Understanding User-Centered Attacks In-The-Wild

Alia Saad
University of Duisburg-Essen
Essen, Germany
alia.saad@stud.uni-due.de

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

Sarah Delgado Rodriguez
Bundeswehr University
Munich, Germany
sarah.delgado@unibw.de

Stefan Schneegass
University of Duisburg-Essen
Essen, Germany
stefan.schneegass@uni-due.de

Roman Heger
University of Duisburg-Essen
Essen, Germany
roman.heger@stud.uni-due.de

CHI'20,, April 25–30, 2020, Honolulu, HI, USA
ACM 978-1-4503-6819-3/20/04.
https://doi.org/10.1145/3334480.XXXXXXX

Abstract
Our understanding of user-centered attacks on smartphone authentication, such as shoulder surfing, is very limited today. The reason is that situations in which such threats occur are difficult to observe and analyze. To address this, we present a research tool that allows user-centered attacks on smartphone authentication to be studied in the real world. The tool consists of two components: (1) a mobile phone enclosure that allows a wide-angle lens to be attached to the front-facing camera of the smartphone, and (2) a smartphone application that captures pictures upon each login attempt together with the current context as well as interaction information and lets users later select images to share with researchers. We report on the development of the research tool and share early insights on how users perceive the tool. We discuss how HCI researchers can benefit from the collected data, also beyond a security context.

Author Keywords
Usable Security and Privacy; User-Centered Attacks; Shoulder-surfing; Smudge attacks; Thermal attacks

CCS Concepts
•Human-centered computing → User studies; •Security and privacy → Usability in security and privacy;

Figure 1: Examples of User-Centered Attacks (from top to bottom): Shoulder-Surfing [5], Smudge Attacks [2], and Thermal Attacks [1]

Introduction

Smartphones allow sensitive information to be stored and accessed anytime and anywhere – both on the device itself as well as in the cloud. Such information includes but is not limited to personal photos, online baking accounts, and emails. Hence, protecting the smartphone from unauthorized access has become essential. Today, different types of authentication mechanisms exist. The most popular ones are biometric schemes, such as face or fingerprint recognition, as well as knowledge-based schemes, such as PINs, passwords, and lock patterns. In this work, we are particularly interested in the latter ones, which are subject to so-called side-channel attacks, such as shoulder-surfing, smudge attacks and thermal attacks (cf. Figure 1).

While prior work demonstrated novel approaches to reduce the vulnerability to each of the aforementioned threats, currently no approach exists that allows a smartphone to be comprehensively protected. One reason for this is that a fundamental understanding of when, how, and in which context attacks happen in the real world is missing as of today. Rather, the exploration of such attacks is performed under controlled conditions in the lab.

We close this gap with our research by proposing a tool that supports researchers in conducting user studies to investigate potential threats and attacks in the real world. The tool includes an Android application that uses contextual inquiry (e.g., each time the user authenticates or uses a specific application on the phone the contextual information is recorded). Additionally, the application is capable of storing the touch input points and used applications after such an event. Second, the tool also includes a hardware attachment that upgrades the phone's front camera with a fish-eye lens to gather information about the authentication context.

With our work, we provide researchers powerful means to assess and understand situations in which threats to smartphone authentication occur and, hence, design appropriate means to mitigate them.

Background and Related Work

In this section, we limit our focus to a thorough understanding of user-centered attacks and investigating existing approached to reduce the risk of user-centered attacks.

Understanding User-Centered Attacks

In this work, the term user-centered attacks refers to three main types of attacks: shoulder surfing, smudge, and thermal attacks. Shoulder surfing refers to the action where an individual observes another individual device, either during or post-authentication, without prior knowledge or consent [14, 17]. Smudge and thermal attacks are reconstructive types of user-centered attacks, where the attacker uses oily or thermal residues to retrieve the credentials of the legitimate user [1, 2]. Previous research focused more on mitigating user-centered attacks than understanding the context in which they occur.

