GazeLockPatterns: Comparing Authentication Using Gaze and Touch for Entering Lock Patterns

Yasmeen Abdrabou
Bundeswehr University Munich
yasmeen.essam@unibw.de

Ken Pfeuffer
Bundeswehr University Munich
ken.pfeuffer@unibw.de

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

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

ABSTRACT

In this work, we present a comparison between Android's lock patterns for mobile devices (TouchLockPatterns) and an implementation of lock patterns that uses gaze input (GazeLockPatterns). We report on results of a between subjects study (N=40) to show that for the same layout of authentication interface, people employ comparable strategies for pattern composition. We discuss the pros and cons of adapting lock patterns to gaze-based user interfaces. We conclude by opportunities for future work, such as using data collected during authentication for calibrating eye trackers.

CCS CONCEPTS

• **Human-centered computing** → **Human computer interaction (HCI)**; **Empirical studies in HCI**.

KEYWORDS

Gaze Patterns, Touch Patterns. Authentication

ACM Reference Format:
Yasmeen Abdrabou, Ken Pfeuffer, Mohamed Khamis, and Florian Alt. 2020. GazeLockPatterns: Comparing Authentication Using Gaze and Touch for Entering Lock Patterns. In *Symposium on Eye Tracking Research and Applications (ETRA '20 Short Papers), June 2–5, 2020, Stuttgart, Germany*. ACM, New York, NY, USA, 6 pages. https://doi.org/10.1145/3379156.3391371

1 INTRODUCTION

Graphical passwords, such as lock patterns, are a popular means of authentication especially among Android users [Ye et al. 2017]. In lock patterns, users authenticate by entering a pattern that connects up to 9 digits on a 3×3 grid. Lock patterns that are entered via touch (TouchLockPatterns, for short), have been extensively studied by the user-centred security community [Egelman et al. 2014; Harbach et al. 2016; Uellenbeck et al. 2013; von Zezschwitz et al. 2015]. This resulted in an understanding of how strong the TouchLockPatterns users create are, common pitfalls, and areas of improvement. At the same time, advances in gaze estimation accuracy and eye tracking hardware led to gaze gaining popularity for authentication as a more natural and secure modality for entering passwords [Katsini et al. 2020]. Gaze offers usability advantages over traditional modalities such as touch and pointing (e.g., mouse) and its subtleness makes it more secure against observation attacks.

Figure 1: Study setup where we investigate the difference between using gaze and touch for entering lock patterns

Although gaze was employed for password entry, and showed promising results for entering graphical passwords [Bulling et al. 2012; De Luca et al. 2009], there is a gap in understanding how users create lock patterns using gaze. For example, do users create stronger lock patterns when using gaze as opposed to touch? Or do they make the same mistakes rendering lock patterns entered via touch vulnerable (e.g., the majority of users create TouchLockPatterns starting on the top left corner, making them more predictable)? This knowledge is important to understand whether adapting lock patterns for gaze authentication is a meaningful approach.

We study how the use of gaze influences the creation of lock patterns. We provide the first comparison of GazeLockPatterns to the well studied TouchLockPatterns to understand differences in usability and security on a tablet mobile device (Figure 1). Through a between-subjects study with 40 participants, we show that for the same interface, people employ similar password composition strategies. An analysis of gaze behaviour when entering lock patterns using touch suggests that long lock patterns could serve as a basis for eye tracker calibration. The findings are valuable for designers of authentication schemes in gaze-based systems.

2 RELATED WORK

Previous work analysed passwords created by users of Android TouchLockPatterns in the wild. Harbach et al. [Harbach et al. 2016] conducted a month-long field study in which they logged locking-related events on smartphones. Almost half of participants they surveyed had been using TouchLockPatterns. They found that the average pattern is of length 5.9 cells, and only 8 of them had set up

ETRA '20 Short Papers, June 2–5, 2020, Stuttgart, Germany

their device to make the strokes invisible. They found authentication times to increase on average by 147 ms for each additional cell in a pattern. Uellenbeck et al. [Uellenbeck et al. 2013] analysed the guessability of patterns and showed that users are biased in their choices; users are biased towards starting their patterns from the top left corner, and are biased against the centre. Von Zezschwitz et al. [von Zezschwitz et al. 2015] studied the the influence of pattern length, line visibility, number of knight moves, number of overlaps and number of intersections on observation resistance. They found that line visibility and length are the most important security factors, in addition to pattern complexity. Literature also showed that users often select patterns that are short and constitute simple strokes [Andriotis et al. 2014; Uellenbeck et al. 2013]. Loge et al. [Loge et al. 2016] showed that age, gender, and experience in IT significantly influence the strength and length of chosen patterns.

