Towards Gaze-Based Quantification of the Security of Graphical Authentication Schemes

Christina Katsini
Human Opsis and HCI Group, Dept. of Electrical and Computer Engineering, University of Patras
Patras, Greece
katsinic@upnet.gr

George E. Raptis
Human Opsis and HCI Group, Dept. of Electrical and Computer Engineering, University of Patras
Patras, Greece
raptisg@upnet.gr

Christos Fidas
Dept. of Cultural Heritage Management and New Technologies, University of Patras
Patras, Greece
fidas@upatras.gr

Nikolaos Avouris
HCI Group, Dept. of Electrical and Computer Engineering, University of Patras
Patras, Greece
avouris@upatras.gr

ABSTRACT

In this paper, we introduce a two-step method for estimating the strength of user-created graphical passwords based on the eye-gaze behaviour during password composition. First, the individuals' gaze patterns, represented by the unique fixations on each area of interest (AOI) and the total fixation duration per AOI, are calculated. Second, the gaze-based entropy of the individual is calculated. To investigate whether the proposed metric is a credible predictor of the password strength, we conducted two feasibility studies. Results revealed a strong positive correlation between the strength of the created passwords and the gaze-based entropy. Hence, we argue that the proposed gaze-based metric allows for unobtrusive prediction of the strength of the password a user is going to create and enables intervention to the password composition for helping users create stronger passwords.

CCS CONCEPTS

• **Security and privacy → Graphical / visual passwords**; • **Computing methodologies** → *Model verification and validation*; • **Human-centered computing** → *Visual analytics*;

KEYWORDS

Graphical user authentication, graphical passwords, eye-tracking, password strength estimation, entropy

ACM Reference Format:
Christina Katsini, George E. Raptis, Christos Fidas, and Nikolaos Avouris. 2018. Towards Gaze-Based Quantification of the Security of Graphical Authentication Schemes. In *ETRA '18: 2018 Symposium on Eye Tracking Research and Applications, June 14–17, 2018, Warsaw, Poland.* ACM, New York, NY, USA, 5 pages. https://doi.org/10.1145/3204493.3204589

ETRA '18, June 14–17, 2018, Warsaw, Poland
© 2018 Association for Computing Machinery.
ACM ISBN 978-1-4503-5706-7/18/06…$15.00
https://doi.org/10.1145/3204493.3204589

1 INTRODUCTION

Graphical user authentication (GUA) is a widely deployed alternative to alphanumeric passwords. GUA schemes lie under two categories, based on the memory function they trigger: recognition and recall. In recognition-based GUA schemes, users select a set of images from a larger set to create a password (e.g., PassFaces [Brostoff and Sasse 2000], DéjàVu [Dhamija and Perrig 2000]). In recall-based GUA schemes, they create a drawing on a canvas (e.g., PassPoints [Wiedenbeck et al. 2005], Cued Click Points [Chiasson et al. 2007]), with background images often being used as cues.

Researchers initially focused on the usability aspects of GUA schemes aiming to provide quicker login services and easier to remember passwords [Biddle et al. 2012]. However, the proposed GUA schemes raised security issues, as their theoretical entropy (i.e., an estimation of the password strength against brute-force attacks) was lower than that of the alphanumeric password schemes deployed in the market [Katsini et al. 2016]. To overcome these issues, GUA schemes with similar entropies to those of alphanumeric authentication schemes were proposed, but, analysis of the strength of the user-created graphical passwords revealed that users make predictable choices [Dirik et al. 2007; Salehi-Abari et al. 2008; Zhao et al. 2015], as they often select images located at the top of the image grid or they draw their passwords on salient points of images. To prevent users from making predictable password choices, Bulling et al. [2012] proposed the use of saliency masks for hiding salient points, Chiasson et al. [2007] proposed a scheme with multiple successive images, where users were allowed to select a single point per image. In their latest work, Chiasson et al. [2012] used a view-port positioned randomly on the image to persuade the users to select passwords less likely to include salient points. Thorpe et al. [2014] used the *drawing-the-curtain* effect (i.e., gradually reveal the image grid either from left to right or from right to left) to influence users' password choices.