A study conducted by Harbach et al. considered shoulder surfing as the most common type of user-centered attacks [6]. They also observed that less than 1% of the authentication sessions were considered as a risk. In their study, Eiband et al. investigated different shoulder surfing situations. Their findings show that these attacks take place in under unplanned and opportunistic circumstances and mostly target instant messages and social networks [5].

Mitigating User-Centered Attacks

There exist a considerable number of studies that explored the user-centered attacks prevention approaches. Therefore, we focus on existing solutions targeting these challenges in this section.

Observation Attacks (Shoulder Surfing) We focus on shoulder surfing as an example for observation attacks, because it is more likely and less obvious compared to camera recordings. Prior work either improved existing solutions [10, 11, 16, 19] or proposed novel approaches, for example, using gaze to enter credentials [4, 12] or combining gaze with traditional authentication means [7, 8, 9].

Reconstruction Attacks (Smudge and Thermal Attacks) As mentioned earlier, the intruder attempts to reconstruct the PIN or Password of the main user without prior knowledge by tracing either the oily or heat traces left after authentication. While some studies investigated the feasibility of smudge attacks [3, 20], other researchers focused on overcoming this problem by modifying the input pattern display either by geometric transformation [18] or changing the PIN or pattern grid size [13, 15]. Unlike smudge residues that can last for a longer period of time, thermal attacks must take place seconds after authentication. Abdelrahman et al. developed a programmatic approach that uses a thermal camera to reconstruct PINs and lock patterns from these heat traces [1]. In this research, the suggested countermeasures to this issue were to emit heat from the device either by increasing the brightness of the display or triggering a computationally heavy process.

Research Tool

After introducing different types of user-centered attacks that threaten users' privacy during authentication as well as proposed countermeasures, we recognized that little work was exerted to thoroughly investigate these attacks in actual realistic scenarios. Therefore, this work's contribution is a tool for logging user-centered attacks that uses a customized mobile phone enclosure and an Android logging application (cf., Figure 2).

Figure 2: The rating app (left), the smartphone enclosure with fish-eye lens design (center), and the produced prototype (right).

Mobile Phone Enclosure

The traditional smartphone front camera's field of view range varies between 60 to 80 degrees. However, as seen in Figure 3, the wider the field of view, the more comprehensive the understanding of the environment becomes. Accordingly, the first part of our work's contribution is to produce a customized phone enclosure that accommodates a fish-eye lens on the device's front camera to extend the field of view to 180 degrees. This 3D-printed enclosure can be customized for every smartphone's design of buttons, camera, and ports. We already produced 10 different enclosures for current mobile phones. The different 3D models are available for download[1].

Android Logging Application

The second contribution in this work is the Android logging application consisting of a logging service and a rating user interface. We designed the logging service to gain a profound understanding of what commonly triggers the user to unlock the phone.

[1] https://hcigroup.de/uca2020/

Figure 3: Different fields of view of a mobile phone enclosure using a fish-eye lens extending the front facing camera in context. Two staged situations in a train and in a park.

It first automatically capturing a picture from the enhanced front camera upon unlocking the phone or during other specific events (e.g., starting an app). The software uses this picture to determine the number of people in the field of view by detecting the number of faces in the scene using the Google Mobile Vision API[2]. Secondly, after authentication, the service records touch events (tap, long press, scroll, swipe, two fingers, and unidentified events) as sets of X and Y coordinates, plus the timestamp and current device location. This data provide insights about users' device interaction, thus allowing the threat from reconstruction attacks to be determined.

Then, users can add further details about each event and its context post-hoc. This is achieved by showing the user a list of all events (i.e., picture, metadata). For each, the user first classifies the location, where the classification of locations is based on the work of Eiband et al. [5]. In addition to location, the user updates information about the number of surrounding people. If the number of people is more than one, based on the aforementioned face detection algorithm, the user is also asked if the people in the image are authorized to look and whether this authentication session is perceived as a threat.

