GazeTouchPIN: Protecting Sensitive Data on Mobile Devices using Secure Multimodal Authentication

Mohamed Khamis
LMU Munich, Germany
mohamed.khamis@ifi.lmu.de

Mariam Hassib
LMU Munich, Germany
VIS, University of Stuttgart, Germany

Emanuel von Zezschwitz
LMU Munich, Germany

Andreas Bulling
Max Planck Institute for Informatics,
Saarland Informatics Campus

Florian Alt
LMU Munich, Germany

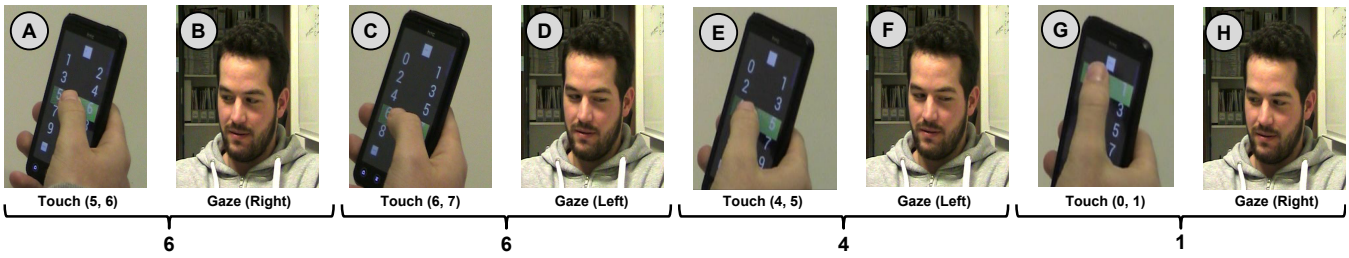


Figure 1: We propose using gaze and touch for authentication on smartphones when accessing sensitive data. GazeTouchPIN is robust against shoulder surfing since it requires attackers to observe the user's eyes and the touchscreen simultaneously. In the example the user enters "6641". Users first select a row of two digits via touch, then gaze left or right to determine the digit to select. To complicate shoulder surfing, one of two digits layouts is randomly chosen at every entry (e.g., compare A to C).

ABSTRACT

Although mobile devices provide access to a plethora of sensitive data, most users still only protect them with PINs or patterns, which are vulnerable to side-channel attacks (e.g., shoulder surfing). However, prior research has shown that privacy-aware users are willing to take further steps to protect their private data. We propose GazeTouchPIN, a novel secure authentication scheme for mobile devices that combines gaze and touch input. Our multimodal approach complicates shoulder-surfing attacks by requiring attackers to observe the screen as well as the user's eyes to find the password. We evaluate the security and usability of GazeTouchPIN in two user studies (N=30). We found that while GazeTouchPIN requires longer entry times, privacy aware users would use it on-demand when feeling observed or when accessing sensitive data. The results show that successful shoulder surfing attack rate drops from 68% to 10.4% when using GazeTouchPIN.

CCS CONCEPTS

• **Human-centered computing → Human computer interaction (HCI)**;

KEYWORDS

Multimodal Authentication, Eye Tracking, Mobile Devices, Gaze

ACM Reference Format:
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 19th ACM International Conference on Multimodal Interaction (ICMI'17).* ACM, New York, NY, USA, 5 pages. https://doi.org/10.1145/3136755.3136809

Permission to make digital or hard copies of all or part 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 components of this work owned by others than the author(s) must be honored. Abstracting with credit is permitted. To copy otherwise, or republish, to post on servers or to redistribute to lists, requires prior specific permission and/or a fee. Request permissions from permissions@acm.org.
ICMI'17, November 13–17, 2017, Glasgow, UK
© 2017 Copyright held by the owner/author(s). Publication rights licensed to the Association for Computing Machinery.
ACM ISBN 978-1-4503-5543-8/17/11…$15.00
https://doi.org/10.1145/3136755.3136809

1 INTRODUCTION

Mobile devices enable access to sensitive data – including personal photos, call logs, or emails – resulting in a need to protect access to such devices. Users lock their phones using different methods such as PINs, lock patterns, and biometrics (e.g., fingerprint) [10]. The former two are vulnerable to shoulder surfing [5, 7, 12, 24], thermal attacks [1], and smudge attacks [2, 19, 25]. While biometric authentication is less susceptible to these attacks, biometric data can be stolen remotely [21, 30], and cannot be changed once leaked.