The discussed research attempts modify GUA schemes and intervene in the users' decision-making process during password creation. In addition, they could be exploited by attackers, as they provide explicit knowledge of points that the users would not or could not select. Given that selecting a graphical password is a visual search activity, eye-tracking technology could enable the prediction of the graphical passwords' strength and influence the users towards better decisions, without revealing any information about their choices. Despite that eye tracking has been used as an input for GUA schemes [Best and Duchowski 2016; Bulling et al. 2012; Hoanca and Mock 2006; Stobert et al. 2010] and in behavioural biometrics authentication [Mock et al. 2012; Sluganovic et al. 2016], to the knowledge of the authors, no research attempts have been made to quantify the security of GUA schemes using eye-tracking data. Hence, in this paper, we propose *gaze-based entropy*, a security metric for GUA schemes based on the user's visual behaviour during password creation and we investigate whether it can be used to estimate the strength of user-created graphical passwords. We believe that knowing how much and for how long the user is looking at images or points of images could provide a measure of the maximum possible strength of a password the user will create.

2 GAZE-BASED ENTROPY

According to information theory, Shannon's entropy for each available discrete random variable X is defined as:

$$H(X) = \sum_{i=1}^{N} p_i log_2 \left(\frac{1}{p_i}\right) \tag{1}$$

In GUA, we define each discrete random variable, which can be used as part of the password, as *choice C*. For example, when a user is asked to select a picture from a set of pictures to create a password, each picture is a probable *choice C* . In parallel to alphanumeric authentication schemes, *choice* is equal to *symbol* (i.e. individual character from a character set). In equation (1), p_i is the probability to select choice c_i out of the N choices. Given that there is a specific number of available choices, we define *choice pool* C_{pool}, which is the number of the available choices. Therefore:

$$p_i = \frac{d_i}{C_{pool}}, \sum_{i=1}^{C_{pool}} = 1 \tag{2}$$

In equation (2), d_i is the distribution of p_i across C_{pool}. Equation (1) computes the entropy of a single choice. Given that each graphical password consists of L choices (i.e., the length of the password), the entropy of the password policy is:

$$H(P) = \sum_{j=1}^{L} \sum_{i=1}^{C_{pool}} \frac{d_i}{C_{pool}} log_2 C_{pool} \tag{3}$$

Equation (3) applies for passwords of non-unique choices (i.e., a choice can be used more than once as part of the password). In case the password policy states that each choice can be used only once in the password, the equation takes the following form:

$$H(P) = \sum_{j=1}^{L} \sum_{i=1}^{C_{pool}} \frac{d_i}{C_{pool} - u \times (i-1)} log_2 C_{pool} \tag{4}$$

If the choices are unique, then $u = 1$, else $u = 0$. Equation (4) applies for a single *set S* of choices. If there is more than one S of choices (e.g., authentication in multiple screens), the equation is:

$$H(P) = \sum_{k=1}^{S} \sum_{j=1}^{L} \sum_{i=1}^{C_{pool}} \frac{d_i}{C_{pool} - u \times (i-1)} log_2 C_{pool} \tag{5}$$

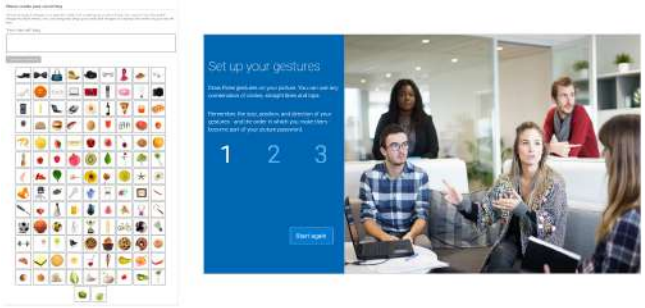

Figure 1: The recognition-based (left) and the recall-based (right) GUA scheme used in our feasibility studies.

