Does Image Grid Visualization Affect Password Strength and Creation Time in Graphical Authentication?

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

Nowadays, technological advances introduce new visualization and user interaction possibilities. Focusing on the user authentication domain, graphical passwords are considered a better fit for interaction environments which lack a physical keyboard. Nonetheless, the current graphical user authentication schemes are deployed in conventional layouts, which introduce security vulnerabilities associated with the strength of the user selected passwords. Aiming to investigate the effectiveness of advanced visualization layouts in selecting stronger passwords, this paper reports a between-subject study, comparing two different design layouts a two-dimensional and a three dimensional. Results provide evidence that advanced visualization techniques provide a more suitable framework for deploying graphical user authentication schemes and underpin the need for considering such techniques for providing assistive and/or adaptive mechanisms to users aiming to assist them to create stronger graphical passwords.

CCS CONCEPTS

• **Security and privacy → Graphical / visual passwords**; *Human and societal aspects of security and privacy*; • **Human-centered computing → Visualization**; *Visualization techniques*; *Empirical studies in visualization*;

KEYWORDS

Recognition-based graphical authentication; usable security; image grid; graphical passwords; graphical password strength

ACM Reference Format:
Christina Katsini, George E. Raptis, Christos Fidas, and Nikolaos Avouris. 2018. Does Image Grid Visualization Affect Password Strength and Creation Time in Graphical Authentication?. In *AVI '18: 2018 International Conference on Advanced Visual Interfaces, AVI '18, May 29-June 1, 2018, Castiglione della Pescaia, Italy.* ACM, New York, NY, USA, 5 pages. https://doi.org/10.1145/3206505.3206546

AVI '18, May 29-June 1, 2018, Castiglione della Pescaia, Italy

ACM ISBN 978-1-4503-5616-9/18/05…$15.00
https://doi.org/10.1145/3206505.3206546

1 INTRODUCTION

The emergence of new interacting environments, along with the usability and security issues associated with alphanumeric passwords [13], has intensified the research on alternative user authentication schemes (e.g., based on graphical elements and biometrics). Graphical authentication is gaining market share as more and more services provide such schemes as alternatives to alphanumeric-based ones, with Android Patterns and Windows Picture Passwords being two examples which reach out to a large share of the world population. *Graphical User Authentication (GUA)* schemes aim to exploit the picture superiority effect (i.e., people can remember images more easily than words) and are based on two functions of the human memory: recall and recognition.

Recall-based GUA schemes require people to draw a secret on a canvas, with cues (e.g., background images) often being used as a means of remembering the secret. Evaluation of these schemes has revealed that users make predictable choices, as they tend to use weak drawings [7, 20] and draw their passwords on image hot-spots [21]. On the other hand, *recognition-based GUA schemes* require people to select a subset of images from a given set to create a password. Examples of such schemes are PassFaces [3], VIP [5] and ImagePass [16]. The content of the images is correlated to the memorability of the passwords, with single-object images outperforming abstract images and images of faces [15].

Focusing on the recognition-based GUA, one of the main issues raised is the requirement of using a large image pool to achieve entropy (i.e., an estimation of the password strength against brute-force attacks) that is similar to that of alphanumeric-based authentication schemes. The user of a large image pool could lead users to cognitive overload. To tackle this issue, various ways have been used to visualize a set of images more effectively. In PassFaces [3], the images are presented in successive image grids and the users must select an image from each image grid. In VIP10 [5], the users must select four out of ten presented images, while in VIP16 the users must select four out of sixteen images. In DéjàVu [6], the users select a set of images p and to authenticate they are presented with a set of decoy images and a subset m of images from the p set which they must correctly identify. In ImagePass [16], a subset of thirty random images from a large image set is presented to the users and they must select five ordered images to create a password.

