An Eye Gaze-driven Metric for Estimating the Strength of Graphical Passwords based on Image Hotspots

Argyris Constantinides
University of Cyprus &
Cognitive UX Ltd.
Nicosia, Cyprus
aconst12@cs.ucy.ac.cy

Marios Belk
Cognitive UX GmbH
Heidelberg, Germany &
University of Cyprus
Nicosia, Cyprus
belk@cognitiveux.de

Christos Fidas
University of Patras
Rio, Patras, Greece
fidas@upatras.gr

Andreas Pitsillides
University of Cyprus
Nicosia, Cyprus
cspitsil@cs.ucy.ac.cy

ABSTRACT

In this paper, we propose an eye gaze-driven metric based on hotspot *vs.* non-hotspot segments of images for unobtrusively estimating the strength of user-created graphical passwords by analyzing the users' eye gaze behavior during password creation. To examine the feasibility of this method, *i.e.*, the existence of correlation between the proposed metric and the strength of users' generated passwords, we conducted an eye-tracking study (n=42), in which users created a graphical password with a personalized image that triggers declarative memory of users (*familiar image*) *vs.* an image illustrating generic content unfamiliar to the users' episodic and semantic memory (*generic image*). Results revealed a strong positive correlation between the password strength and the proposed eye gaze-driven metric, pointing towards a new direction for the design of intelligent eye gaze-driven graphical password schemes for unobtrusively assisting users in making better password choices.

CCS CONCEPTS

• Human-centered computing ~ Human computer interaction (HCI) • Security and privacy ~ Human and societal aspects of security and privacy

KEYWORDS

User Authentication, Graphical Passwords, Security, Eye-Tracking, Entropy.

ACM Reference format:

Constantinides, A., Belk, M., Fidas, C., Pitsillides, A. 2020. An Eye Gaze-driven Metric for Estimating the Strength of Graphical Passwords based on Image Hotspots. In *Proceedings of ACM Intelligent User Interface conference (IUI '20). ACM, New York, NY, USA, 5 pages.*

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 ACM 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.
IUI '20, March 17–20, 2020, Cagliari, Italy
© 2020 Association for Computing Machinery.
ACM ISBN 978-1-4503-7118-6/20/03…$15.00
https://doi.org/10.1145/3377325.3377537

1 INTRODUCTION

Intelligent user authentication schemes are moving in the center of attention lately [1, 3, 7-9, 16] aiming to assist users with the creation of secure and memorable passwords. Focusing on graphical user authentication (GUA) schemes, which require users to select images (or parts thereof) as their secret password, state-of-the-art research has provided evidence that the background images influence the strength of the graphical passwords [3, 29, 30, 34, 35].

A key issue in GUA schemes relates to the existence of *hotspots (points on an image that attract users to select them)* [29, 34], thus, leading to the creation of easily predictable passwords which are prone to automated attacks [33]. Several works have focused on preventing users from making poor password selections, mainly by limiting the available choices during password creation. Chiasson et al. [6] proposed a scheme in which users' choices are limited to one click-point per image for a total of five images. In their subsequent work, Chiasson et al. [5] used a viewport that highlights a random small area of the image aiming to persuade users selecting passwords that are less likely to include salient regions. Bulling et al. [3] proposed to hide potential hotspots using saliency maps, thus, preventing users from selecting them as part of their passwords. Thorpe et al. [28] used the "presentation effect" that gradually reveals the underlying image to influence users' choices during password creation. Katsini et al. [17] used a similar fade-out effect which starts from the highest saliency mask level and gradually reveals the image based on users' cognitive processing styles.

The discussed works primarily focus on alleviating the hotspots issue by intervening in a rather obtrusive way during password creation to influence users towards making better decisions. Given that the creation of a graphical password is a visual search task, and considering that various images contain hotspots, eye-tracking technology could be used to shed light on how users' gaze paths relate to hotspots, and eventually predict whether users may select passwords within hotspot segments. While attempts have been made towards improving and estimating the security of user authentication schemes by using eye-tracking technology [2, 3, 18, 21, 22, 27], to the best of the authors' knowledge, no research attempts have been made to estimate the strength of the potential password in GUA schemes by considering the users' eye gaze data on hotspots in an

unobtrusive way. Bearing in mind that individuals who produce fixations on image segments tend to select them as part of their password [25], and that users' visual behavior is affected by the hotspots on an image and the users' familiarity with the image [7, 10], we propose an eye gaze-driven metric based on hotspot *vs.* non-hotspot segments of the image for unobtrusively estimating the strength of user-created passwords by analyzing the users' eye gaze behavior during password creation.