The aforementioned work helped shape the user-centred security community's understanding of TouchLockPatterns' usability, and how the way people use them influences security. Work by Katsini and colleagues analysed touch or mouse-based graphical authentication schemes where passwords consist of a series of pictures [Katsini et al. 2019, 2018a,b,c]. However, none of these works discussed the use of gaze for entering lock patterns. We close this gap in understanding whether the same behaviours observed when creating and using lock patterns pertain for gaze, opposed to touch.

A recent survey on eye gaze for security and privacy applications [Katsini et al. 2020] showed that gaze is promising for password entry. In addition to usability benefits, gaze is subtle and hard to observe, and can be a powerful means to add biometrics as a layer on top of gaze-based passwords. Gaze can be used for implicit (biometric) authentication [Abdulin and Komogortsev 2015; Cantoni et al. 2018; Holland and Komogortsev 2012; Juhola et al. 2013; Pfeuffer et al. 2019; Sluganovic et al. 2018; Zhang et al. 2014]) or explicit authentication, i.e., entering a password using gaze [Abdrabou et al. 2019; Best and Duchowski 2016; Kumar et al. 2019]. The latter is more relevant to our work: examples include EyePass [De Luca et al. 2008] and others [De Luca et al. 2007; Salehifar et al. 2019] based on gaze gestures, and smooth pursuit eye movement based systems [Khamis et al. 2018b,c; Pfeuffer et al. 2013; Rajanna et al. 2018; Rajanna et al. 2017]. De Luca et al. [De Luca et al. 2009] proposed EyePassShapes, that extend PassShapes [Weiss and De Luca 2008], a mouse-based scheme similar to lock patterns. EyePassShapes was not compared with its touch-based counterparts. The slight differences between PassShapes and lock patterns suggest that users' behaviour might be different when using either, thus warranting the need to understand users' behaviour for gaze lock patterns.

3 GAZELOCKPATTERNS: IMPLEMENTATION

We implemented a version of TouchLockPatterns that employs eye gaze for drawing the strokes between digits on a 3×3 grid. The system is based an existing application [Code 2016] and was implemented in C#. We used a radius of 34 pixels for the interface buttons and the entry pad area size was 0.4 of the screen width and 0.25 of the screen height. The pad was centred in the middle of the screen. For gaze tracking, we used the raw data stream of a Tobii eye tracker and mapped it to the screen size. The gaze trace feature of Tobii was enabled during the gaze condition as an indication of where the user is looking. The entry pad size and the gaze trace features were enabled as result of a pilot test with 3 participants. The pattern pad implementation enables users to enter patterns of size 4-9, overlaps were enabled and closed shapes were disabled. To trigger gaze input, users touch on the screen, perform the gesture and release. We used the same interface for TouchLockPatterns. Input was logged via touch rather than using the eye tracker.

4 EVALUATION

The main research question is: 'How different gaze authentication is from touch authentication?' We designed a between subjects experiment where half of the participants underwent the touch condition (TouchLockPatterns) while the other half underwent the gaze condition (GazeLockPatterns). There were security level *scenarios* inspired from literature [Loge et al. 2016]: The participants were asked to create a pattern for a smartphone, an account for online shopping (i.e. Amazon), and a new online banking profile. We studied the effect on different factors as used in literature [von Zezschwitz et al. 2015], e.g.: *Pattern Length*, *Intersections*, *Overlaps*, *Knight Moves*, *Observation risk*, *Start and End Positions*.

We invited 40 users (15F, 1 lefthanded, 2 contact lenses, 14 glasses) between 20 to 55 years (Mean=28.52, SD=9.5) to the experiment. A Microsoft Surface Pro 4 (2736×1824) was used with a Tobii 4C eye tracker (Figure 1).

Upon arrival, participants were introduced to the study, filled in a consent form and a demographics questionnaire, then calibrated the eye tracker. Participants then went through three blocks, one per scenario. For each scenario, participants 1) created a lock pattern, then reentered it for confirmation, and 2) rated the strength and the memorability of the entered pattern on a scale from 1 to 5 (5=very strong; highly memorable). At the end participants filled a questionnaire to share their experience with IT , IT security, lock patterns, the operating system of their smartphone, which authentication schemes they use, and their dominant hand. Those who experienced GazeLockPatterns additionally rated their experience of entering patterns using gaze, and reflected on the technique.