Nonetheless, the proposed mechanisms provide theoretical entropies between 12 and 23 bits which is far from the 39 to 53 bits of alphanumeric-based schemes used currently by large service

providers [8]. Belk et. al [2] proposed a GUA scheme consisting of 120 images with an entropy of 34 bits where the users must select five ordered images to create a password. Their recent research revealed that when using a large image pool during password creation the users are overwhelmed, and they not only spend more time to create their password but also they select images located at the top of the image grid. In addition, conventional two-dimensional (2D) interfaces fail to engage users to scan the full image grid when using a large image grid [9].

Considering the difficulties in using a large image grid in recognition-based GUA, we are motivated to exploit the possibilities of a three-dimensional (3D) environment and design a 3D interface which will enable us to provide a large number of images with better spatial distribution (in contrast to a 2D interface), and achieve high entropy without causing high cognitive load to the users. We aim to investigate how a 3D interface could affect the password creation process in terms of *password strength* and *time to create password* and compare the results with that of a conventional 2D interface. Our intention lies in understanding whether and how the difference in the visualization of the GUA scheme affects the users.

2 GUA INTERFACE

To achieve a high theoretical entropy in our GUA scheme, we used a large image pool showing single-objects, as they are more memorable than faces and abstract images [4, 14]. Hence, we designed two recognition-based GUA schemes depicted in Fig. 1, based on the guidelines of well-known recognition-based GUA schemes: PassFaces [3], DéjàVu [6], and ImagePass [16].

Each GUA interface consists of 150 unique images, and they both have the same password policy: the users select five distinct images, in a specific order, to create their password. The theoretical entropy of the GUA is 36.05 bits (Equation 1), which is comparably similar to the entropy of text-based user authentication schemes used by large service providers [8]. The images are presented in the same order both in the registration and the login phase.

$$H_{max} = log_2 \prod_{i=146}^{150} i \quad (1)$$

To design the 2D interface, we adopted the GUA layout proposed in [1]. A total of 150 images of objects are presented in a 10x15 image grid in a single screen in the registration phase (Fig. 1 - top). To design the 3D GUA layout, we divided the 150 images of the 2D interface into subsets of 25 images (Fig. 1 - middle), as 10-36 images have been widely used in image grids of recognition-based GUA schemes [8]. Each section is represented by a side of a polygon 3D shape; thus, the user of the 3D GUA scheme is presented with a total of 150 images of objects distributed on the 6 sides of a polygon on 5x5 image grids (Fig. 1 - bottom). The user can rotate the 3D object clockwise (or counterclockwise) to view the images of the next (or the previous) interface side.

At the top of each layout (either 2D or 3D) a preview of the created password is presented, and the user can drag and drop the images to change their order. The user can also delete an image by using the delete button at the top right corner of each selected image at the preview field.