2 ESTIMATING GRAPHICAL PASSWORD STRENGTH USING EYE GAZE-BASED ANALYSIS

Considering that hotspot selections negatively affect the strength of a graphical password, we focus on estimating the potential strength with respect to users' eye gaze behavior on hotspots during graphical password creation. To capture the variability of users' eye movement characteristics, we rely on the gaze transition entropy proposed by Krejtz et al. [20]. In particular, we focus on estimating the stationary entropy H_s, which captures the distribution of fixations over the stimulus (*i.e.*, areas of interest (AOIs) in which the eye-tracking metrics are applied). Lower values of H_s indicate that fixations tend to be concentrated on certain AOIs, while greater values of H_s occur when the visual attention is distributed more equally among AOIs. Stationary entropy H_s was conducted using Shannon's entropy equation expressed as:

$$H_s(X) = \sum_{i=1}^{N} p_i * log_2\left(\frac{1}{p_i}\right) \quad (1)$$

where X is the set of fixations for each user, N is the number of the available AOIs, and p is the probability of a user to fixate on AOI i. Considering that fixation duration correlates with cognitive processing [14, 24] and that users who exhibit longer fixations on AOIs tend to select them [25], we compute the probability p_i as follows:

$$p_i = \frac{d_i}{N}, \sum_{i=1}^{N} = 1 \quad (2)$$

where d_i is the distribution of p_i across N, representing the total fixation duration on AOI i. By applying equation (2) to equation (1), we compute the entropy of fixations as follows:

$$H_s(X) = \sum_{i=1}^{N} \frac{d_i}{N} * log_2(N) \quad (3)$$

N=3: the image is divided into three vertical AOIs [20].

Building on existing work [18], we compute the potential strength of the graphical password using the gaze-based entropy metric as follows:

$$H(P) = \sum_{k=1}^{L} \sum_{j=1}^{H_{pool}} \frac{d_j}{H_{pool}} * log_2(H_{pool}) \quad (4)$$

L=3: the graphical password consists of three gestures.

Unlike [18], we consider only the segments covering the hotspots of the image. Therefore, we define the H_{pool} as the number of available hotspots choices on an image. Given that longer fixations on hotspot choices increase the likelihood that users will potentially choose them as part of their passwords, d_j represents the total fixation duration on hotspot choice j.

Since hotspot selections lead to weak graphical passwords, we take an extra step to penalize fixations on hotspots. Considering the additive nature of Shannon's entropy [19], we subtract fixations on hotspots as calculated in equation (4) from the fixations on AOIs as calculated in equation (3). Therefore, equations (3) and (4) are combined as follows:

$$H(P) = \sum_{i=1}^{N} \frac{d_i}{N} * log_2(N) - \sum_{k=1}^{L} \sum_{j=1}^{H_{pool}} \frac{d_j}{H_{pool}} * log_2(H_{pool}) \quad (5)$$

Equation (5) represents the eye gaze-based metric used for the estimation of the potential graphical password strength in terms of entropy. The higher the gaze-based entropy a user has, the higher the chance a strong password will be created.

3 FEASIBILITY STUDY

3.1 Research Question

RQ. Is there a correlation between the proposed metric from equation (5) and the password strength in GUA schemes?

3.2 Study Instruments and Metrics

3.2.1 Graphical User Authentication Scheme. We implemented a Web-based cued-recall graphical authentication scheme, similar to Windows 10™ PGA [15], in which users can create gesture-based passwords on a background image that acts as a cue. Three types of gestures are allowed: taps, lines and circles. The image is divided in a grid containing 100 segments on the longest side and scaled accordingly on the shortest side. The mechanism allows for a tolerance distance (36 segments around each selected segment are acceptable[1] [17]), but there is no tolerance regarding the ordering, type, directionality of gestures.