5 RESULTS

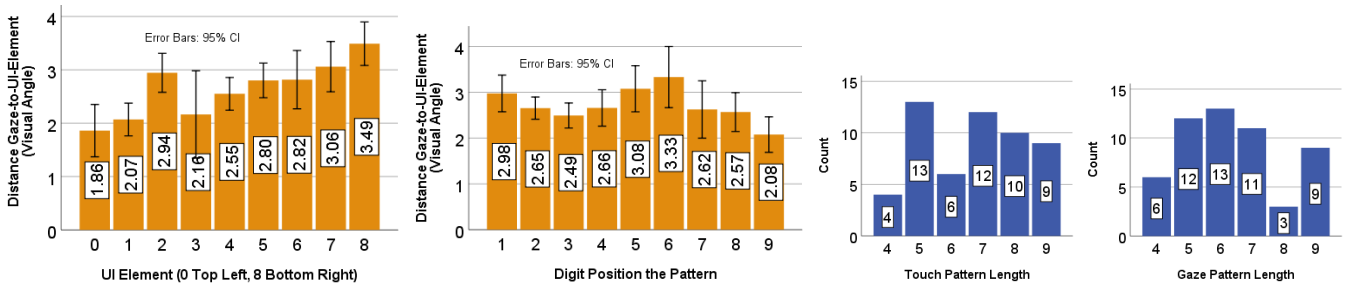
We analysed the effect of input modality on the aforementioned lock pattern properties for 120 patterns. Results are presented in Table 1. Statistical analysis was performed with repeated measures ANOVA and posthoc pairwise comparisons with Bonferroni correction.

5.1 Pattern Length

We first analyse the length of the patterns. The distributions of pattern lengths is shown in Figures 2c and 2d. The mean pattern length across TouchLockPatterns and GazeLockPatterns for each scenario. As seen, there are almost no noticeable differences. No significant differences were found between input modalities ($F(1,53) = 1.308$, $p = .258$) of gaze (M=6.41; SD=1.654) and touch (M=6.80; SD=1.784). However, factor context revealed significant differences ($F(2,58) = 5.396$, $p = .014$). Posthoc tests showed the smartphone context (M=5.93; SD=1.337) had a significantly lower length than bank context (M=7.33; SD=2.07).

Table 1: Comparison between gaze and touch modalities for the 3 situations

	Length		Intersections		Overlaps		Knight Moves		Observation Risk		Memorability		Perceived Strength	
	Touch	Gaze	Touch	Gaze	Touch	Gaze	Touch	Gaze	Touch	Gaze	Touch	Gaze	Touch	Gaze
Smartphone	5.7	5.9	1	3	1	1	2	2	80.25	79.48	4.4	4.2	2.9	2.8
Shopping	6.9	6.6	3	6	1	4	4	1	73.71	77.31	3.9	3.7	3.2	3.2
Bank	7.6	7.2	9	8	5	5	9	4	67.88	72.28	3.4	3.0	3.9	3.5



(a) Gaze distance relative to UI 9 digits **(b) Gaze distance relative to positions** **(c) Touch frequency** **(d) Gaze frequency**

Figure 2: Gaze distance relative to the 9 grid digits (a) and the pattern positions (b), showing how closely users follow their finger; and the frequency of the users' chosen pattern lengths (c, d).

5.2 Intersections

Intersections are "strokes which cross already drawn strokes" [von Zezschwitz 2016]. Users tend to include more intersections when using gaze than touch. However, the analysis did not reveal significant difference between gaze (M=.31; SD=.54) and touch (M=.24; SD=.51) modality ($F(1,53) = .611$, $p = .438$). Factor context showed significant differences between smartphone (M=.10; SD=.31), shopping (M=.27; SD=.450) and bank (M=.43; SD=.68), at $F(2,58) = 3.718$, $p = .025$. Comparisons showed significantly less intersections with smartphone than bank context ($p = .047$), potentially as drawing intersecting patterns using gaze is easier than when using touch.