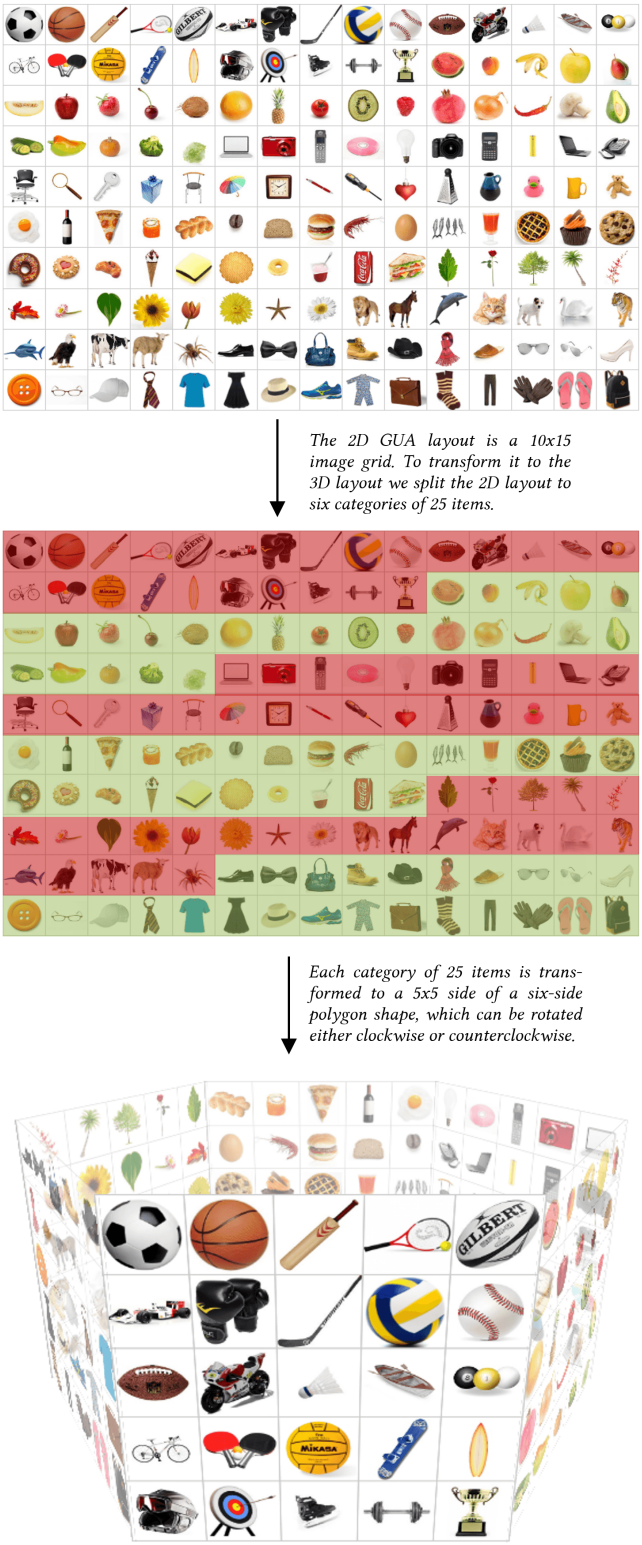

Figure 1: The Graphical User Authentication (GUA) scheme used in our study.

3 EVALUATION STUDY

To evaluate the proposed interface, we designed a between-subject study where users were required to create a graphical password using either the 2D or the 3D GUA interface, following the policy described in Section 2.

3.1 Method

3.1.1 Hypotheses. To investigate our research question, we formed the following null hypotheses:

- **H0**$_1$ There is no significant difference on the password strength between individuals who used the 2D and the 3D interface;
- **H0**$_2$ There is no significant difference on the performance (task completion time) between individuals who used the 2D and the 3D interface.

3.1.2 Participants. A total of 46 individuals (25 females) participated in the study. Their age ranged between 18 and 43 years ($m = 28.3; sd = 5.3$). Participants did not have any vision problems or had corrected to normal vision (i.e., wore glasses or contact lenses). The recruitment took place by communicating the research via social media, mailing lists, posting flyers on bulletin boards at various places on campus, and directly contacting acquaintances of the research team. Participants had varying educational backgrounds (18 undergraduate students, 15 postgraduate students, and 13 professionals). To increase internal validity, we aimed to recruit participants that had no experience with a recognition-based GUA mechanism to avoid any familiarity effects.

3.1.3 Metrics. To measure the created graphical passwords' strength, we adopted password guessability, a widely used metric for measuring password strength. 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 2D interface and traversing it row by row. The password strength was measured in number of guesses required to crack each password. For the 3D interface we used the same brute-force approach to check all possible combinations of graphical passwords comprising of five unique images starting from the top left of the first side and traversing it row by row, then moving to the next side, and so forth.

3.1.4 Procedure. Each participant visited our lab at a previously agreed date and time. The study was conducted in a quiet room and the procedure involved the following steps: first, the participants were informed about the data that would be collected during the session and were asked to provide their consent. They were introduced to the task without revealing any information about the research objective. Given that the participants had no prior experience with GUA schemes, instructions on the authentication policy were provided and the participants were encouraged to ask any questions before proceeding to the password creation.

