On Cultural-centered Graphical Passwords: Leveraging on Users' Cultural Experiences for Improving Password Memorability

Argyris Constantinides
Department of Computer Science,
University of Cyprus, 1678 Nicosia, Cyprus &
CiTARD Services Ltd., 2064 Nicosia, Cyprus
aconst12@cs.ucy.ac.cy

Marios Belk
Cognitive UX GmbH, 69253 Heidelberg, Germany &
Department of Computer Science,
University of Cyprus, 1678 Nicosia, Cyprus
belk@cognitiveux.de

Christos Fidas
Department of Cultural Heritage Management and New Technologies, University of Patras, 26504 Rio, Greece
fidas@upatras.gr

George Samaras
Department of Computer Science
University of Cyprus, 1678 Nicosia, Cyprus
cssamara@cs.ucy.ac.cy

ABSTRACT

Adaptive user authentication policies are moving in the center of attention lately aiming to assist users in creating memorable and secure passwords. Focusing on graphical user authentication, state-of-the-art research has provided evidence that image-related attributes affect password memorability and security. Nonetheless, the effects of users' contemporary cultural-related memories towards password memorability and security have not been investigated so far, although it is known that user authentication is a cross-cultural task. Aiming to shed light on whether such effects exist, we conducted a study in which users created a graphical password with a contemporary culture-intensive *vs.* a culture-neutral image. Results indicate that image content related to one's cultural-related memories affects the interaction behavior during password composition, and consequently password memorability. Findings point towards a promising new direction for considering human contemporary cultural memories in the design of adaptive password policies to increase memorability and preserve security.

CCS CONCEPTS

• **Human-centered computing** → Human computer interaction → HCI theory, concepts and models; Empirical studies in HCI

KEYWORDS

Cultural-centered Graphical Passwords; Memorability; Security.

ACM Reference format:

A. Constantinides, M. Belk, C. Fidas, G. Samaras. 2018. On Cultural-centered Graphical Passwords: Leveraging on Users' Cultural Experiences for Improving Password Memorability. In *Proceedings of ACM User Modeling, Adaptation and Personalization conference, Singapore, July 2018 (UMAP'18)*, 5 pages. https://doi.org/10.1145/3209219.3209254

UMAP '18, July 8–11, 2018, Singapore, Singapore

ACM ISBN 978-1-4503-5589-6/18/07…$15.00
https://doi.org/10.1145/3209219.3209254

1 INTRODUCTION

User authentication tasks are becoming important from a cultural-centered point of view since these tasks are performed daily by millions of users across diverse cultures which share distinct characteristics and behaviors. Evidence has shown that users across various cultures exhibit different behaviors in security systems [1-7], underpinning the added value of *cultural-centered adaptive security systems*.

Graphical user authentication (GUA) schemes, which ask users to complete an image-based task to login, are increasingly being adopted by researchers and practitioners as they leverage on new interaction design capabilities and adapt to nowadays mobile and immersive user interaction realms [8-10]. Many GUA schemes have been proposed (see [11] for a review) which either require users to sketch a secret pattern on the screen [12], select various positions on a background picture [13], or select pictures on a grid [14, 15].

Two important quality dimensions of an effective GUA scheme are related to its *security* and *usability* aspects. The security level of a graphical password determines its strength against adversary attacks, whereas usability levels are commonly determined by *memorability of selected passwords* [11]. A cornerstone factor that influences both the security and usability of graphical passwords is the background image(s) used [16].

Figure 1: Contemporary culture-intensive image (left) illustrating people in a Greek coffee shop/restaurant *vs.* **culture-neutral image (right)** illustrating people in a Chinese restaurant[1]. We recruited participants that had spent the last 5 years in Greek societies; assuming that they would have had more experience with regional Greek coffee shops' and restaurants' culture, traditions, etc.

From the *security perspective*, studies have shown that the selection of images can be predictable since studies have shown that users prefer clear *vs.* incoherent images [16], and choose images that illustrate people [17, 18], sceneries [17], comics [17]. Furthermore, user choices are influenced by human attributes in an image (*e.g.*, race, age, gender [19]), image colors and type [20]. From the *usability perspective*, studies have shown that the background image attributes of a graphical password have an effect on memorability such as image type (*e.g.*, faces *vs.* abstract images) [15], image properties (*e.g.*, color, shape) [20], image distortion [21, 22], and interference [23]. Finally, the complexity of a background image (*i.e.*, how many attention points it entails) affects password strength and memorability [24-26]. A recent work in [27, 28] revealed that users with different human cognitive attributes follow different patterns of visual behavior and make different selections on images which affect the strength and memorability of graphical passwords.