Focusing on the eye-gaze behaviour of the users, we define the C_{pool} as the number of the fixated choices, as a choice can be used in a password once it has been fixated by the user. For example, if a GUA scheme requires a user to select an image out of twenty images, and she/he fixates on six of them, then $C_{pool} = 6$. Given that fixation duration is correlated to cognitive processing [Irwin 2004; Raptis et al. 2018] and that people who produce longer fixations to segments tend to select them [Raptis et al. 2017], d_i represents the total fixation duration on the choice c_i. Adopting these modifications, equation (5) is now a gaze-based metric, which represents an estimation of the graphical password strength in terms of entropy: *gaze-based entropy.*

3 FEASIBILITY STUDIES

To evaluate the proposed gaze-based entropy towards the user-created password strength, we performed a correlation analysis between the gaze-based entropy and the created passwords' strength for a recognition-based and a recall-based GUA scheme. The null hypotheses of our studies are:

- **H0**$_1$ The gaze-based entropy is not correlated with the graphical password strength in a recognition-based GUA scheme;
- **H0**$_2$ The gaze-based entropy is not correlated with the graphical password strength in a recall-based GUA scheme.

3.1 Methodology

3.1.1 Graphical user authentication schemes . As a recognition-based GUA scheme (Fig. 1:left), we used the one presented in [Belk et al. 2017], which is based on well-known recognition-based GUA schemes, such as DéjàVu [Dhamija and Perrig 2000], PassFaces [Brostoff and Sasse 2000] and ImagePass [Mihajlov et al. 2011]. To create a graphical password, the user must select 5 unique images from a set of 120 images. Hence, the parameters of equation (5) are:

L=5: the password consists of five images;
u=1: the images can only be used once;
S=1: all images are presented in one screen.

C_{pool} and d_i are calculated for each user, based on the number of unique fixated images during password composition. Hence, equation (5) takes the following form:

$$H(P) = \sum_{j=1}^{5} \sum_{i=1}^{C_{pool}} \frac{d_i}{C_{pool} - (i-1)} log_2 C_{pool}$$

As a recall-based GUA scheme (Fig. 1:right), we used a scheme similar to Windows Picture Passwords [Sinofsky 2011]. A background image is selected as a cue and the user must draw three gestures (taps, lines or circles) on the image to create a graphical password. The background image is divided in 100x100 segments and there is a tolerance of 36 segments around each segment when reproducing a password. The parameters of equation (5) are:

L=3: the password consists of three gestures;
u=0: each segment can be re-used for another gesture;
S=1: all the gestures are drawn in one screen.

C_{pool} and d_i are calculated for each user, based on the number of unique fixated segments and the number of available gestures for each fixated segment. Equation (5) takes the following form:

$$H(P) = \sum_{j=1}^{3} \sum_{i=1}^{C_{pool}} \frac{d_i}{C_{pool}} log_2 C_{pool}$$

3.1.2 Participants. For the recognition-based GUA scheme, we recruited 109 individuals (50 females), ranging in age between 18 and 47 years ($m = 30.5; sd = 7.3$). For the recall-based GUA scheme, we recruited 36 individuals (16 females), ranging in age between 22 and 38 years ($m = 31.7; sd = 6.1$). The participants had diverse educational and professional profiles (recognition-based GUA: 28 undergraduate students, 36 postgraduate students, 45 professionals; recall-based GUA: 13 undergraduate students, 19 postgraduate students, 4 professionals). For both studies, we communicated the research via posting flyers on bulletin boards at various places on the campus, and directly contacted acquaintances of the research team. All recruited participants had no vision problems, or wore glasses, and had no prior experience with GUA.

