Alia.khaled@guc.edu.eg
[2]University of Duisburg-Essen, Essen, Germany, stefan.schneegass@uni-due.de

ABSTRACT
Since mobile interaction takes place in almost every context, shoulder surfing attacks are becoming more and more a threat to user's privacy. While several approaches exist to prevent these attacks for the authentication process, protecting the actual interaction has not yet been in the main focus of research. In this work, we present the concept of communicating shoulder surfing attacks to the user. This should create awareness on the user side and help preventing this type of privacy invasion. We present out shoulder surfer detection mobile application, called DSSytem, and report on a focus group that helped to design this system. We also report on the results of a user study in which we compare four different notification methods, namely, vibro-tactile, front LED, on-screen icon, and video preview feedback. Vibro-tactile feedback results in the lowest reaction time of the participants and is also favoured throughout the follow-up semi-structured interviews.

CCS Concepts
•**Security and privacy** → **Usability in security and privacy;**

Author Keywords
Shoulder Surfing; Notification; Usable Security and Privacy.

INTRODUCTION
Mobile devices are essential in modern day life. They are used to handle private information, communicate with family and friends, and store pictures of recent life events. While classical desktop computers are mainly used at home, mobile devices are used in various public situations. This results in novel challenges for protecting the user's content since unauthorized bystanders can peek on the mobile's display. These so called shoulder surfing attacks [24] can be used to gain insights on the user's passwords but also on other private information. Thus, shoulder surfing is considered to be one of the most severe threats to an individual's privacy [12].

Most of the recently introduced countermeasures are directed towards protecting the user authentication process since it is one of the most crucial moments from a security perspective. These previous solutions varied from gaze-based passwords, graphical unlock patterns, gestures for authentication to the deployment of external hardware [2, 7, 12, 15]. While such approaches are efficient in preventing the shoulder surfer from capturing and figuring out the authentication credentials, they do not protect the entire interaction of the user.

MUM '18, November 25–28, 2018, Cairo, Egypt

ISBN 978-1-4503-6594-9/18/11…$15.00

DOI: https://doi.org/10.1145/3282894.3282919

Figure 1. An attacker is shoulder surfing while a user is interacting with the phone.

In this work, we investigate how we can protect the entire interaction of a user with the mobile phone from shoulder surfing attacks. One of the main challenges of preventing shoulder surfing attacks is to perceive that attacker. This is challenging when the attacker is positioned at a blind spot, either at the back or at the sides of the user. To tackle this challenge, we present DSSytem, a system that detects shoulder surfers and notifies the user on such an attack. It uses the front facing camera of the mobile device to detect shoulder surfers peeking from behind the user and notifies the user using four different feedback methods, namely, vibro-tactile feedback, front LED blinking, iconic screen overlay, and live video stream. We report on the user-centered design process of DSSytem and an evaluation comparing the different feedback methods.

CONTRIBUTION STATEMENT
The contributions of the paper are presented as follows:

1. The design and implementation of a notification system that detects and communicates the event of shoulder surfing to users.

2. A comparison between four notification approaches to define the most suitable form of communication of shoulder surfing incidents, following users' preferences.

RELATED WORK

Shoulder Surfing likeliness

Detecting shoulder surfing, the act of over the shoulder observation of an individual personal information, is a difficult task. Its likeliness however has been widely researched in more than the last decade, ever since the first release of the early touch screen phones. Eiband et al. [5] studied this action in the wild by conducting an exploratory survey about shoulder surfing experiences. The majority of the participants(48.3%) admitted that they were observers of others' personal information, 33.3% indicated that they were the users and only 7% of the observers confirmed that they were noticed by the users. The study also showed that most of the shoulder surfing incidences do not occur on purpose but merely on opportunistic situations. A study by Harbach et al. [6] showed that only 0.3% of the time shoulder surfing was perceived as a serious risk [6]. However, both of the previously mentioned studies were mainly based on the authentication process. One of the automated implementations was a design of a three phases automated shoulder surfing attack for the iPhone [16]. Ye et al. proposed a video-based shoulder surfing attack to track finger movement to reconstruct the unlock pattern from a distance that can reach up to 2 meters away, in less than the legitimate Android's 5 attempts [25, 26]. Another novel shoulder surfing technique was presented by Abdelrahman et al. [1], where the attacker uses a thermal camera to reconstruct passwords from the heat traces left directly after authentication.