There is a need for a wide range of authentication mechanisms to fit different user preferences, tasks and contexts. Meanwhile, advances in remote gaze estimation enable eye tracking [11, 27] and gaze gestures detection [12, 13, 22, 28] using the front-facing cameras of unmodified mobile devices. These advances enable systems to use gaze for mobile authentication [12, 13, 16, 20].

In this work, we propose a novel multimodal authentication scheme that combines gaze and touch input for secure user authentication on off-the-shelf mobile devices (see Figure 1). GazeTouchPIN is particularly useful for situations where users are feeling observed, or if they are accessing private data in sensitive contexts (e.g., in public transport [7]). It is highly secure against two advanced threat models that we describe later.

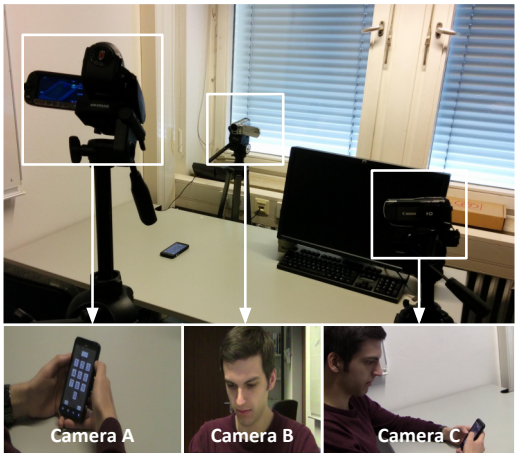


Figure 2: The usability study setup. Camera A recorded the phone screen (phone-view) to observe the touch input. Camera B recorded the participant's face (eyes-view) to observe the eye movements. Camera C simultaneously recorded the screen and the user's eyes (side-view).

The contributions of this work are two-fold. First, we introduce the concept and implementation of GazeTouchPIN, a novel multimodal authentication scheme that secures mobile devices against two advanced shoulder-surfing attacks. Second, we report on an evaluation of our system with regard to usability and security according to criteria identified by Schaub et al. [18] and compare it to state-of-the-art authentication schemes.

2 THREAT MODELS

To cover basic and advanced attacks, our scheme addresses two threat models. For both models the user is in a public space. The attacker knows how to authenticate, but does not know the PIN. Both models require monitoring both the device's touchscreen as well as the user's eyes:

Side attack model. The user is observed from a viewpoint that shows the user's gaze input and touch input (e.g., in a train). The distance to the user is close enough to see the touchscreen, but far enough to reduce the effort of switching focus back and forth between the user's eyes and the device's touchscreen (Figure 2C).

Iterative attack model. The attacker is able to observe the user several times (e.g., a colleague at work [26]). The attacker exclusively focuses on one modality per observation – for example, first on the users' eyes and then on the input on the screen, or vice versa (Figures 2A and 2B). The challenges are to (a) correctly remember both sequences and (b) to correctly combine them later.

3 GAZETOUCHPIN

Based on these threat models we propose GazeTouchPIN, a multimodal authentication scheme that requires touch-based selection as well as gaze gestures. The system is implemented as an Android application and does not require any additional hardware. Instead, gaze gestures are detected using the front-facing camera. We detect the user's face and eyes using the Viola-Jones detector [23]. Gaze gestures are detected using a calibration-free gaze estimation approach [29]. The distance between the face's center and the pupil for the left (d_{left}) and right (d_{right}) eyes is measured. Gaze directions are then estimated based on the ratio $d_{left} : d_{right}$; e.g., if $d_{left} > d_{right}$, we conclude that the user is looking to the left.

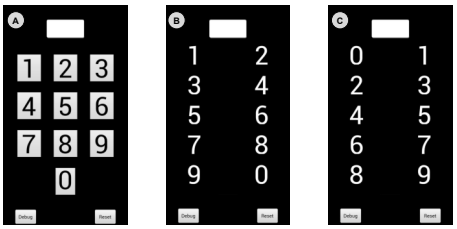


Figure 3: Layout (a) was used for touch-only (the baseline). Layouts (b) and (c) are the only two possible layouts for the touch+random as well as for GazeTouchPIN.