5.3 Overlaps

We use overlaps as "crossing over an already activated cell by connecting to a distant cell" [von Zezschwitz 2016]. No significant differences were found for the modality between gaze (M=.19; SD=.39) and touch (M=.13; SD=.39) at $F(1,53) = .525$, $p = .472$, neither for the context between smartphone (M=.07; SD=.25), shopping (M=.13; SD=.34) and bank (M=30; SD=.54) at $F(2,58) = 3.222$, $p = .097$.

5.4 Knight Moves

A knight move "specifies the connection of two distant cells which are not directly neighboured." [von Zezschwitz 2016]. Analysis did not reveal significant difference between gaze (M=.13; SD=.34) and touch (M=.28; SD=.66) modality ($F(1,53) = 2.180$, $p = .146$), neither for the context ($F(2,58) = 1.661$, $p = .269$), between smartphone (M=.10; SD=.31), shopping (M=.17; SD=.46) and bank (M=.33; SD=.71). It was noticed that users include more knight moves in the bank situation, potentially due to the perceived sensitivity of the situation which requires a stronger password.

5.5 Observation Risk

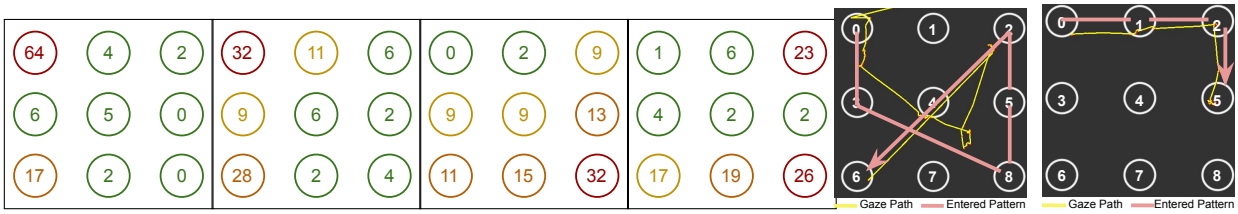
Observation risk is a function of number of cells, knight moves, overlaps, and intersections [von Zezschwitz 2016] that outputs a higher number with higher risk. We discard the parameter "visibility of the strokes" as the strokes were visible in both conditions. We find gaze has a slightly higher mean observation risk than touch, although no significant differences were found between gaze (M=76.49; SD= 9.89) and touch (M=74.18; SD=11.66) modality ($F(1,53) = 1.345$, $p = .251$). A significant difference was revealed for smartphone (M=79.92; SD= 7.30), shopping (M=74.89; SD=9.21) and bank (M=70.19; SD=13.68) context at $F(2,58) = 7.05$, $p = .005$. The posthoc test showed that the smartphone context resulted in significantly higher vulnerability than the bank context ($p = .004$), indicating touch patterns are slightly more secure to observation attacks. However, the nature of gaze input implies that it is robust to observation attacks, indicating that in future work the observation risk equation should be refined.

5.6 Memorability

Participants were asked to rate the memorability of the created patterns. Table 1 shows participants created similar patterns for both modalities. Analysis did not reveal significant difference between gaze (M=3.62; SD=1.44) and touch (M=3.98; SD= 1.15) modality ($F(1,49) = 2.309$, $p = .135$). Significant differences were found for smartphone (M=4.30; SD= 1.06), shopping (M=3.77; SD= 1.22) and bank (M=3.03; SD= 1.38), at $F(2,58) = 9.05$, $p = .001$. Posthoc tests showed, as expected, that smartphone patters are significantly more memorable than bank ($p = .001$).

5.7 Perceived Strength

There is almost no difference between the rated strength of the patterns between gaze and touch (Table 1). There are minor differences for the 3 scenarios between gaze (M=3.14; SD=.990) and touch (M=3.30; SD=1.129) modality ($F(1,49) = .635$, $p = .429$). A significant difference was found for smartphone (M=2.77; SD=1.01), shopping (M=3.20; SD=.89) and bank (M=3.63; SD=1.16) context



(a) Gaze start points (b) Touch start points (c) Gaze end points (d) Touch end points (e) Touch pattern (f) Gaze pattern

Figure 3: Start and end point distribution for gaze and touch patterns in percentages (a-d) showing top-left / bottom-right trends; and examples of the gaze path when entering a lock pattern with touch (e) or with gaze (f).

(F(2,58) = 6.44, p =.002), showing that bank patterns were perceived significantly stronger than smartphone patterns (p =.002).