Authentication approaches tackling shoulder surfing

PIN, passwords, and graphical unlock patterns, though their usability, do not offer robust and secure solutions, especially in the case of shoulder surfing. Therefore, there is a necessity to overcome this problem by developing supplementary methods that enhance the security of such verification approaches. Typically, Personal Identification Number (PIN) is using a 4-digit number to unlock the phone, or use at a bank's ATM. Studies showed that PIN entry is more vulnerable to shoulder surfing than graphical passwords [11].

Many approaches tackled this issue and developed methods to overcome the vulnerability problem while maintaining the usability of PIN code. Papadopoulos et al. used a hybrid keypad that could only be correctly perceived by the user at a close distance, preventing the attacker from learning the PIN code [18]. Assigning a pressure value to each of the digits was another method to prevent shoulder surfing attacks [13, 14]. Eye gaze-based methods are used to improve the security level of PIN entry against shoulder surfing attacks [4, 15]. This can be done using relative eye movements which does not require calibration [3]. SwiPIN [23] is another method of applying basic gestures to mislead the a shoulder surfer from noticing the PIN code. Kumar et al. reduced shoulder surfing by using gaze-based password entry, instead of using the regular keyboard [15]. It was assumed that an attacker cannot look at both the authentication screen and user's eyes concurrently. This study showed significant performance with a relatively small error rate and user acceptance was above 80%. Graphical passwords, such as Android unlock pattern and image-based passwords are other ways for a secure yet usable authentication approaches [17, 19].

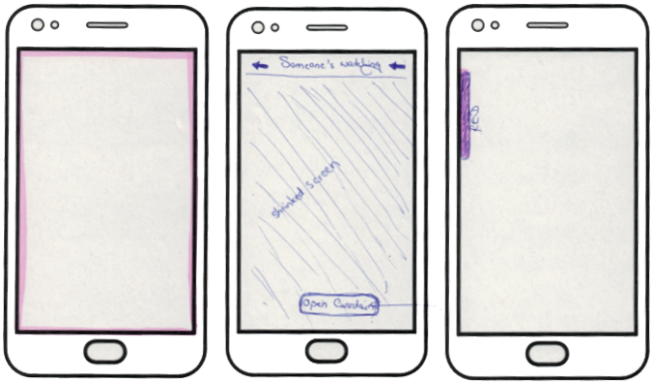

Figure 2. Examples of proposed methods of communicating shoulder surfing to users.

There are also multimodal scheme that target shoulder surfing like GazeTouchPass and GazeTouchPIN [8, 10] where a combination of gaze-based and PIN or password entry was implemented to distract the shoulder surfer from learning the access key. Such multimodals have also proved resilience against another major issue of multiple shoulder surfers [9], where a group of more than one of shoulder surfers is teamed up targeting a single victim.

COMMUNICATING SHOULDER SURFING INCIDENTS

The main idea of our work is to communicate the shoulder surfing incidents to the user. To understand what potential means of communication can be used, we conducted a focus group to generate design alternatives. Further, we aim at assessing additional user requirements.

Focus Group

We conducted a focus group to gain insights into how we can communicate a shoulder surfing event to the user. We invited five participants (3 females, 2 males), aged between 22 and 29 years ($M = 25.4$, $SD = 3.2$), to take part in the focus group.

At first, we focused on shoulder surfing as a potential privacy threat. All participants agreed that their threat perception is depending on the nature of the application currently using and its content.The more critical the application, such as banking application, the more concerned the participants become. Second, we asked about modalities to be used to communicate shoulder surfing. The first idea was using vibration to not interfere with the visual content on the display.While some participants viewed it as acceptable, others saw that they would be annoyed with a frequent vibration of the mobile. Next different visual notifications were discussed and we asked the participants to sketch them. Examples of the sketches are depicted in Figure 2. Participants suggested that potential ways of communicating such events could be the LED flash light on the front of the mobile, a (toast) message on the display, a notification icon, a red boarder on the screen, or showing a preview of the attacker. One participant suggested that the boundaries of the display should change color when an attacker is perceived. Second example advised that the display should be dimmed and in the third example it was proposed that only a section of the display changes color according to the adversary's position.