3.2.2 Image Types. We expect that users will follow different approaches during password creation depending on the image content delivered to them (*i.e.*, familiar *vs.* generic images) [8, 9]. Furthermore, we expect that users from the familiar image group will make less hotspot selections for their passwords. This is based on sociocultural theories which state that familiar images will trigger users' episodic memories (*i.e.*, the part of long-term memory that involves the recollection of personal experiences in events and certain situations) [31], which could affect them in choosing segments related to their personal experiences with the depicted content rather than to hotspots which attract visual attention by default and are more easily remembered by users. Hence, to better control the study, we chose two specific image sets: *i) personalized images:* familiar images highly related to the participants' daily life context, *i.e.*, lab rooms, cafeteria, etc.; and *ii) generic images:* images illustrating generic content unfamiliar to the users, *i.e.*, with generic sceneries and people.

The selection of images was based on research that has shown that users tend to select images illustrating people [1, 11] and scenery [11, 36]. To minimize bias effects of using one image per group, we provided a set of nine images per group and users could select only one image from their corresponding image set.

[1] bit.ly/2tmvOru

Figure 1. At the top, a *generic* image depicting a generic scenery with people (left), and a *familiar* image depicting a lab room at the participants' University (right). At the bottom, the saliency maps of the images are depicted.

Considering that the number of hotspots and the image complexity affect the password strength [17, 35], we chose images of similar number of hotspots and complexity between and within images belonging to the two groups. To calculate the number of hotspots, we followed a semi-automated approach through a combination of computer vision techniques for object detection[2,3], and a combination of saliency maps[4] and saliency filters [23] for the salient segments. Furthermore, we assessed the equivalence of the two image sets by calculating the image complexity through entropy estimators[5] [4]. Figure 1 illustrates two example image types and their saliency maps.

3.2.3 Apparatus. The study was conducted using a personal computer with a 24" monitor at a screen resolution of 1920x1080 pixels. To capture eye movements, we used the Gazepoint GP3 eye tracker [13]. No equipment was attached to the participants.

3.2.4 Password Strength Metric. We measured the number of guesses required to crack passwords, a widely used password strength metric [36, 37]. Following existing approaches [17, 26, 36, 37], we used a *brute-force attack* starting from the segments covering the hotspots, then checking the neighboring segments, and finally checking the rest of the segments. The final number of guesses represents the strength of the graphical password.

3.3 Sampling and Procedure

3.3.1 Participants. A total of 42 individuals (13 females) participated in the study, ranging in age between 20-32 years old (m=24, sd=3.1). Participants were split evenly into two groups, and the image type was randomly varied across all users. To increase the internal validity of the study, we recruited participants that had no prior experience with PGA-like authentication mechanisms, and had spent the last three years at the University campus, assuming they would have had experiences within the University's context.

3.3.2 Experimental Design and Procedure. We adopted the University's human research protocol that takes into consideration users' privacy, confidentiality and anonymity. All participants performed the task in a quiet lab room with only the researcher present. The study involved the following steps: first, participants signed a consent form. Next, they completed a questionnaire on demographics and the eye-calibration process followed. Next, the participants were introduced to a demo page to familiarize themselves with the process of drawing gestures. Half of the participants received a selection of nine familiar images, and the other half a selection of nine generic images. To increase ecological validity and keep security as a secondary task [12], participants were requested to create a user account using our PGA scheme, in order to use this account in the subsequent weeks for accessing student materials within a University's course Website. First, they selected one image out of the nine available images, on which they drew three gestures using a computer mouse. To confirm their password, they were requested to reproduce the initial three gestures.

4 ANALYSIS OF RESULTS

In the analyses that follow, data are mean ± standard error, unless otherwise stated. There were no significant outliers.

To investigate our *RQ*, we performed a Pearson's Product Moment correlation test, between the gaze-based entropy from equation (5) and password strength. The analysis revealed a strong positive correlation between gaze-based entropy and password strength (r=.562, p<.001) as shown in Figure 2 (left). The higher the gaze-based entropy, the stronger the graphical password. We further ran an independent-samples t-test to investigate the effect of image type on gaze-based entropy revealing that entropy between the groups was significantly different (t(35)=2.834, p=.008); the familiar group had an entropy of 11.71 ± 6.71, while the generic group had an entropy of 6.12 ± 5.22. To get further insights about the correlation, we computed the percentages of fixation count and fixation duration on (non)hotspot segments of the image. Users of the generic group exhibited more and longer fixations on hotspots *vs.* non-hotspots compared to the users of the familiar group, as depicted in Figure 2 (middle) and Figure 2 (right) respectively.