GazeTouchPIN augments PIN selection by splitting the input into two stages. Users first select the row containing the required digit using touch and then choose one of both digits by looking left or right (see Figure 1). The layout of the shown digits is chosen randomly at every input (i.e., the layout changes 4 times when entering a 4-digit PIN). We use only two layouts to support learning effects and avoid any cognitive load caused by selecting from a totally random arrangement (see Figures 3B and 3C) .

(1) *touch-only* (Figure 3a): uses a PIN keypad (baseline).
(2) *touch+random* (Figures 3b and 3c): uses touch to select the desired digit from one of two randomly shuffling layouts. This will provide insights about the shuffling idea and help distinguish the impact of the multimodal factor on the usability and security of GazeTouchPIN.
(3) GazeTouchPIN (Figures 3b and 3c) uses touch input to select a pair of horizontally aligned PIN digits and then a gaze-gesture to the left/right to select the desired PIN.

4 EVALUATION

4.1 Usability Study

We started with a usability study to collect realistic password entries for a subsequent security study and to compare the usability of the three methods. The study was designed as a repeated measures experiment. Participants entered 6 pre-defined PINs using all three authentication methods. We logged all authentication attempts and showed the home screen after successful logins. We recorded the participants using three HD video cameras as shown in Figure 2.

4.1.1 Participants and Procedure. We recruited 12 participants (2 females), aged between 19 and 31 years ($M = 24.8$, $SD = 3.6$), who had normal or corrected-to-normal vision. Upon arrival, the experimenter explained the study and asked the participant to sign a consent form. The experimenter then started the application, handed the phone to the participant, and described how it works. Each participant then performed three training runs, one per condition, to get acquainted with the system. Those runs were excluded from further analyses. At each authentication attempt, the experimenter read out the PIN and input method according to a previously generated randomized list. The list was randomized to avoid frequent consecutive gaze inputs, which leads to fatigue and in turn influences performance and acceptance [14]. The participant would then enter the PIN until successful. We concluded with an interview.

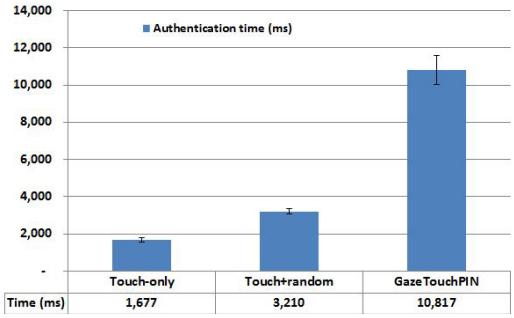


Figure 4: Untrained users need more time using GazeTouchPIN than when using touch+random and touch-only. GazeTouchPIN users performed faster by time; mean input time decreased from 10.8 to 9.5 seconds at the sixth entry.

4.1.2 Results. In total we recorded 54 videos per participant (6 passwords × 3 methods × 3 camera views). Apart from the videos, we analyzed the data with regard to input speed and error rate.

Input Speed. Figure 4 summarizes the time needed to authenticate for each method. Prior to analysis, we excluded 2 out of 216 input time measurements as outliers ($> \mu + 2.5\times$SD). A repeated measures ANOVA showed significant effects for method on input speed ($F_{1.021,9.192} = 156.106$, $p < 0.001$). Post-hoc analyses using Bonferroni correction revealed that there is a significant difference ($p < 0.001$) in input speed between touch-only input ($M = 1677$, $SD = 120$) and GazeTouchPIN input ($M = 10817$, $SD = 712$). There is also a significant difference ($p < 0.001$) between touch+random input ($M = 3210$, $SD = 124$) and GazeTouchPIN input ($M = 10817$, $SD = 712$). The third pair (touch-only vs touch+random) is also significantly different ($p < 0.001$).

Error Rate. Using a Pearson chi-square test we could not find a statistically significant effect of method on error rate $\chi^2(11) = 12, p = 0.364$. However we found a tendency to make less errors as participants entered more PINs using GazeTouchPIN, which suggests that there is a learning effect. For example, 10 out of 12 participants entered their fifth and sixth PIN correctly on their first attempt. Participants 2 and 6 never failed, while participants 1, 7 and 11 failed once each. Finally, participant 4 improved steadily from 4 failures at the first PIN to no failures at the last one.