3.1.3 Password strength metrics. To measure the created graphical passwords' strength, we adopted password guessability. For the recognition-based GUA scheme, we used a brute-force approach by checking all possible combinations of graphical passwords comprising of five unique images starting from the upper left of the image grid and traversing it row by row. For the recall-based GUA scheme, we measured password strength, using a brute-force approach based on the attention points of each background image, as discussed in Sadovnik and Chen [2013], Zhao et al. [2015], and Katsini et al. [2018b]. The brute-force algorithm started from the segments covering the attention points, next, checked the neighbouring segments, and finally checked the rest of the image segments. In both cases, the password strength was measured in number of guesses required to crack a password.

3.1.4 Apparatus. To capture the eye movements, we used Tobii Pro Glasses 2, which captures data at 50Hz. To process the raw data and extract the fixations, we: a) used a customized velocity threshold identification (I-VT) algorithm, with minimum fixation duration set to 80ms, as it is accepted to use fixations shorter than 100ms, when analysing visual scene perception [Velichkovsky et al. 2005]; b) we mapped the fixations on each GUA picture using the mapping function of Tobii Pro Lab; c) we matched each mapped fixation to an AOI (recognition-based: an image-option; recall-based: a segment) using a self-developed Python script. To create their passwords, the study participants used a Samsung Galaxy Tab S2 tablet computer with a 9.7" monitor at a screen resolution of 2048x1536 pixels.

Table 1: Pearson's correlation analysis between the password strength and the gaze-based entropy.

GUA	Participants	Password strength	Gaze entropy
Recognition based	$N = 109$	$m = 10.58, sd = 5.93$ (in billion guesses)	$m = 26.76, sd = 4.24$ (in bits)
	Correlation: $r = .823, p < .001, t_{(107)} = 14.986$		
Recall based	$N = 36$	$m = .187, sd = .094$ (in million guesses)	$m = 54.86, sd = 12.58$ (in bits)
	Correlation: $r = .718, p = .017, t_{(34)} = 6.015$		

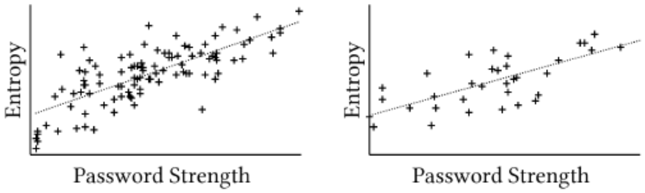

Figure 2: Scatter-plots for the recognition-based (left) and the recall-based (right) GUA scheme.

3.1.5 Experimental design and procedure. Each participant visited our lab at an agreed date and time. The participants were informed about the collected data during the session and provided their consent. To avoid bias effects, they were not given any details on the research objective. The procedure involved the following steps: a) the participants were introduced to the task and familiarized with the eye-tracking equipment. Participants wearing glasses wore the eye-tracking glasses on top of their glasses; b) the eye-tracking calibration process followed; c) the participants created a graphical password using the recognition-based scheme (or the recall-based scheme); d) the participants were distracted for about 20 minutes performing GEFT [Oltman et al. 1971] (a hidden figures activity); e) they used the password they created to log-in and answer a short questionnaire on demographics (we included this step to ensure users did not create the passwords randomly; all participants remembered their passwords); f) an informal discussion on how the participants created their graphical passwords took place.

4 RESULTS AND DISCUSSION

To investigate **H0**$_1$ and **H0**$_2$ we performed Pearson's Product Moment correlation tests, between gaze-based entropy and password strength. Preliminary analyses in both GUA schemes revealed a linear relationship with both variables normally distributed (Shapiro-Wilk's test: $p > .05$), and there were no outliers. The analysis revealed a strong positive correlation between gaze-based entropy and password strength for both the recognition-based ($r = .823, p < .001$) and the recall-based ($r = .718, p = 0.017$) GUA scheme (Table 1; Fig. 2). In both cases, the higher the gaze-based entropy a user has, the stronger graphical password she/he creates. However, a stronger correlation for the recognition-based passwords than the recall-based passwords was revealed, which could be due to the tolerance introduced to the recall-based scheme. An example of low and high entropies is depicted in Fig. 3.