Results have shown that the proposed gaze-based metric is a credible predictor of password strength based on how user's attention shifts and is distributed between AOIs, and how many hotspots have been explored (Figure 2 middle) and for how long (Figure 2 right). Such a metric could be a valuable tool for security experts for calculating the practical security of a GUA scheme aiming to estimate how strong the graphical password will be, without intervening in the password creation task. Compared to traditional password strength meters that intervene in the user interaction by requiring users to first enter the password and then provide a strength estimation [32], the proposed metric provides an unobtrusive way to influence users towards better password decisions until a certain level of eye gaze entropy is reached.

[2] tensorflow.org
[3] cloud.google.com/vision
[4] bit.ly/38aJswB
[5] bit.ly/2wB7Erm

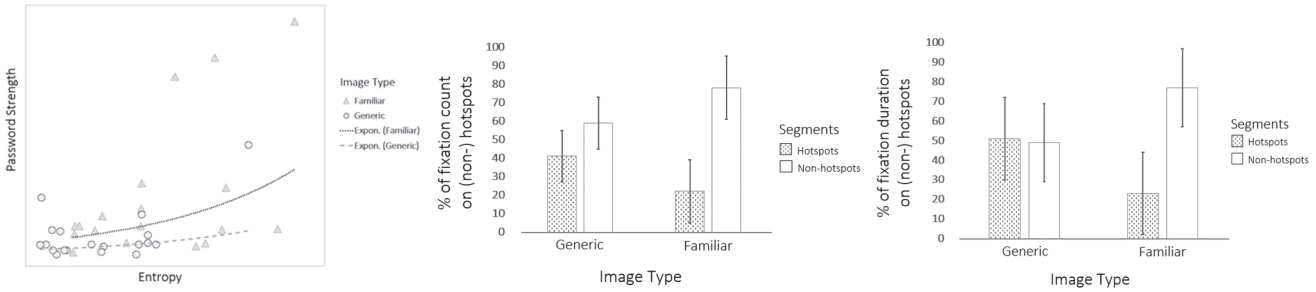

Figure 2: Scatter-plots for password strength and entropy (left). Percentage of fixation count (middle) and fixation duration (right) on hotspots *vs.* non-hotspots across the two groups.

5 IMPLICATIONS

Findings of this work point towards a new direction for the design of intelligent eye gaze-driven graphical password schemes for unobtrusively assisting users in making better password choices. Specifically, we envision an intelligent eye gaze-driven graphical password scheme (Figure 3), which consists of the following components:

Image Engine: Responsible for the retrieval, analysis, and filtering of the images that will be used in the GUA scheme. Images could be fetched from online sources[6] or uploaded by the end-users. To ensure that the candidate images contain visually rich content (in terms of number of attention points they entail), the image complexity will be calculated through a combination of saliency maps [23] and entropy estimators [4]. With respect to the detection of hotspot segments contained in each image, a combination of saliency maps similar to [3] and [23] will be used. Furthermore, we expect that users will make their password selections around objects easily distinguishable from their surroundings on the image [29, 37]. Therefore, an extra step will be taken to consider these objects as potential hotspots using object detection mechanisms[2,3]. Finally, the filtering mechanism will filter out inappropriate candidate images (*e.g.*, simple images with limited number of attention points).

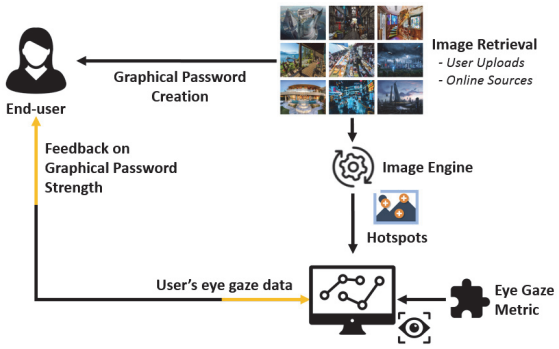

Figure 3. An intelligent eye gaze-driven GUA scheme assisting users towards making better password choices.

[6] developers.google.com/custom-search

Eye-Tracking Software: Responsible for capturing users' visual behavior during graphical password creation. The hotspot segments detected by the *Image Engine* will be automatically applied in the software. During users' interaction with the GUA scheme, the proposed eye gaze-driven metric will be calculated in real-time, thus, allowing for unobtrusively estimating the potential password strength by considering the hotspot segments of the image. Finally, the end-users will be notified whether they are moving towards the creation of a weak or a strong password.