Qualitative Feedback. Participants noted that the touch+random and GazeTouchPIN are more secure than the regular touch-only method. Despite longer login times, all participants agreed that with training they would be able to enter PINs faster. This aligns with the quantitative data, which showed that the mean input time of the participants' first entry using GazeTouchPIN is 10.8 seconds, which decreased to 9.5 seconds at their sixth entry using GazeTouchPIN. Participants imagined GazeTouchPIN to be particularly useful in situations where they are more exposed, such as in public transport. Also using the approach as a second layer of authentication for particular cases (e.g., online banking applications, or for opening messages from a specific person) was mentioned as an application area. Overall while one participant reported that he would use GazeTouchPIN for frequent phone unlocking, 10 participants reported they would use it to protect sensitive data or in situations where they feel observed. This suggests that GazeTouchPIN is attractive for security-aware users, while less concerned users would use it in sensitive contexts.

4.2 Security Study

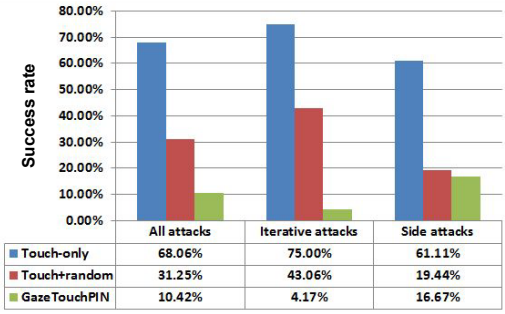
In this study we focused on the security of the three methods. The study also followed a repeated-measures design. Participants attacked passwords entered using all three methods and observed from all views using the videos recorded during the usability study. In total, each participant attacked 24 PIN entries – 8 for each method, (1) 12 were iterative attacks, each required watching an eyes video and a phone video, and (2) 12 were side attacks, each required a side view video. Participants performed half of the 24 attacks using the side-view and the other half using the phone-view and the eyes-view. For iterative attacks against the GazeTouchPIN method, participants were provided both the eyes-view as well as the phone-view. Half of these started by the eyes-view, while the other half started with the phone-view. For any two observations against GazeTouchPIN, there is a $\frac{1}{2^n}$ chance that the phone-view and the eyes-view match. Hence, we randomly assigned the views such that there was a $\frac{1}{16}$ chance for a match (4-digit PINs). The order of methods was randomized per participant. To avoid learning effects, no participant attacked the same password from different views.

4.2.1 Participants and Procedure. We recruited 18 participants (5 females) aged between 18 and 36 ($M = 24.6$, $SD = 4.54$). None had participated in the usability study. Participants were compensated with a 10 Euro gift voucher. In addition, all participants took part in a draw for an additional 20 Euro gift voucher, where their chances of winning the draw increased with the number of successfully attacked passwords. Participants were introduced to the study procedure and the reward mechanism, the experimenter then explained the system and participants could try the app themselves. They were then given draft papers and the experimenter started playing the videos. All videos were watched once. Participants were allowed to examine the layouts at any time during the study (see Figure 3). Participants provided up to three guesses based on their observations. In case of iterative attacks, the experimenter alternated the order at which the participant watched the videos, i.e., in half of the cases the participant watched the eyes-view first, while in the other half the participant watched the phone-view first. The study was concluded with a semi-structured interview.

4.2.2 Results. In total, participants performed $18 \times 24 = 432$ attacks, providing three guesses for each.

Successful Attacks. We calculated the Levenshtein distance between the guesses and the correct PIN. Out of the three guesses, the guess with the least distance to the correct PIN (i.e., the guess that is closest to the correct PIN) was considered for further analysis. We also calculated the overall success rate in attacking PINs for each input method and view angle. An attack is successful if at least one of the 3 guesses matches the correct password. Figure 5 shows the rate of successful attacks against PINs entered using each method through each view.

A repeated measures ANOVA showed significant main effects for input method ($F_{2,34} = 42.36$, $p < 0.001$) on attack success. This means that the distance between the guesses and the correct PIN depends on the input method. Post-hoc analysis using Bonferroni correction revealed that there is a significant difference ($p < 0.001$) in the distances for PINs entered using GazeTouchPIN ($M = 1.88$, $SD = 0.11$) compared to touch-only PINs ($M = 0.65$, $SD = 0.1$).



	All attacks	Iterative attacks	Side attacks
Touch-only	68.06%	75.00%	61.11%
Touch+random	31.25%	43.06%	19.44%
GazeTouchPIN	10.42%	4.17%	16.67%

Figure 5: Success rate of attacking PINs entered using the three methods. GazeTouchPIN is the most secure among the tested methods, in particular against iterative attacks.