Next, they were asked to use the touch-screen device (Samsung P1000 Galaxy Tab tablet computer with a 7.0" monitor at a screen resolution of 1024x600 pixels) and create a graphical password, by creating a username in the first step and then by selecting five images in a specific order. The position of each image on the image grid was the same for all participants during the password creation phase. The first 26 participants used the 2D image grid while the next 20 used the 3D image grid. After creating the password, the participants were distracted for 5 minutes with an irrelevant pattern-recognition task and then they were asked to log-in to answer a short questionnaire about demographic information, to ensure that they did not create their password at random. The session was completed with an informal discussion on the password creation strategy adopted by the participants.

3.2 Results

3.2.1 The effect of the interface on the password strength. To investigate **H0**$_1$, we performed an Independent-Samples T-Test, with password strength as the dependent variable, and the GUA visualization interface as the independent variable (2D or 3D). The password strength data was not normally distributed, thus, we transformed them according to Templeton [19] method. After the transformation, the data were normally distributed according to Shapiro-Wilk's test both for the 2D ($p = .381$) and the 3D ($p = .502$) interfaces, and there was homogeneity of variances, as assessed by Levene's test for equality of variances ($p = .087$). Moreover, there were no outliers in the data, as assessed by inspection of the boxplots. The results of the Independent-Samples T-Test revealed that the passwords that were created using the 3D GUA scheme were significantly stronger than the passwords created using the 2D GUA scheme (3D: $m = 19.560, sd = 7.554$; 2D: $m = 8.863, sd = 5.981$; 3D vs 2D: $p = .021, t(44) = 2.396, 95\%CI[1.843, 21.551]$) Therefore, the users who used the tree-dimensional interface created stronger passwords than the users who used the conventional two-dimensional interface. The results are depicted in Fig. 2.

3.2.2 The effect of the interface on the user performance. To investigate **H0**$_2$, we performed an Independent-Samples T-Test, with password composition time as the dependent variable, and the GUA visualization interface as the independent variable (2D or 3D). The password composition times were normally distributed, according to Shapiro-Wilk's test both for the 2D ($p = .171$) and the 3D ($p = .097$) interfaces, and there was homogeneity of variances, as assessed by Levene's test for equality of variances ($p = .441$). Moreover, there were no outliers in the data, as assessed by inspection of the boxplots. The results of the Independent-Samples T-Test revealed that the users who used the 3D interface created their graphical password in less time than the users who used the 2D interface; however, the difference was not statistically significant (3D: $m = 59.810, sd = 30.068$; 2D: $m = 70.117, sd = 36.196$; 3D vs 2D: $p = .324, t(44) = -1.033, 95\%CI[-31.308, 10.580]$). The results are depicted in Fig. 3.

4 DISCUSSION

The results of the study suggest that the visualization of the GUA schemes has an impact on the strength of the graphical passwords. It is possible to influence users towards creating stronger passwords by providing the visual information in smaller chunks and the present study provides evidence that more natural interfaces, such as 3D rotating polygons, enable the users to better process the visual information. As we move towards more natural interfaces (e.g., mixed-reality), where the handling of 3D virtual objects is easier, more efficient, and more precise, the designers of GUA schemes could adopt 3D-based rendering techniques to deploy the GUA

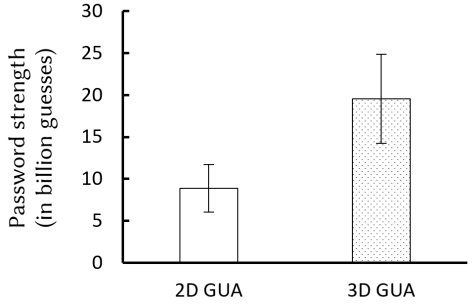

Figure 2: The users who used the 3D GUA layout created significantly stronger passwords than the users who used the 2D GUA layout.