Finally, the application lets users upload collected data in textual form, where none of the captured images would be sent to researchers, hence preserving the privacy of both the user and the people in the image. We deliberately chose not to allow any pictures to be uploaded since users might do so accidentally.

We also provide an introduction to the tool on the first launch, explaining that even if a person is seen on the image, it still does not mean that this person has bad intentions.

Early Insights

In the following sections, we share early insights from (a) the design and development process of the tool as well as (b) from providing 13 users the tool for two weeks and collecting data on their authentication contexts.

Attracting Attention

One challenge with the research prototype is attracting attention. One of the first hardware prototypes has been printed with yellow PLA material. The yellow color of the device attracted a lot of attention. In addition, participants were asked for the attachment on their phones. To address this, we changed the color to black and used thinner and more flexible TPU material. Subsequently, we did not receive any further reports of similar events.

Influence on Phone Handling

Another challenge we encountered was that the attached lens made it more difficult to carry the smartphone in the pocket. This was less of an issue for participants who carry the phone in a bag.

[2] https://developers.google.com/vision/android/face-tracker-tutorial

Logging Effort
Manually verifying the contextual information required some effort from participants. However, we did not receive any negative comments about this. We compensated participants with 10 Euros plus one additional Euro per day on which they rated all authentication events. If a participant completed the full two weeks, they received an additional 10 Euros.

Shoulder Surfing or Not
Even when seeing the picture, it remains in many cases unclear if someone is actually looking at the device. Furthermore, we currently record only one point in time which means that glancing prior to this or afterward is not recorded. Current mobile technology, however, does not provide enough computational power to do a more sophisticated analysis of multiple images or videos. For the future, we plan to investigate gaze detecting algorithms and record videos of the whole interaction process to further improve the tool.

Conclusion
In this work, we presented a research tool that can be used to explore user-centered attacks on mobile phones in the wild. The tool (hardware & software) is available as open-source and can be used for further research projects.

We believe that the collected data provide promising insights about the likelihood of user-centered attacks in real-life situations and, hence, help in designing usable yet secure countermeasures. Furthermore, we hope that the community will further evolve the tool and adapt it to other contexts of use.

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*. ACM, 3751–3763.

[2] Adam J Aviv, Katherine L Gibson, Evan Mossop, Matt Blaze, and Jonathan M Smith. 2010. Smudge Attacks on Smartphone Touch Screens. *Woot* 10 (2010), 1–7.

[3] Seunghun Cha, Sungsu Kwag, Hyoungshick Kim, and Jun Ho Huh. 2017. Boosting the Guessing Attack Performance on Android Lock Patterns with Smudge Attacks. In *Proceedings of the 2017 ACM on Asia Conference on Computer and Communications Security*. ACM, 313–326.

[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] 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.

[8] 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.

[9] 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.

[10] 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.

[11] 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

[12] 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.

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

[14] Arash Habibi Lashkari, Samaneh Farmand, Omar Bin Zakaria, and Rosli Saleh. 2009. Shoulder Surfing attack in graphical password authentication. *CoRR* abs/0912.0951 (2009). http://arxiv.org/abs/0912.0951

[15] Ian Oakley and Andrea Bianchi. 2012. Multi-touch passwords for mobile device access. In *Proceedings of the 2012 ACM Conference on Ubiquitous Computing*. ACM, 611–612.

[16] 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

[17] 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 (MUM 2018)*. Association for Computing Machinery, New York, NY, USA, 147–152. DOI: http://dx.doi.org/10.1145/3282894.3282919

[18] 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 (UbiComp '14)*. ACM, New York, NY, USA, 775–786. DOI: http://dx.doi.org/10.1145/2632048.2636090

[19] 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.

[20] Yang Zhang, Peng Xia, Junzhou Luo, Zhen Ling, Benyuan Liu, and Xinwen Fu. 2012. Fingerprint attack against touch-enabled devices. In *Proceedings of the second ACM workshop on Security and privacy in smartphones and mobile devices*. ACM, 57–68.