Figure 3. DSSytem interface in case of shoulder surfing: LED flash light is on(Left), a preview of the front camera appears (second to left) , vibration(second to right) and icon overlay (right)

Next, we focused on details of the shoulder surfing attack that should be communicated in addition to the fact of being shoulder surfed in general. Participants mentioned the direction and distance of the attacker plays an important role. Further, the amount of time of being shoulder surfed is important since it can differentiate a brief peek from a more privacy invading reading of content.

We also wanted to know if the shoulder-surfing event should also be communicated to the attacker. Most participants agreed that it is fine to let the attacker know that he or she was detected. This could also be done to create social pressure and, thus, prevent the attacker from further looking on the phone. Finally, 2 participants said that it is preferred that the system should automatically perform countermeasures such as locking the phone, switching off the display, or changing the screen brightness. However, the other 3 participants favoured that the user should entirely stay in control to take the action rather than the phone itself.

Overall, participants mentioned different means of communicating shoulder surfing events. They all agreed that it is important to not disturb the user in its current task and keep the user in control. Based on these findings, we designed DSSytem.

DSS-SYSTEM: DETECT SHOULDER SURFER SYSTEM

We developed an Android application that targets the challenges of shoulder surfing among Android mobile phone users during and after authentication process. The application runs as a background service that periodically takes pictures using the front facing camera. We use the face tracking capabilities of the Android vision API[1] to detect faces and, thus, potential shoulder surfers.

In this application, we communicate shoulder surfing attacks to the user so that a proper reaction should be taken (tilting the device, closing the current action, etc.). We implemented four different notification types: (1) front LED switches, (2) vibro-tactile feedback, (3) iconic on-screen visualization, and (4) a live preview of the front facing camera. All four notification types are depicted in Figure 3. Each feedback is presented as soon as an attacker is detected until the attacker is no longer detected.

[1] https://developers.google.com/vision/

STUDY

In this section, we compare the design of the four different feedback modalities gathered in the focus group.

Participants and Procedures

We invited 10 participants (1 female, 9 male), aged 18 to 50 years ($M = 25.69$, $SD = 8.04$) to participate in our user study. All participants had prior experience with smart phones. However, we had to exclude one participant due to technical reasons (i.e., a missing log file).

After the participants arrived at the lab, we first introduced them to the purpose of the study and asked them to fill in an informed-consent form. Next, we handed them a smart phone (Huawei Mate 10 Lite) with a wide-angle lens attached to the front facing camera and introduced them to a specific task they should perform. The main purpose of this task was to distract them from the surrounding and, thus, create a more realistic environment for the study. The task was to go through an image gallery of 66 pictures and answer certain questions asked by the experimenter (e.g., "How many red cars are in the pictures?"). While the user is busy with this task, one experimenter sneaked behind the user and shoulder surfed the participant (cf., Figure 1). The system detects the shoulder surfer and notifies the user with one of the four feedback methods. Each feedback method is presented three times and the order of the feedback methods is chosen based on a latin square. As a performance measure, we logged how long the participants needs to detect the attacker and make an action as countermeasure to the attack. Once notified, the user is asked to switch off the display to acknowledge that he or she detected a shoulder surfer. After the task, we asked the participants to fill in a user experience questionnaire and rate the four methods. Further, we conducted semi-structured interviews. The overall study lasts for about 30 minutes.

Results

The key element for our data analysis is the user's response time after being notified with the shoulder surfing event (i.e., the time the user takes between notification and and switching off the display). Results show that vibro-tactile feedback took the least time with value ($M = 2.30s$, $SD = 1.27$), followed by front LED ($M = 2.80s$, $SD = 0.98$) and on-screen overlay ($M = 3.23s$, $SD = 1.86$). The notification method with the highest response time is the preview of the front-facing camera ($M = 5.07$, $SD = 2.03$). Figure 4 depicts the results of the