5.8 Start and End Position

The majority of users tend to start their patterns from the top left corner [Uellenbeck et al. 2013]. We also analysed start and end positions for our patterns. We found that the majority of users (64%) also tend to start their patterns from the top left corner while using gaze. However, for touch 32% of the patterns started from the top left corner and 28% of the patterns started from the bottom left corner. For the end position in the gaze condition, we found that the majority of users (32%) tend to end their patterns with the right down position. However, for the touch end position 26% of the users ended their pattern with the right down position and 23% ended their patterns with top right point.

5.9 Additional Analysis: Gaze Calibration

Authentication and calibration are both secondary tasks, in the user's way to achieve their goal (e.g., write a message). Calibration is a tedious task, and conducting the calibration implicitly can improve usability [Pfeuffer et al. 2013]. We investigated whether the gaze data collected during TouchLockPattern authentication can be used to calibrate the eye tracker. The idea is that if the user's TouchLockPattern matches their gaze points, we could draw mappings between eye movements and positions on the screen, and use this data to calibrate the eye tracker.

We plotted the gaze path while entering patterns (Figure 3e-f). Users tend to look at the digits they are selecting when entering a TouchLockPattern. We calculated the visual angle of the gaze path for each point on the UI grid (the distance between the center of the UI element and the users gaze at the moment the finger enters the digit), shown in Figure 2a. We found the gaze is close to the digit at top left corner digits 0, 1, 3 (M=1.45 °), and further away at bottom right corner digits 5, 7, 8 (M=3.1 °).

We then analysed the gaze path with respect to the digit position in the patterns (i.e., distance between gaze at the moment the finger enters the digit, and the center digit position. As the pattern length increases, the gaze data becomes more accurate from 3 to 2 ° (Figure 2b). A reason may be, as with longer patterns, difficulty increases and users visually carefully inspect their touch. Thus, longer patterns can lead to more precise calibration data, which needs to be carefully designed as longer patterns reduce memorability (a Pearson correlation indicated negative correlation between memorability and length of patterns (r = -0.34, n = 284, p < 0.001)).

5.10 Discussion

Overall we found no significant difference between gaze and touch modalities, suggesting that findings from studies that investigated TouchLockPatterns are likely to match those on GazeLockPatterns. Users tend to use similar strategies (i.e. length and overlaps) while using the same interface with different modalities. Also, finding that user's gaze while doing TouchLockPatterns in 2 angles view opens a new design paradigm for future calibration methods. In addition to its known resistance to the common attack schemes ,i.e., shoulder surfing [Kumar et al. 2007], smudge attacks [Aviv et al. 2010], and thermal attacks [Abdelrahman et al. 2017], we find gaze has promising potential as a secure and usable modality for entering lock patterns. Eye tracking is increasingly becoming more available in off the shelf devices (e.g., many smartphones come with front-facing depth cameras) [Khamis et al. 2018a], which makes this an even more promising time to adopt gaze for authentication.

6 CONCLUSION AND FUTURE WORK

In this work, we investigated the difference between how users created touch and gaze patterns for authentication where we recorded gaze data for both conditions. We conducted a between subjects evaluation (N=40) where we asked the participants to create 3 patterns for 3 different scenarios. We found that as long as the interface is the same, people tend to use the same strategies. We also found that gaze is similar to touch while doing patterns, hence , it can be integrated to existing systems with no additional changes to the interface. We also found that user's gaze follow their touch pattern; future work should investigate in depth whether the user's gaze during authentication can be leveraged for calibration.

ACKNOWLEDGMENTS

This work was supported by the Royal Society of Edinburgh (RSE award number 65040), the Deutsche Forschungsgemeinschaft (DFG) (grant no. 316457582 and 425869382) and the Studienstiftung des deutschen Volkes ("German Academic Scholarship Foundation").