There is also a significant difference ($p < 0.005$) in the distances for PINs entered using GazeTouchPIN ($M = 1.88$, $SD = 0.11$) compared to touch+random PINs ($M = 1.37$, $SD = 0.13$). The final pair is also significantly different ($p < 0.001$). This means that guesses against PINs are statistically closer to the correct PIN in case of touch-only PINs, followed by touch+random PINs. However guesses against GazeTouchPIN PINs are the least similar to the correct one.

Interviews. All participants reported that attacking multimodal PINs (GazeTouchPIN) through the side-view is the most difficult task. Some attributed this to the difficulty of focusing on the eyes and phone in parallel, particularly if the users were fast in entering their password. "It is just very hard to concentrate on two numbers, look at his eyes, then again at the screen", said P0. One participant noted that she had to keep track of: (1) the user's finger, (2) which layout is displayed and (3) the eye movements. Another participant added that it is particularly difficult when multiple fingers are used. Multiple attackers indicated that shuffling the layout confused them.

5 DISCUSSION

Successful iterative attack rate against GazeTouchPIN is very low (only 4.2% success rate). An attacker who observes all touch inputs through the phone-view would still have to try 2^n possibilities to find the correct PIN combination (where n is the number of digits in the PIN) because of the randomness of the layout. When observing the eyes-view, the attacker would not know which layout the user is responding to. There is only a $\frac{1}{2^n}$ chance that the attacker observes a matching phone-view and eyes-view. For this reason GazeTouchPIN is highly resistant to iterative attacks. Side attacks perform better than iterative attacks (17% success rate) as the adversary expects gaze-input right after touch input. However success rate is still very low compared to the other methods due to having to switch focus back and forth between the eyes and the screen (see Figure 5). Successful attack rates against GazeTouchPIN show that it is a significant improvement over state-of-the-art gaze-based authentication schemes, such as 42% [3], 55% [6], 15% – 63% [12], and 60% [17]. GazeTouchPass [12] uses passwords that consist of gaze input and touch input (e.g., gaze(left), touch(1), gaze(right), touch(2)), while GazeTouchPIN uses gaze and touch in addition to a random layout to enter a 4-digit PIN. This makes GazeTouchPIN (A) more secure against iterative attacks (only 4.2% success rate) compared to GazeTouchPass (42% success rate [12]), and (B) compatible with existing backends that accept PINs. Our work shows how multimodal authentication can be made resilient against iterative attacks, which GazeTouchPass [15] is vulnerable to. Our system also compares well with non-gaze systems such as XSide [4] which had a success rate of 9% – 38%. Additionally, GazeTouchPIN does not require hardware modifications, and is resilient to smudge and thermal attacks by design since the entire password cannot be recovered from the touchscreen.

It should be noted that all previous conclusions are based on the assumption that the attacker knows how GazeTouchPIN works. The threat models we propose are realistic but also ensure optimal attacking conditions. Additionally, participants of the security studies were highly motivated and trained. This is evidenced from their performance against the baselines which was as high as 75% (see Figure 5), which is comparable to results from state-of-the-art schemes; attackers of ColorSnakes [9] and XSide [4] achieved 75% and 53% success rate against the respective baselines.

The usability analysis of GazeTouchPIN revealed that authentication speed is, despite being slower than single modal input, faster than many other state-of-the-art multimodal authentication systems. For example, 15 s [17], 9.6 s [16], 12.5 s [3], 48.5 s [6], 36.7 s [8], 9.2 s – 12.1 s [15]. Furthermore, as it is based on only two layouts, we expect users to become faster as they use the system more frequently due to training effects. This is evident in the quantitative results, which show that mean login time using GazeTouchPIN decreases from 10.8 seconds to 9.5 seconds as participants used it more often. Since users unlock their phones almost 50 times a day [10], we recommend the use of GazeTouchPIN in sensitive contexts rather than on regular basis. Overall, and as several participants indicated, multimodal authentication can be particularly useful as a secondary authentication mechanism that users can choose to opt to when feeling observed (e.g., public setting), or when accessing critical data (e.g., online banking). A limitation is that users do not always hold the phone in a way that shows the eyes. The system might not detect both eyes if the phone is too close to the face. Future work can guide users into an optimal posture.