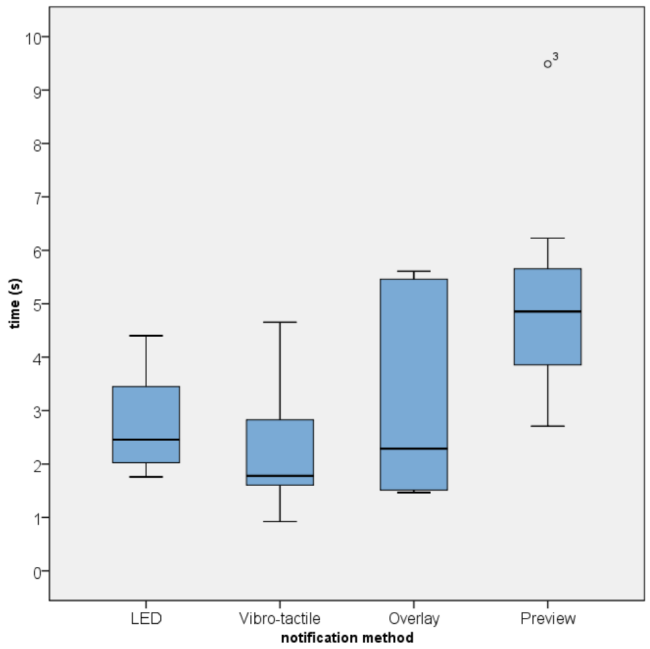

Figure 4. Boxplot of the reaction time (in s) of the different feedback methods.

study. A repeated measured analysis of variance (ANOVA) shows a statistically significant difference between the feedback methods, $F(3,24) = 10.537$, $p = .000$. Holm-Bonferroni corrected pairwise comparisons of the feedback methods show that the preview of the front-facing camera is statistically significant slower compared to the other feedback methods ($p_{Vibration} = .001, p_{LED} = .002, p_{Overlay} = 0.032$). All other comparisons could not find a statistically significant difference ($p > .050$).

When asked about the level of annoyance of each method, most of the participants agreed that the four approaches were not annoying nor distracting However, all participants agreed that vibration was the least annoying of the four methods. We also asked the participants about the notification modality they preferred the most, six of the participants recommended vibration. The choice was based on the subtle nature of the vibration as it notifies only the user and not the shoulder surfer. Finally, seven of the users preferred to have automated countermeasures on their devices. Choices varied mostly between locking the phone and changing display's brightness. Participants also suggested that smart devices should be aware of the context. A system should be able to recognize a friend and should consider the distance in addition to the dwell time of the extra perceived person.

DISCUSSION

Privacy vs. Privacy

Our approach uses the front facing camera in combination with face detection to protect the privacy of the user. This, however, provides a contradicting approach since the fact of running face-detection algorithms in public potentially infers with the privacy of others. Although – throughout the focus group and user study – none of the participants complaint about this potential implication of our approach, such an approach needs to be thoughtfully designed to not give up more privacy than we protect.

Notification Method

The results show that non-visual feedback is preferred by the user and performs fastest. However, it also has inherent drawbacks such as having a limited amount of information that can be transferred. Particularly with the results of the focus group, it might be beneficial to communicate more information than the fact that the attack is happening. Additionally, the user needs to be able to differentiate the feedback from other sources of vibro-tactile feedback. This could be achieved by employing a specific vibration pattern that reflects shoulder surfing incidents. However, this still needs to be investigated in future work.

User control

One of the key discussions in the focus group as well as in the interviews was on who should be in control of initiating a countermeasure. Interface design guidelines suggest that the user should be in control of the system [22]. While participants argued that they would also like to stay in control all the time for such an application, others indicated that the system would be more efficient in initiating countermeasures by itself. Thus, we need further investigate whether users are fine with being not in control and using other interaction approaches instead (e.g., intervention-based interaction [20]).

Technical Limitations

The camera angle of nowadays front-facing cameras of smart phones is rather limited. Thus, We conducted the study using a fish-eye lens on the front-facing camera to extend the viewing angle of the camera. This is currently not practical for everyday interaction. However, including such a lens in the mobile device itself can easily be achieved. Additionally, the fact that a face is detected does not automatically imply that the person is also shoulder surfing the user. Thus, a gaze estimation model needs to be developed that detects whether or not the potential attacker is looking at the user's phone.

CONCLUSION

In this work, we present the concept of notifying the user on shoulder surfing attacks. We report on the design and implementation of DSSytem that uses face detection to automatically detect shoulder surfer and notifies users with four different notification methods based on results of a focus group. Additionally, we report on a user study that shows that vibro-tactile feedback is superior compared to other feedback modalities. While securing the authentication process of mobile devices against shoulder surfing receives considerable attention (e.g., through various forms of biometrics [21]), the interaction process is still prone to this kind of attacks. With this paper, we work towards protecting the user against shoulder surfing attacks throughout the entire interaction process.