REFERENCES

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* (Denver, Colorado, USA) *(CHI '17)*. Association for Computing Machinery, New York, NY, USA, 3751–3763. https://doi.org/10.1145/3025453.3025461

Yasmeen Abdrabou, Mohamed Khamis, Rana Mohamed Eisa, Sherif Ismail, and Amr Elmougy. 2019. Just Gaze and Wave: Exploring the Use of Gaze and Gestures for Shoulder-Surfing Resilient Authentication. In *Proceedings of the 11th ACM*

Symposium on Eye Tracking Research & Applications (Denver, Colorado) *(ETRA '19)*. ACM, New York, NY, USA, 10. https://doi.org/10.1145/3314111.3319837

Evgeniy R. Abdulin and Oleg V. Komogortsev. 2015. Person Verification via Eye Movement-driven Text Reading Model. In *2015 IEEE 7th International Conference on Biometrics Theory, Applications and Systems (BTAS)*. IEEE, USA, 1–8. https://doi.org/10.1109/BTAS.2015.7358786

Panagiotis Andriotis, Theo Tryfonas, and George Oikonomou. 2014. Complexity Metrics and User Strength Perceptions of the Pattern-Lock Graphical Authentication Method. In *Proceedings of the Second International Conference on Human Aspects of Information Security, Privacy, and Trust - Volume 8533*. Springer-Verlag, Berlin, Heidelberg, 115–126. https://doi.org/10.1007/978-3-319-07620-1_11

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* (Washington, DC) *(WOOT'10)*. USENIX Association, USA, 1–7.

Darrell S. Best and Andrew T. Duchowski. 2016. A Rotary Dial for Gaze-based PIN Entry. In *Proceedings of the Ninth Biennial ACM Symposium on Eye Tracking Research & Applications* (Charleston, South Carolina) *(ETRA '16)*. ACM, New York, NY, USA, 69–76. https://doi.org/10.1145/2857491.2857527

Andreas Bulling, Florian Alt, and Albrecht Schmidt. 2012. Increasing the Security of Gaze-Based Cued-Recall Graphical Passwords Using Saliency Masks. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems* (Austin, Texas, USA) *(CHI '12)*. Association for Computing Machinery, New York, NY, USA, 3011–3020. https://doi.org/10.1145/2207676.2208712

Virginio Cantoni, Tomas Lacovara, Marco Porta, and Haochen Wang. 2018. A Study on Gaze-Controlled PIN Input with Biometric Data Analysis. In *Proceedings of the 19th International Conference on Computer Systems and Technologies* (Ruse, Bulgaria) *(CompSysTech '18)*. ACM, New York, NY, USA, 99–103. https://doi.org/10.1145/3274005.3274029

Cyber Code. Feb 2016. *C# - Gestural Pattern Draw Lock Screen Control (from Android devices) [RO]*. Youtube. https://www.youtube.com/watch?v=8dhO-P0wcyo&list=PLSqjYSJtqeaXQDuNi0Ko0fHSBk95Rcxjw&index=31

Alexander De Luca, Martin Denzel, and Heinrich Hussmann. 2009. Look into My Eyes! Can You Guess My Password?. In *Proceedings of the 5th Symposium on Usable Privacy and Security* (Mountain View, California, USA) *(SOUPS '09)*. Association for Computing Machinery, New York, NY, USA, Article 7, 12 pages. https://doi.org/10.1145/1572532.1572542

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

Alexander De Luca, Roman Weiss, Heinrich Hussmann, and Xueli An. 2008. Eyepass - Eye-stroke Authentication for Public Terminals. In *CHI '08 Extended Abstracts on Human Factors in Computing Systems* (Florence, Italy) *(CHI EA '08)*. ACM, New York, NY, USA, 3003–3008. https://doi.org/10.1145/1358628.1358798

Serge Egelman, Sakshi Jain, Rebecca S. Portnoff, Kerwell Liao, Sunny Consolvo, and David Wagner. 2014. Are You Ready to Lock?. In *Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security* (Scottsdale, Arizona, USA) *(CCS '14)*. Association for Computing Machinery, New York, NY, USA, 750–761. https://doi.org/10.1145/2660267.2660273

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* (San Jose, California, USA) *(CHI '16)*. Association for Computing Machinery, New York, NY, USA, 4806–4817. https://doi.org/10.1145/2858036.2858267

Corey D. Holland and Oleg V. Komogortsev. 2012. Biometric Verification via Complex Eye Movements: The Effects of Environment and Stimulus. In *2012 IEEE Fifth International Conference on Biometrics: Theory, Applications and Systems (BTAS)*. IEEE, USA, 39–46. https://doi.org/10.1109/BTAS.2012.6374556

Martti Juhola, Youming Zhang, and Jyrki Rasku. 2013. Biometric Verification of a Subject through Eye Movements. *Computers in Biology and Medicine* 43, 1 (2013), 42–50. https://doi.org/10.1016/j.compbiomed.2012.10.005