6 CONCLUSIONS

In this paper we proposed an eye gaze-driven metric for unobtrusively estimating the strength of user-chosen graphical passwords based on eye gaze variability and attention on hotspots during graphical password creation. These constitute the basis of an intelligent eye gaze-driven graphical password scheme (Figure 3) for unobtrusively assisting users in making better password choices during password creation.

Limitations relate to the nature of the in-lab eye-tracking study in which the users' selections might have been influenced, however, no such comment was received from our participants. Also, we used a rather simple guessing algorithm to measure and compare the strength of the user-chosen passwords since the aim of this work was not to create and test another cracking algorithm, but instead a valid baseline approach for measuring and comparing the users' graphical password strength.

ACKNOWLEDGEMENTS

This research has been partially supported by the EU Horizon 2020 Grant 826278 "Securing Medical Data in Smart Patient-Centric Healthcare Systems" (Serums).

REFERENCES

[1] Florian Alt, Stefan Schneegass, Alireza Sahami Shirazi, Mariam Hassib, and Andreas Bulling. 2015. Graphical Passwords in the Wild: Understanding How Users Choose Pictures and Passwords in Image-based Authentication Schemes. In *Proceedings of the 17th International Conference on Human-Computer Interaction with Mobile Devices and Services (MobileHCI '15)*. ACM, 316-322. DOI: https://doi.org/10.1145/2785830.2785882

[2] 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 (ETRA '16)*. ACM, 69–76. DOI: https://doi.org/10.1145/2857491.2857527

[3] 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 (CHI '12)*. ACM, 3011-3020. DOI: https://doi.org/10.1145/2207676.2208712

[4] Maurizio Cardaci, Vito Di Gesù, Maria Petrou, and Marco Elio Tabacchi. 2009. A fuzzy approach to the evaluation of image complexity. *Fuzzy Sets and Systems* 160, 10 (May 2009), 1474-1484. DOI: http://dx.doi.org/10.1016/j.fss.2008.11.017

[5] Sonia Chiasson, Alain Forget, Robert Biddle, and Paul C. van Oorschot. 2008. Influencing users towards better passwords: persuasive cued click- points. In *Proceedings of the 22nd British HCI Group Annual Conference on People and Computers: Culture, Creativity, Interaction-Volume 1 (BCS-HCI '08)*. BCS Learning & Development Ltd., Swindon, UK, 121-130.

[6] Sonia Chiasson, P. C. Van Oorschot, and Robert Biddle. 2007. Graphical password authentication using cued click points. In *Proceedings of the 12th European conference on Research in Computer Security (ESORICS '07)*, Joachim Biskup and Javier Lopez (Eds.). Springer-Verlag, Berlin, Heidelberg, 359-374. DOI: https://doi.org/10.1007/978-3-540-74835-9_24

[7] Argyris Constantinides, Marios Belk, Christos Fidas, Andreas Pitsillides. 2019. On the Accuracy of Eye Gaze-driven Classifiers for Predicting Image Content Familiarity in Graphical Passwords. In *Proceedings of 27th Conference on User Modeling, Adaptation and Personalization (UMAP '19)*, ACM, 201-205. DOI: https://doi.org/10.1145/3320435.3320474

[8] Argyris Constantinides, Marios Belk, Christos Fidas, and George Samaras. 2018. On Cultural-centered Graphical Passwords: Leveraging on Users' Cultural Experiences for Improving Password Memorability. In *Proceedings of the 26th Conference on User Modeling, Adaptation and Personalization (UMAP '18)*. ACM, 245-249. DOI: https://doi.org/10.1145/3209219.3209254

[9] Argyris Constantinides, Christos Fidas, Marios Belk, Andreas Pitsillides. 2019. October). "I Recall this Picture": Understanding Picture Password Selections based on Users' Sociocultural Experiences. In *IEEE/WIC/ACM International Conference on Web Intelligence (WI '19)* (pp. 408-412). ACM. DOI: https://doi.org/10.1145/3350546.3352557