ACKNOWLEDGEMENT

This research is funded by the DAAD within the context of the Computing for Intercultural Competences (ComIC) project.

REFERENCES

1. Yomna Abdelrahman, Mohamed Khamis, Stefan Schneegass, and Florian Alt. 2017. Stay Cool! Understanding Thermal Attacks on Mobile-based User Authentication. In *Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems (CHI '17)*. ACM, New York, NY, USA, 3751–3763. DOI: http://dx.doi.org/10.1145/3025453.3025461
2. 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 *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*. ACM, 2937–2946.
3. Alexander De Luca, Roman Weiss, and Heiko Drewes. 2007. Evaluation of eye-gaze interaction methods for security enhanced PIN-entry. In *Proceedings of the 19th australasian conference on computer-human interaction: Entertaining user interfaces*. ACM, 199–202.
4. 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 (Mobility '07)*. ACM, New York, NY, USA, 364–371. DOI: http://dx.doi.org/10.1145/1378063.1378122
5. 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.
6. 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.
7. Feng Hong, Meiyu Wei, Shujuan You, Yuan Feng, and Zhongwen Guo. 2015. Waving Authentication: Your Smartphone Authenticate You on Motion Gesture. In *Proceedings of the 33rd Annual ACM Conference Extended Abstracts on Human Factors in Computing Systems (CHI EA '15)*. ACM, New York, NY, USA, 263–266. DOI: http://dx.doi.org/10.1145/2702613.2725444
8. 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.
9. Mohamed Khamis, Linda Bandelow, Stina Schick, Dario Casadevall, Andreas Bulling, and Florian Alt. 2017a. 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.
10. Mohamed Khamis, Mariam Hassib, Emanuel von Zezschwitz, Andreas Bulling, and Florian Alt. 2017b. 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.
11. David Kim, Paul Dunphy, Pam Briggs, Jonathan Hook, John W Nicholson, James Nicholson, and Patrick Olivier. 2010. Multi-touch authentication on tabletops. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*. ACM, 1093–1102.
12. Sung-Hwan Kim, Jong-Woo Kim, Seon-Yeong Kim, and Hwan-Gue Cho. 2011. A new shoulder-surfing resistant password for mobile environments. In *Proceedings of the 5th International Conference on Ubiquitous Information Management and Communication*. ACM, 27.
13. 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.
14. 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. DOI: http://dx.doi.org/10.1109/MIC.2017.78
15. 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.
16. Federico Maggi, Alberto Volpatto, Simone Gasparini, Giacomo Boracchi, and Stefano Zanero. 2011. Poster: Fast, automatic iphone shoulder surfing. In *Proceedings of the 18th ACM conference on Computer and communications security*. ACM, 805–808.
17. Wendy Moncur and Grégory Leplâtre. 2007. Pictures at the ATM: exploring the usability of multiple graphical passwords. In *Proceedings of the SIGCHI conference on Human factors in computing systems*. ACM, 887–894.
18. 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. DOI: http://dx.doi.org/10.1109/TIFS.2017.2725199
19. Florian Schaub, Marcel Walch, Bastian Könings, and Michael Weber. 2013. Exploring the design space of graphical passwords on smartphones. In *Proceedings of the Ninth Symposium on Usable Privacy and Security*. ACM, 11.

20. Albrecht Schmidt and Thomas Herrmann. 2017. Intervention User Interfaces: A New Interaction Paradigm for Automated Systems. *interactions* 24, 5 (Aug. 2017), 40–45. DOI: http://dx.doi.org/10.1145/3121357
21. Stefan Schneegass, Youssef Oualil, and Andreas Bulling. 2016. SkullConduct: Biometric user identification on eyewear computers using bone conduction through the skull. In *Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems*. ACM, 1379–1384.
22. Ben Shneiderman. 2010. *Designing the user interface: strategies for effective human-computer interaction*. Pearson Education India.
23. 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.
24. 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.
25. Guixin Ye, Zhanyong Tang, Dingyi Fang, Xiaojiang Chen, Kwang In Kim, Ben Taylor, and Zheng Wang. 2017. Cracking Android pattern lock in five attempts. (2017).
26. Guixin Ye, Zhanyong Tang, Dingyi Fang, Xiaojiang Chen, Willy Wolff, Adam Aviv, and Zheng Wang. 2018. A Video-based Attack for Android Pattern Lock. *ACM Transactions on Privacy and Security* (2018).