Gaze-based entropy provides an estimation of the users' available choices based on how many AOIs have been explored and for how long, and adapts to GUA policies. Hence, it is a valuable tool for security experts for calculating the practical security of a GUA scheme, which is often essential for comparing the GUA scheme with other authentication schemes (e.g., alphanumeric) and deciding which alternative is a better fit for securing a service. The service providers can leverage the proposed metric to provide adaptive and/or assistive mechanisms, such as the one proposed by Katsini et al. [2018b], to increase the probability that the users will create strong passwords, without intervening in the password creation task. For example, the service provider could set a threshold for the gaze-based entropy which the users must reach before they can start creating their password. This is an unobtrusive way of influencing the users towards better password decisions, compared to the password strength meters that require the user to enter the password and then provide a strength estimation, which may negatively influence the user experience [Ur et al. 2012].

The proposed metric could be used to make the passwords proof to eye-tracking attacks, by guiding users to explore a larger part of the password space. Combining this with other mechanisms (e.g., *draw-the-curtain* effect [Thorpe et al. 2014], gaze-based saliency masks [Katsini et al. 2018b]) could discourage users from selecting identifiable patterns, making the selected passwords to also hold against dictionary attacks. The proposed metric does not hold against capture attacks (e.g., shoulder surfing), but it can be used as part of a multi-factor authentication scheme, where the authentication process not only requires the user to enter the password but the user's visual behaviour is also considered a part of the secret.

To optimise the password strength estimation, other gaze-based metrics could be used complementarily. For example, combining our metric (i.e., how many AOIs are explored and for how long) with Krejtz et al. [2015] entropy (i.e., how attention shifts and is distributed between AOIs) could not only guide users to explore a larger part of the password space but also to distribute their attention more equally among the AOIs. This would provide insights on how people explore the password space and enable the design of appropriate run-time assistive and/or adaptive mechanisms, tailored to the users' characteristics and preferences [Katsini et al. 2018a]. Hence, our future steps include: a) investigating the correlation effect when combined with other gaze-based metrics (e.g., scanpaths [Eraslan et al. 2016b], transition entropy [Krejtz et al. 2015]) aiming to consider them as building factors of an optimized eye-gaze based password strength prediction tool, and b) measuring the effect in other threat models. Both will contribute towards building a more accurate and inclusive real-time gaze-based estimator of the graphical passwords' strength, which could guide the users towards making less predictable graphical passwords.

4.1 Limitations

While we made efforts to maintain our studies' validity, some design aspects of our experimental study introduce limitations. The sample size was rather small, especially for the recall-based scheme, considering that more than 50 participants are typically required to draw clearer conclusions for visual search tasks [Eraslan et al. 2016a]. However, the statistical tests met all the required assumptions. Regarding the approach used to crack the created passwords, it could not be applied to commercial GUA schemes, like Windows Picture Pass, given that they typically allow for a specific number of wrong password guesses (e.g., up to five guesses) before an alternative scheme (e.g., alphanumerical) is required. The guessing algorithm we used was simple, but the aim of the studies was not to create and test another cracking algorithm, but instead, use this as a valid approach for measuring and comparing the strength of a given set of passwords. Despite the limitations, we expect that similar effects will be replicated in the contexts of different GUA schemes, contributing to the external validity of our studies.

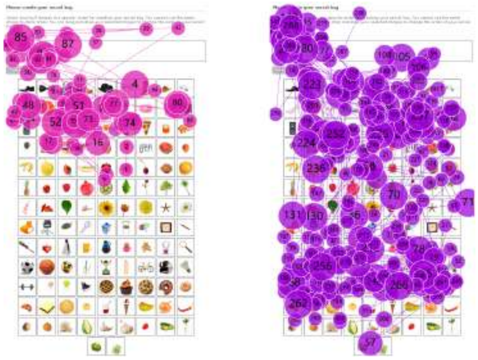

Figure 3: Gaze plots of a user who created a weak password/low entropy (left), and a user who created a strong password /high entropy (right) when using the recognition-based GUA scheme.