Christina Katsini, Yasmeen Abdrabou, George Raptis, Mohamed Khamis, and Florian Alt. 2020. The Role of Eye Gaze in Security and Privacy Applications: Survey and Future HCI Research Directions.. In *Proceedings of the 38th Annual ACM Conference on Human Factors in Computing Systems* (Honolulu, Hawaii, USA) *(CHI '20)*. ACM, New York, NY, USA, 21. https://doi.org/10.1145/3313831.3376840

Christina Katsini, Christos Fidas, Marios Belk, George Samaras, and Nikolaos Avouris. 2019. A Human-Cognitive Perspective of Users' Password Choices in Recognition-Based Graphical Authentication. *International Journal of Human-Computer Interaction* 25, 19 (2019), 1800–1812. https://doi.org/10.1080/10447318.2019.1574057

Christina Katsini, Christos Fidas, George E. Raptis, Marios Belk, George Samaras, and Nikolaos Avouris. 2018a. Eye Gaze-Driven Prediction of Cognitive Differences during Graphical Password Composition. In *23rd International Conference on Intelligent User Interfaces* (Tokyo, Japan) *(IUI '18)*. ACM, New York, NY, USA, 147–152. https://doi.org/10.1145/3172944.3172996

Christina Katsini, Christos Fidas, George E. Raptis, Marios Belk, George Samaras, and Nikolaos Avouris. 2018b. Influences of Human Cognition and Visual Behavior on Password Strength During Picture Password Composition. In *Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems* (Montreal QC, Canada) *(CHI '18)*. ACM, New York, NY, USA, Article 87, 14 pages. https://doi.org/10.1145/3173574.3173661

Christina Katsini, George E. Raptis, Christos Fidas, and Nikolaos Avouris. 2018c. Towards Gaze-based Quantification of the Security of Graphical Authentication Schemes. In *Proceedings of the 2018 ACM Symposium on Eye Tracking Research & Applications* (Warsaw, Poland) *(ETRA '18)*. ACM, New York, NY, USA, Article 17, 5 pages. https://doi.org/10.1145/3204493.3204589

Mohamed Khamis, Florian Alt, and Andreas Bulling. 2018a. The Past, Present, and Future of Gaze-enabled Handheld Mobile Devices: Survey and Lessons Learned. In *Proceedings of the 20th International Conference on Human-Computer Interaction with Mobile Devices and Services* (Barcelona, Spain) *(MobileHCI '18)*. ACM, New York, NY, USA. https://doi.org/10.1145/3229434.3229452

Mohamed Khamis, Carl Oechsner, Florian Alt, and Andreas Bulling. 2018b. VRpursuits: Interaction in Virtual Reality Using Smooth Pursuit Eye Movements. In *Proceedings of the 2018 International Conference on Advanced Visual Interfaces* (Castiglione della Pescaia, Grosseto, Italy) *(AVI '18)*. ACM, New York, NY, USA, Article 18, 8 pages. https://doi.org/10.1145/3206505.3206522

Mohamed Khamis, Ludwig Trotter, Ville Mäkelä, Emanuel von Zezschwitz, Jens Le, Andreas Bulling, and Florian Alt. 2018c. CueAuth: Comparing Touch, Mid-Air Gestures, and Gaze for Cue-based Authentication on Situated Displays. *Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies* 2, 4, Article 174 (Dec. 2018), 22 pages. https://doi.org/10.1145/3287052

Chandan Kumar, Daniyal Akbari, Raphael Menges, Scott MacKenzie, and Steffen Staab. 2019. TouchGazePath: Multimodal Interaction with Touch and Gaze Path for Secure Yet Efficient PIN Entry. In *2019 International Conference on Multimodal Interaction* (Suzhou, China) *(ICMI '19)*. Association for Computing Machinery, New York, NY, USA, 329–338. https://doi.org/10.1145/3340555.3353734

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* (Pittsburgh, Pennsylvania, USA) *(SOUPS '07)*. Association for Computing Machinery, New York, NY, USA, 13–19. https://doi.org/10.1145/1280680.1280683

Marte Loge, Markus Duermuth, and Lillian Rostad. 2016. On user choice for android unlock patterns. In *European Workshop on Usable Security, ser. EuroUSEC*, Vol. 16.