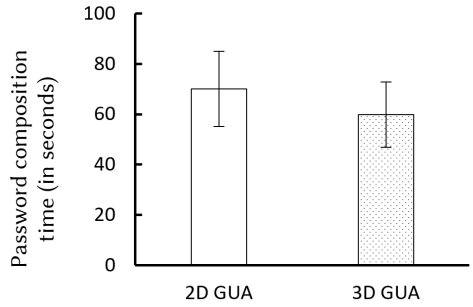

Figure 3: The users who used the 3D GUA layout created their password in less time than the users who used the 2D GUA layout, without the difference being statistically significant.

schemes. Therefore, they would help both the end-users, as they would create stronger passwords, and the service providers, as they would be more resistant to malicious attacks (e.g., off-line attacks), which aim to exploit sensitive user data.

The visualization type (e.g., 2D or 3D) of the image grid of a GUA scheme could be considered as a GUA adaptation factor, along with other factors that influence password strength, such as gender [15], image complexity [22], and individual cognitive differences [11]. These factors are the building blocks of adaptive GUA schemes, aiming to fortify the performance of the authentication process, regarding both security and usability aspects. Such mechanisms act as an assistive medium between the user and the GUA provider, and allow for adapting the characteristics of the GUA scheme when identifying users who are prone to make predictable password choices and help them build stronger passwords. For example, considering that people who face difficulties to identify details in complex visual scenes (i.e., field-dependent) tend to create weak graphical passwords [11] and that eye-tracking can a) infer whether a user is field-dependent during the early stages of the password composition task [10, 18] and b) estimate the password strength [12], the GUA assistive mechanism could adapt accordingly to display the 3D interface to the field-dependent users and help them create stronger passwords. This is important in immersive environments (e.g., Augmented/Mixed/Virtual Reality) where the individual cognitive differences amplify their influence on users' task performance and experience [17].

4.1 Study validity and future work

While we took great efforts to maintain our study validity, some design aspects of our experimental in-lab study introduce limitations. The sample size of our study was rather small, but the performed statistical tests met all the required assumptions. Regarding the approach used to crack the created passwords, it could not be applied to commercial GUAs, given that they typically allow for a specific number of wrong password guesses (e.g., up to five guesses) before an alternative password (e.g., text-based) is required. In addition, the guessing algorithm we used was very simple, but the aim of our study 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 study external validity.

Regarding the future work, further research in 3D interfaces in GUA schemes is required to better understand how people interact with them both during password composition and login tasks. To reveal such interaction patterns, eye-tracking studies can be performed, which could also provide evidence on the weaknesses of the proposed interface and lead to improved design approaches. Hence, our immediate future work consists of a) considering and evaluating other interfaces (e.g., rotating cylinder) as alternatives to current GUA visualization types, b) conducting an eye-tracking study aiming to get a deeper understanding of users' strategy when creating a graphical password and improve the proposed interface, and c) evaluating the proposed interface in immersive environments (e.g., augmented and virtual reality) which are based on natural interaction paradigms (e.g., free gestures to handle 3D objects).

5 CONCLUSION

In summary, we presented the design and evaluation of a 3D interface for the images of a recognition-based graphical user authentication (GUA) scheme. To the best of our knowledge, this is the first attempt of exploiting 3D visualization techniques to improve the visibility of images in recognition-based GUA. The analysis of the created passwords revealed a larger dispersion of selected images in the 3D interface in contrast to the 2D interface. This is translated to a significant difference on the number of required guesses to crack a password between the passwords created using the 3D interface and the passwords created using the 2D interface. Moreover, the users needed less time to navigate through the 3D interface and decide on their password; a difference that was not significant. The findings underpin the necessity of introducing new ways of presenting the information by taking advantage of 3D environments.