[10] Argyris Constantinides, Christos Fidas, Marios Belk, and George Samaras. 2018. On sociocultural-centered graphical passwords: an initial framework. In *Proceedings of the 20th International Conference on Human-Computer Interaction with Mobile Devices and Services Adjunct (MobileHCI '18)*. ACM, 277-284. DOI: https://doi.org/10.1145/3236112.3236150

[11] Paul Dunphy and Jeff Yan. 2007. Do background images improve "draw a secret" graphical passwords?. In *Proceedings of the 14th ACM conference on Computer and communications security (CCS '07)*. ACM, 36-47. DOI: https://doi.org/10.1145/1315245.1315252

[12] Serge Egelman, Andreas Sotirakopoulos, Ildar Muslukhov, Konstantin Beznosov, and Cormac Herley. 2013. Does my password go up to eleven?: the impact of password meters on password selection. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems (CHI '13)*. ACM, 2379-2388. DOI: https://doi.org/10.1145/2470654.2481329

[13] GP3 Eye Tracker. 2018. [Online] Available at: https://www.gazept.com/

[14] David E. Irwin. 2004. Fixation Location and Fixation Duration as Indices of Cognitive Processing. In J. M. Henderson & F. Ferreira (Eds.), *The interface of language, vision, and action: Eye movements and the visual world* (p. 105–133). Psychology Press.

[15] Jeffrey Jay Johnson, Steve Seixeiro, Zachary Pace, Giles van der Bogert, Sean Gilmour, Levi Siebens, and Kenneth Tubbs. 2014. Picture Gesture Authentication. Retrieved from https://www.google.com/patents/US8910253

[16] Christina Katsini, Christos Fidas, George E. Raptis, Marios Belk, George Samaras, and Nikolaos Avouris. 2018. Eye Gaze-driven Prediction of Cognitive Differences during Graphical Password Composition. In *23rd International Conference on Intelligent User Interfaces (IUI '18)*. ACM, 147-152. DOI: https://doi.org/10.1145/3172944.3172996

[17] Christina Katsini, Christos Fidas, George E. Raptis, Marios Belk, George Samaras, and Nikolaos Avouris. 2018. 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 (CHI '18)*. ACM, Paper 87, 14 pages. DOI: https://doi.org/10.1145/3173574.3173661

[18] Christina Katsini, George E. Raptis, Christos Fidas, and Nikolaos Avouris. 2018. Towards gaze-based quantification of the security of graphical authentication schemes. In *Proceedings of the 2018 ACM Symposium on Eye Tracking Research & Applications (ETRA '18)*. ACM, Article 17, 5 pages. DOI: https://doi.org/10.1145/3204493.3204589

[19] Saranga Komanduri, Richard Shay, Patrick Gage Kelley, Michelle L. Mazurek, Lujo Bauer, Nicolas Christin, Lorrie Faith Cranor, and Serge Egelman. 2011. Of passwords and people: measuring the effect of password-composition policies. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems (CHI '11)*. ACM, 2595-2604. DOI: https://doi.org/10.1145/1978942.1979321

[20] Krzysztof Krejtz, Andrew Duchowski, Tomasz Szmidt, Izabela Krejtz, Fernando González Perilli, Ana Pires, Anna Vilaro, and Natalia Villalobos. 2015. Gaze Transition Entropy. *ACM Transactions on Applied Perception (TAP)* 13, 1, Article 4 (Dec. 2015), 20 pages. DOI: https://doi.org/10.1145/2834121

[21] 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, Article 7 , 12 pages. DOI: http://dx.doi.org/10.1145/1572532.1572542

[22] Kenrick Mock, Bogdan Hoanca, Justin Weaver, and Mikal Milton. 2012. Real-time Continuous Iris Recognition for Authentication Using an Eye Tracker. In *Proceedings of the 2012 ACM Conference on Computer and Communications Security (CCS '12)*. ACM, 1007–1009. DOI: https://doi.org/10.1145/2382196.2382307

[23] Federico Perazzi, Philipp Krähenbühl, Yael Pritch, and Alexander Hornung. 2012. Saliency filters: Contrast based filtering for salient region detection. *2012 IEEE Conference on Computer Vision and Pattern Recognition (CVPR '12)*. IEEE, Providence, RI, USA, 733-740. DOI: 10.1109/CVPR.2012.6247743