Ken Pfeuffer, Matthias J. Geiger, Sarah Prange, Lukas Mecke, Daniel Buschek, and Florian Alt. 2019. Behavioural Biometrics in VR: Identifying People from Body Motion and Relations in Virtual Reality. In *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems* (Glasgow, Scotland Uk) *(CHI '19)*. Association for Computing Machinery, New York, NY, USA, Article 110, 12 pages. https://doi.org/10.1145/3290605.3300340

Ken Pfeuffer, Melodie Vidal, Jayson Turner, Andreas Bulling, and Hans Gellersen. 2013. Pursuit Calibration: Making Gaze Calibration Less Tedious and More Flexible. In *Proceedings of the 26th Annual ACM Symposium on User Interface Software and Technology* (St. Andrews, Scotland, United Kingdom) *(UIST '13)*. Association for Computing Machinery, New York, NY, USA, 261–270. https://doi.org/10.1145/2501988.2501998

Vijay Rajanna, Adil H. Malla, Rahul A. Bhagat, and Tracy Hammond. 2018. DyGazePass: A Gaze Gesture-based Dynamic Authentication System to Counter Shoulder Surfing and Video Analysis Attacks. In *2018 IEEE 4th International Conference on Identity, Security, and Behavior Analysis (ISBA)*. IEEE, USA, 1–8. https://doi.org/10.1109/ISBA.2018.8311458

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* (Denver, Colorado, USA) *(CHI EA '17)*. ACM, New York, NY, USA, 1978–1986. https://doi.org/10.1145/3027063.3053070

Hananeh Salehifar, Peyman Bayat, and Mojtaba Amiri Majd. 2019. Eye Gesture Blink Password: A New Authentication System with High Memorable and Maximum Password Length. *Multimedia Tools and Applications* 78, 12 (Jun 2019), 16861–16885. https://doi.org/10.1007/s11042-018-7043-9

Ivo Sluganovic, Marc Roeschlin, Kasper B. Rasmussen, and Ivan Martinovic. 2018. Analysis of Reflexive Eye Movements for Fast Replay-Resistant Biometric Authentication. *ACM Transactions on Privacy and Security* 22, 1, Article 4 (Nov 2018), 30 pages. https://doi.org/10.1145/3281745

Sebastian Uellenbeck, Markus Dürmuth, Christopher Wolf, and Thorsten Holz. 2013. Quantifying the Security of Graphical Passwords: The Case of Android Unlock Patterns. In *Proceedings of the 2013 ACM SIGSAC Conference on Computer & Communications Security* (Berlin, Germany) *(CCS '13)*. Association for Computing Machinery, New York, NY, USA, 161–172. https://doi.org/10.1145/2508859.2516700

Emanuel von Zezschwitz. 2016. *Risks and Potentials of Graphical and Gesture-based Authentication for Touchscreen Mobile Devices Balancing Usability and Security through User-centered Analysis and Design*. PhD dissertation. Der Fakultät für Mathematik, Informatik und Statistik der Ludwig-Maximilians-Universität München.

Emanuel von Zezschwitz, Alexander De Luca, Philipp Janssen, and Heinrich Hussmann. 2015. Easy to Draw, but Hard to Trace? On the Observability of Grid-Based (Un)Lock Patterns. In *Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems* (Seoul, Republic of Korea) *(CHI '15)*. Association for Computing Machinery, New York, NY, USA, 2339–2342. https://doi.org/10.1145/2702123.2702202

Roman Weiss and Alexander De Luca. 2008. PassShapes: Utilizing Stroke Based Authentication to Increase Password Memorability. In *Proceedings of the 5th Nordic Conference on Human-Computer Interaction: Building Bridges* (Lund, Sweden) *(NordiCHI '08)*. Association for Computing Machinery, New York, NY, USA, 383–392. https://doi.org/10.1145/1463160.1463202

Guixin Ye, Zhanyong Tang, Dingyi Fang, Xiaojiang Chen, Kwang In Kim, Ben Taylor, and Zheng Wang. 2017. Cracking Android pattern lock in five attempts. In *Proceedings of the 2017 Network and Distributed System Security Symposium 2017 (NDSS 17)*. Internet Society.

Youming Zhang, Jorma Laurikkala, and Martti Juhola. 2014. Biometric Verification of a Subject with Eye Movements, with Special Reference to Temporal Variability in Saccades between a Subject's Measurements. *International Journal of Biometrics* 6, 1 (2014), 75. https://doi.org/10.1504/ijbm.2014.059643