ACKNOWLEDGMENTS

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

REFERENCES

[1] 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

[2] Marios Belk, Andreas Pamboris, Christos Fidas, Christina Katsini, Nikolaos Avouris, and George Samaras. 2017. Sweet-spotting Security and Usability for Intelligent Graphical Authentication Mechanisms. In *Proceedings of the International Conference on Web Intelligence (WI '17)*. ACM, New York, NY, USA, 252–259. https://doi.org/10.1145/3106426.3106488

[3] 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

[4] Soumyadeb Chowdhury, Ron Poet, and Lewis Mackenzie. 2013. A Comprehensive Study of the Usability of Multiple Graphical Passwords. In *Human-Computer Interaction – INTERACT 2013*, Paula Kotzé, Gary Marsden, Gitte Lindgaard, Janet Wesson, and Marco Winckler (Eds.). Springer Berlin Heidelberg, Berlin, Heidelberg, 424–441. https://doi.org/10.1007/978-3-642-40477-1_26

[5] Antonella De Angeli, Mike Coutts, Lynne Coventry, Graham I. Johnson, David Cameron, and Martin H. Fischer. 2002. VIP: A Visual Approach to User Authentication. In *Proceedings of the Working Conference on Advanced Visual Interfaces (AVI '02)*. ACM, New York, NY, USA, 316–323. https://doi.org/10.1145/1556262.1556312

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

[7] 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

[8] 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

[9] Christina Katsini, Christos Fidas, Marios Belk, Nikolaos Avouris, and George Samaras. 2017. Influences of Users' Cognitive Strategies on Graphical Password Composition. In *Proceedings of the 2017 CHI Conference Extended Abstracts on Human Factors in Computing Systems (CHI EA '17)*. ACM, New York, NY, USA, 2698–2705. https://doi.org/10.1145/3027063.3053217

[10] 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, New York, NY, USA, 147–152. https://doi.org/10.1145/3172944.3172996

[11] 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, New York, NY, USA, Article 87, 14 pages. https://doi.org/10.1145/3173574.3173661

[12] 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 Tenth Biennial ACM Symposium on Eye Tracking Research & Applications (ETRA '18)*. ACM, New York, NY, USA. https://doi.org/10.1145/3204493.3204589

[13] William Melicher, Darya Kurilova, Sean M. Segreti, Pranshu Kalvani, Richard Shay, Blase Ur, Lujo Bauer, Nicolas Christin, Lorrie Faith Cranor, and Michelle L. Mazurek. 2016. Usability and Security of Text Passwords on Mobile Devices. In *Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems (CHI '16)*. ACM, New York, NY, USA, 527–539. https://doi.org/10.1145/2858036.2858384

[14] Martin Mihajlov and Borka Jerman-Blažič. 2011. On Designing Usable and Secure Recognition-based Graphical Authentication Mechanisms. *Interacting with Computers* 23, 6 (Nov 2011), 582–593. https://doi.org/10.1016/j.intcom.2011.09.001

[15] Martin Mihajlov, Borka Jerman-Blažič, and Anita Ciunova Shuleska. 2016. Why That Picture? Discovering Password Properties in Recognition-Based Graphical Authentication. *International Journal of Human-Computer Interaction* 32, 12 (2016), 975–988. https://doi.org/10.1080/10447318.2016.1220103

[16] 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

[17] 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* (2018). https://doi.org/10.1016/j.ijhcs.2018.02.003

[18] 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

[19] Gary F. Templeton. 2011. A Two-step Approach for Transforming Continuous Variables to Normal: Implications and Recommendations for IS Research. *CAIS* 28, 1 (2011), 41–58. http://aisel.aisnet.org/cais/vol28/iss1/4

[20] Julie Thorpe and Paul C. van Oorschot. 2007. Human-seeded Attacks and Exploiting Hot-spots in Graphical Passwords. In *Proceedings of 16th USENIX Security Symposium on USENIX Security Symposium (SS'07)*. USENIX Association, Berkeley, CA, USA, Article 8, 16 pages. http://dl.acm.org/citation.cfm?id=1362903.1362911

[21] 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 (CCS '13)*. ACM, New York, NY, USA, 161–172. https://doi.org/10.1145/2508859.2516700

[22] 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, New York, NY, USA, 1–12. https://doi.org/10.1145/1073001.1073002