5 CONCLUSION

In this paper we introduced *gaze-based entropy*, a new metric for calculating an estimation of the strength of a graphical password based on the eye-gaze behaviour of the user during password composition. To explore the feasibility of the proposed metric, we conducted two studies across two GUA scheme types. Results revealed a strong positive correlation with the password guessability, confirming our assumptions about the association between the strength of the passwords and the user's visual behaviour: the higher the gaze-based entropy, the higher the chance the user will create a strong password. Our metric provides a real-time quantification of the estimated security of a graphical password based on the eye-gaze behaviour during graphical password composition. Estimating the graphical passwords' strength is a challenging research endeavour and this work could be the basis of an adaptive framework in GUA for helping users make more secure password choices.

ACKNOWLEDGMENTS

This research was supported by the General Secretariat for Research and Technology (GSRT) and the Hellenic Foundation for Research and Innovation (H.F.R.I.) - 1st Proclamation of Scholarships for PhD Candidates / Code: 617.

REFERENCES

Marios Belk, Christos Fidas, Panagiotis Germanakos, and George Samaras. 2017. The Interplay Between Humans, Technology and User Authentication: A Cognitive Processing Perspective. *Computers in Human Behavior* 76 (2017), 184 – 200. https://doi.org/10.1016/j.chb.2017.06.042

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, New York, NY, USA, 69–76. https://doi.org/10.1145/2857491.2857527

Robert Biddle, Sonia Chiasson, and Paul C. Van Oorschot. 2012. Graphical Passwords: Learning from the First Twelve Years. *ACM Computing Surveys (CSUR)* 44, 4, Article 19 (Sept. 2012), 41 pages. https://doi.org/10.1145/2333112.2333114

Sacha Brostoff and M. Angela Sasse. 2000. Are Passfaces More Usable Than Passwords? A Field Trial Investigation. In *People and Computers XIV — Usability or Else!*, Sharon McDonald, Yvonne Waern, and Gilbert Cockton (Eds.). Springer London, London, 405–424. https://doi.org/10.1007/978-1-4471-0515-2_27

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, New York, NY, USA, 3011–3020. https://doi.org/10.1145/2207676.2208712

Sonia Chiasson, Elizabet Stobert, Alain Forget, Robert Biddle, and Paul C. Van Oorschot. 2012. Persuasive Cued Click-Points: Design, Implementation, and Evaluation of a Knowledge-Based Authentication Mechanism. *IEEE Transactions on Dependable and Secure Computing* 9, 2 (March 2012), 222–235. https://doi.org/10.1109/TDSC.2011.55

Sonia Chiasson, Paul C. van Oorschot, and Robert Biddle. 2007. Graphical Password Authentication Using Cued Click Points. In *Computer Security – ESORICS 2007*, Joachim Biskup and Javier López (Eds.). Springer Berlin Heidelberg, Berlin, Heidelberg, 359–374. https://doi.org/10.1007/978-3-540-74835-9_24

Rachna Dhamija and Adrian Perrig. 2000. Deja Vu-A User Study: Using Images for Authentication. In *USENIX Security Symposium*, Vol. 9. 4–4.

Ahmet Emir Dirik, Nasir Memon, and Jean-Camille Birget. 2007. Modeling User Choice in the PassPoints Graphical Password Scheme. In *Proceedings of the 3rd Symposium on Usable Privacy and Security (SOUPS '07)*. ACM, New York, NY, USA, 20–28. https://doi.org/10.1145/1280680.1280684

Sukru Eraslan, Yeliz Yesilada, and Simon Harper. 2016a. Eye Tracking Scanpath Analysis on Web Pages: How Many Users?. In *Proceedings of the Ninth Biennial ACM Symposium on Eye Tracking Research & Applications (ETRA '16)*. ACM, New York, NY, USA, 103–110. https://doi.org/10.1145/2857491.2857519

Sukru Eraslan, Yeliz Yesilada, and Simon Harper. 2016b. Scanpath Trend Analysis on Web Pages: Clustering Eye Tracking Scanpaths. *ACM Transactions on the Web (TWEB)* 10, 4, Article 20 (Nov. 2016), 35 pages. https://doi.org/10.1145/2970818