[24] George E. Raptis, Christos Fidas, and Nikolaos Avouris. 2018. Effects of Mixed-Reality on Players' Behaviour and Immersion in a Cultural Tourism Game: A Cognitive Processing Perspective. *International Journal of Human-Computer Studies* 114 (2018), 69 – 79. DOI: https://doi.org/10.1016/j.ijhcs.2018.02.003

[25] George E. Raptis, Christina Katsini, Marios Belk, Christos Fidas, George Samaras, and Nikolaos Avouris. 2017. Using Eye Gaze Data and Visual Activities to Infer Human Cognitive Styles: Method and Feasibility Studies. In *Proceedings of the 25th Conference on User Modeling, Adaptation and Personalization (UMAP '17)*. ACM, 164–173. DOI: https://doi.org/10.1145/3079628.3079690

[26] Amir Sadovnik and Tsuhan Chen. 2013. A Visual Dictionary Attack on Picture Passwords. In *2013 IEEE International Conference on Image Processing*. 4447–4451. DOI: 10.1109/ICIP.2013.6738916

[27] Ivo Sluganovic, Marc Roeschlin, Kasper B. Rasmussen, and Ivan Martinovic. 2016. Using Reflexive Eye Movements for Fast Challenge-Response Authentication. In *Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security (CCS '16)*. ACM, 1056–1067. DOI: https://doi.org/10.1145/2976749.2978311

[28] Julie Thorpe, Muath Al-Badawi, Brent MacRae, and Amirali Salehi-Abari. 2014. The presentation effect on graphical passwords. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems (CHI '14)*. ACM, 2947-2950. DOI: https://doi.org/10.1145/2556288.2557212

[29] Julie Thorpe, and Paul C. van Oorschot. 2007. Human-seeded attacks and exploiting hot-spots in graphical passwords. In *Proceedings of the 16th USENIX Security Symposium (SS '07)*. USENIX Association, Berkeley, CA, USA, Article 8, 16 pages.

[30] Thomas S. Tullis and Donna P. Tedesco. 2005. Using personal photos as pictorial passwords. In *CHI'05 Extended Abstracts on Human Factors in Computing Systems (CHI EA '05)*. ACM, 1841-1844. DOI: http://dx.doi.org/10.1145/1056808.1057036

[31] Tulving, E. (1972). Episodic and semantic memory. Organization of memory, 1, 381-403.

[32] Blase Ur, Patrick Gage Kelley, Saranga Komanduri, Joel Lee, Michael Maass, Michelle L. Mazurek, Timothy Passaro, Richard Shay, Timothy Vidas, Lujo Bauer, Nicolas Christin, and Lorrie Faith Cranor. 2012. How Does Your Password Measure Up? The Effect of Strength Meters on Password Creation. In *21st USENIX Security Symposium (USENIX Security '12)*. USENIX, Bellevue, WA, 65–80.

[33] Paul C. van Oorschot, Amirali Salehi-Abari, and Julie Thorpe. 2010. Purely Automated Attacks on PassPoints-Style Graphical Passwords. In *IEEE Transactions on Information Forensics and Security* 5, 3 (September 2010), 393-405. DOI: 10.1109/TIFS.2010.2053706

[34] Paul C. van Oorschot and Julie Thorpe. 2011. Exploiting predictability in click-based graphical passwords. *Journal of Computer Security* 19, 4 (December 2011), 669-702. DOI: 10.3233/JCS-2010-0411

[35] Susan Wiedenbeck, Jim Waters, Jean-Camille Birget, Alex Brodskiy, and Nasir Memon. 2005. Authentication using graphical passwords: effects of tolerance and image choice. In *Proceedings of the 2005 symposium on Usable privacy and security (SOUPS '05)*. ACM, 1-12. DOI: http://dx.doi.org/10.1145/1073001.1073002

[36] Ziming Zhao, Gail-Joon Ahn, and Hongxin Hu. 2015. Picture Gesture Authentication: Empirical Analysis, Automated Attacks, and Scheme Evaluation. *Journal of ACM Transactions on Information and System Security (TISSEC)* 17, 4, Article 14 (April 2015), 37 pages. DOI: http://dx.doi.org/10.1145/2701423

[37] Ziming Zhao, Gail-Joon Ahn, Jeong-Jin Seo, and Hongxin Hu. 2013. On the security of picture gesture authentication. In *Proceedings of the 22nd USENIX conference on Security (SEC '13)*. USENIX Association, Berkeley, CA, USA, 383-398.