6 CONCLUSION

In this work we proposed GazeTouchPIN, a novel scheme that combines gaze and touch for highly secure multimodal authentication on mobile devices. Our findings show that GazeTouchPIN is significantly secure against both iterative and side shoulder surfing attacks. Its usability is comparable to related work, making it suitable for use when feeling observed or when accessing sensitive data. We expect these advantages to multiply with further advances in remote gaze estimation on mobile devices. In the future we plan to evaluate our system against other threat models such as video attacks [24], insiders [26], and multiple observers.

7 ACKNOWLEDGEMENTS

This work was partially funded by the Bavarian State Ministry of Education, Science and the Arts in the framework of the Centre Digitisation.Bavaria (ZD.B), and by the Cluster of Excellence on Multimodal Computing and Interaction (MMCI) at Saarland University, Germany.

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, 12.

[2] Adam J. Aviv, Katherine Gibson, Evan Mossop, Matt Blaze, and Jonathan M. Smith. 2010. Smudge Attacks on Smartphone Touch Screens. In *Proceedings of the 4th USENIX Conference on Offensive Technologies (WOOT'10)*. USENIX Association, Berkeley, CA, USA, 1–7. http://dl.acm.org/citation.cfm?id=1925004.1925009

[3] 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 (SOUPS '09)*. ACM, New York, NY, USA, Article 7, 12 pages. https://doi.org/10.1145/1572532.1572542

[4] 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 32Nd Annual ACM Conference on Human Factors in Computing Systems (CHI '14)*. ACM, New York, NY, USA, 2937–2946. https://doi.org/10.1145/2556288.2557097

[5] Alexander De Luca, Emanuel von Zezschwitz, Ngo Dieu Huong Nguyen, Max-Emanuel Maurer, Elisa Rubegni, Marcello Paolo Scipioni, and Marc Langheinrich. 2013. Back-of-device Authentication on Smartphones. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems (CHI '13)*. ACM, New York, NY, USA, 2389–2398. https://doi.org/10.1145/2470654.2481330

[6] 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 (OZCHI '07)*. ACM, New York, NY, USA, 199–202. https://doi.org/10.1145/1324892.1324932

[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 (CHI '17)*. ACM, New York, NY, USA, 11.

[8] Alain Forget, Sonia Chiasson, and Robert Biddle. 2010. Shoulder-surfing Resistance with Eye-gaze Entry in Cued-recall Graphical Passwords. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems (CHI '10)*. ACM, New York, NY, USA, 1107–1110. https://doi.org/10.1145/1753326.1753491

[9] Jan Gugenheimer, Alexander De Luca, Hayato Hess, Stefan Karg, Dennis Wolf, and Enrico Rukzio. 2015. ColorSnakes: Using Colored Decoys to Secure Authentication in Sensitive Contexts. In *Proceedings of the 17th International Conference on Human-Computer Interaction with Mobile Devices and Services (MobileHCI '15)*. ACM, New York, NY, USA, 274–283. https://doi.org/10.1145/2785830.2785834

[10] 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 (CHI '16)*. ACM, New York, NY, USA, 4806–4817. https://doi.org/10.1145/2858036.2858267

[11] Oliver Hohlfeld, André Pomp, Jó Ágila Bitsch Link, and Dennis Guse. 2015. On the Applicability of Computer Vision Based Gaze Tracking in Mobile Scenarios. In *Proceedings of the 17th International Conference on Human-Computer Interaction with Mobile Devices and Services (MobileHCI '15)*. ACM, New York, NY, USA, 427–434. https://doi.org/10.1145/2785830.2785869

[12] 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 (CHI EA '16)*. ACM, New York, NY, USA, 2156–2164. https://doi.org/10.1145/2851581.2892314

[13] Mohamed Khamis, Regina Hasholzner, Andreas Bulling, and Florian Alt. 2017. GTmoPass: Two-factor Authentication on Public Displays Using Gaze-touch Passwords and Personal Mobile Devices. In *Proceedings of the 6th ACM International Symposium on Pervasive Displays (PerDis '17)*. ACM, New York, NY, USA, Article 8, 9 pages. https://doi.org/10.1145/3078810.3078815

[14] Mohamed Khamis, Ozan Saltuk, Alina Hang, Katharina Stolz, Andreas Bulling, and Florian Alt. 2016. TextPursuits: Using Text for Pursuits-Based Interaction and Calibration on Public Displays. In *Proceedings of the 2016 ACM International Joint Conference on Pervasive and Ubiquitous Computing (UbiComp '16)*. ACM, New York, NY, USA, 12. https://doi.org/10.1145/2971648.2971679

[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 (SOUPS '07)*. ACM, New York, NY, USA, 13–19. https://doi.org/10.1145/1280680.1280683

[16] Dachuan Liu, Bo Dong, Xing Gao, and Haining Wang. 2015. Exploiting Eye Tracking for Smartphone Authentication. In *Proceedings of the 13th International Conference on Applied Cryptography and Network Security (ACNS '15)*. 20.