Bogdan Hoanca and Kenrick Mock. 2006. Secure Graphical Password System for High Traffic Public Areas. In *Proceedings of the 2006 Symposium on Eye Tracking Research & Applications (ETRA '06)*. ACM, New York, NY, USA, 35–35. https://doi.org/10.1145/1117309.1117319

David E. Irwin. 2004. Fixation Location and Fixation Duration as Indices of Cognitive Processing. In *The Interface of Language, Vision, and Action: Eye Movements and the Visual World*, John M. Henderson and Fernanda Ferreira (Eds.). Psychology Press, New York, NY, USA, Chapter 3, 105–133.

Christina Katsini, Marios Belk, Christos Fidas, Nikolaos Avouris, and George Samaras. 2016. Security and Usability in Knowledge-based User Authentication: A Review. In *Proceedings of the 20th Pan-Hellenic Conference on Informatics (PCI '16)*. ACM, New York, NY, USA, Article 63, 6 pages. https://doi.org/10.1145/3003733.3003764

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 (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 Security during Picture Password Composition. In *Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems (CHI '18)*. ACM, New York, NY, USA. https://doi.org/10.1145/3173574.3173661

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. https://doi.org/10.1145/2834121

Martin Mihajlov, Borka Jerman-Blažič, and Marko Ilievski. 2011. ImagePass - Designing Graphical Authentication for Security. In *7th International Conference on Next Generation Web Services Practices*. 262–267. https://doi.org/10.1109/NWeSP.2011.6088188

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, New York, NY, USA, 1007–1009. https://doi.org/10.1145/2382196.2382307

Philip K. Oltman, Evelyn Raskin, and Herman A. Witkin. 1971. *Group Embedded Figures Test*. Consulting Psychologists Press Palo Alto, CA.

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. https://doi.org/10.1016/j.ijhcs.2018.02.003

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, New York, NY, USA, 164–173. https://doi.org/10.1145/3079628.3079690

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

Amirali Salehi-Abari, Julie Thorpe, and Paul C. van Oorschot. 2008. On Purely Automated Attacks and Click-Based Graphical Passwords. In *2008 Annual Computer Security Applications Conference (ACSAC)*. 111–120. https://doi.org/10.1109/ACSAC.2008.18

Steven Sinofsky. 2011. Signing in with a Picture Password. (dec 2011). https://blogs.msdn.microsoft.com/b8/2011/12/16/signing-in-with-a-picture-password/

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, New York, NY, USA, 1056–1067. https://doi.org/10.1145/2976749.2978311

Elizabeth Stobert, Alain Forget, Sonia Chiasson, Paul C. van Oorschot, and Robert Biddle. 2010. Exploring Usability Effects of Increasing Security in Click-based Graphical Passwords. In *Proceedings of the 26th Annual Computer Security Applications Conference (ACSAC '10)*. ACM, New York, NY, USA, 79–88. https://doi.org/10.1145/1920261.1920273

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, New York, NY, USA, 2947–2950. https://doi.org/10.1145/2556288.2557212

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. https://www.usenix.org/conference/usenixsecurity12/technical-sessions/presentation/ur

Boris M. Velichkovsky, Markus Joos, Jens R. Helmert, and Sebastian Pannasch. 2005. Two Visual Systems and Their Eye Movements: Evidence from Static and Dynamic Scene Perception. In *Proceedings of the XXVII Annual Conference of the Cognitive Science Society (CogSci 2005)*. Stresa, Italy.

Susan Wiedenbeck, Jim Waters, Jean-Camille Birget, Alex Brodskiy, and Nasir Memon. 2005. PassPoints: Design and Longitudinal Evaluation of a Graphical Password System. *International Journal of Human-Computer Studies* 63, 1 (2005), 102 – 127. https://doi.org/10.1016/j.ijhcs.2005.04.010 HCI research in privacy and security.

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