[17] Vijay Rajanna, Seth Polsley, Paul Taele, and Tracy Hammond. 2017. A Gaze Gesture-Based User Authentication System to Counter Shoulder-Surfing Attacks. In *Proceedings of the 2017 CHI Conference Extended Abstracts on Human Factors in Computing Systems (CHI EA '17)*. ACM, New York, NY, USA, 1978–1986. https://doi.org/10.1145/3027063.3053070

[18] 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 (SOUPS '13)*. ACM, New York, NY, USA, Article 11, 14 pages. https://doi.org/10.1145/2501604.2501615

[19] 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. https://doi.org/10.1145/2632048.2636090

[20] Chen Song, Aosen Wang, Kui Ren, and Wenyao Xu. 2016. "EyeVeri: A Secure and Usable Approach for Smartphone User Authentication". In *IEEE International Conference on Computer Communication (INFOCOM'16)*. San Francisco, California, 1 – 9.

[21] Martin Stokkenes, Raghavendra Ramachandra, and Christoph Busch. 2016. Biometric Authentication Protocols on Smartphones: An Overview. In *Proceedings of the 9th International Conference on Security of Information and Networks (SIN '16)*. ACM, New York, NY, USA, 136–140. https://doi.org/10.1145/2947626.2951962

[22] Vytautas Vaitukaitis and Andreas Bulling. 2012. Eye Gesture Recognition on Portable Devices. In *Proceedings of the 2012 ACM Conference on Ubiquitous Computing (UbiComp '12)*. ACM, New York, NY, USA, 711–714. https://doi.org/10.1145/2370216.2370370

[23] Paul Viola and Michael J. Jones. 2004. Robust Real-Time Face Detection. *International Journal of Computer Vision* 57, 2 (2004), 137–154. https://doi.org/10.1023/B:VISI.0000013087.49260.fb

[24] 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 (CHI '15)*. ACM, New York, NY, USA, 1403–1406. https://doi.org/10.1145/2702123.2702212

[25] Emanuel von Zezschwitz, Anton Koslow, Alexander De Luca, and Heinrich Hussmann. 2013. Making Graphic-based Authentication Secure Against Smudge Attacks. In *Proceedings of the 2013 International Conference on Intelligent User Interfaces (IUI '13)*. ACM, New York, NY, USA, 277–286. https://doi.org/10.1145/2449396.2449432

[26] Oliver Wiese and Roth Volker. 2016. See you next time: A model for modern shoulder surfers. In *Proceedings of the 18th International Conference on Human-computer Interaction with Mobile Devices and Services (MobileHCI '16)*.

[27] Erroll Wood and Andreas Bulling. 2014. EyeTab: Model-based Gaze Estimation on Unmodified Tablet Computers. In *Proceedings of the Symposium on Eye Tracking Research and Applications (ETRA '14)*. ACM, New York, NY, USA, 207–210. https://doi.org/10.1145/2578153.2578185

[28] Meredith Ringel Morris Xiaoyi Zhang, Harish S. Kulkarni. 2017. Smartphone-Based Gaze Gesture Communication for People with Motor Disabilities. In *Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems (CHI '17)*. ACM, New York, NY, USA. https://doi.org/10.1145/3025453.3025790

[29] Yanxia Zhang, Andreas Bulling, and Hans Gellersen. 2014. Pupil-canthi-ratio: a calibration-free method for tracking horizontal gaze direction. In *Proc. of the 2014 International Working Conference on Advanced Visual Interfaces (AVI 14)* (2014-05-27). ACM, New York, NY, USA, 129–132. http://dx.doi.org/10.1145/2598153.2598186

[30] Yulong Zhang, Zhaonfeng Chen, Hui Xue, and Tao Wei. 2015. Fingerprints On Mobile Devices: Abusing and leaking. In *Black Hat Conference*.