Research Motivation. The aforementioned research works have provided evidence that several image-related attributes affect memorability and security of selected passwords. However, despite the fact that GUA is a globalized and a cross-cultural task in nearly every interactive system world-wide, *cultural-centered* studies and design issues have not been incorporated in state-of-the-art GUA policies for the benefits of the end-users. In this context, our work focuses on whether, how and why certain images related to the contemporary cultural-related memories of users (*e.g.*, societal habits like going to a coffee shop, going to concerts, etc.) will positively affect the time spent to create a password and subsequently memorability. Doing so, can assist service providers to deliver "best-fit" pictures in GUA schemes by considering intrinsic relationships among users' inter- and intra-cultural differences towards memorability, aiming to drive the *design of cultural-centered adaptive user authentication policies.*

2 METHOD OF STUDY

2.1 Null Hypotheses

***H*$_{01}$.** There is no significant difference in *graphical password creation time* among users that utilize contemporary culture-intensive images *vs.* culture-neutral images[1];

***H*$_{02}$.** There is no significant difference in *memorability* of the user-selected graphical password between users that utilize contemporary culture-intensive images *vs.* culture-neutral images;

***H*$_{03}$.** There is no correlation between the time to create a graphical password and memorability for users that utilize contemporary culture-intensive images *vs.* culture-neutral images;

***H*$_{04}$.** There is no significant difference in *graphical password strength* between users that utilize contemporary culture-intensive images *vs.* culture-neutral images.

2.2 Procedure

We developed a Web-based GUA scheme, similar to Windows™ Picture Gesture Authentication (PGA) [29] in which users draw three gestures (taps, lines and circles) on a background image to create a graphical password. To increase ecological validity, we applied the GUA task within an existing real-life service. To keep the authentication task as a secondary task, users were asked to comment on a blog that first required them to login.

The study was split in two phases. In *Phase A (Day 1)*, participants were introduced to the GUA scheme, completed a questionnaire on demographics and then created and confirmed their graphical password. Users were required to create three gestures on the image which was used as their secret graphical password. Half of the participants received a contemporary

[1] We refer to *culture-intensive images* as images that are relevant to the study participants' own culture (*i.e.*, Greek), and to *culture-neutral images* as images that are not relevant to the study participants' own culture (*i.e.*, China).

culture-intensive image, and the other half a culture-neutral image (Figure 1). We intentionally chose images with a scenery and people since research revealed that users tend to select images illustrating people [17, 25] and scenery [25, 30]. The *culture-intensive image* illustrated a common societal habit of people falling into the age category of our participants and within their cultural context (region they live in). In contrast, the *culture-neutral image* was related to the same societal habit, however in a different socio-cultural context.

Furthermore, given that image complexity affects password strength [26] and gesture combinations [17, 31, 32, 33], we intentionally chose two images of similar complexity (in terms of number of attention points), and examine whether image type during password composition affects the time spent to create the password, and eventually memorability. To control image complexity, we calculated the saliency map and the entropy of several images which is a common measure of image complexity [34], and accordingly used the images depicted in Figure 1.

Following the method in [35], in *Phase B* (performed in *Day 7, 10 and 14*), we sent out emails asking users to access blog posts which required them to login through the GUA scheme.

2.3 Study Variables

Password Creation Time: password creation time was measured from page load (after training) until the user successfully created the graphical password, for attempts that were completed at first trial;

Memorability: we used two metrics as a measure of memorability (following the approach in [35]): *i)* memory time which is the greatest length of time between a password creation and a successful password login using the same graphical password; and *ii)* number of password resets;

Password Strength: we adopted password guessability, a widely used metric for measuring password strength [18, 30]. Following existing approaches in [27, 36, 18, 30], we performed a brute-force attack starting from the segments covering the attention points, then checked the neighboring segments, and finally checked the rest of the segments. The final number of guesses represents the graphical password strength.

2.4 Participants

A total of 61 individuals (18 females) were recruited, ranging in age from 20 to 23 (m=21.13; sd=1.43). Participants are Greek Cypriots living in Nicosia, Cyprus. Participants were split evenly in two groups. The image type (contemporary culture-intensive *vs.* culture-neutral) was randomly varied across all users. To increase internal validity, we recruited individuals with no prior experience with PGA, and participants that had spent the last 5 years in Greek societies; hence we assumed that they would have had experience with Greek regional coffee shops' culture.

2.5 Analysis of Results

In the analyses that follow, data are mean ± standard deviation, unless otherwise stated. There were no significant outliers in the data. Figure 2 depicts a summary of all results.

Password Creation Time Differences. To investigate H_{01}, we ran a Welch t-test since the assumption of homogeneity of variances was violated, as assessed by Levene's test for equality of variances (p=.009). The analysis determined if there were differences in the total time spent to create a graphical password between users that utilized the contemporary culture-intensive image *vs.* those that utilized the culture-neutral image. Creation times for each level of image type were normally distributed, as assessed by Shapiro-Wilk's test (p>.05). Users with the culture-intensive image spent more time to create their graphical password (50.1 ± 23.79) than users with the culture-neutral image (38.06 ± 9.05), a statistically significant difference of 12.03 (95% CI, 955.67 to 23.12), t(29.882)=2.219, p=.034.

Memorability Differences. The maximum memory time that someone could achieve was approximately 336 hours (14 days x 24 hours). To investigate H_{02}, we ran an independent-samples t-test to determine if there were differences in memory time between users that utilized the contemporary culture-intensive image *vs.* those that utilized the culture-neutral image. Memory time for each level of user group was not normally distributed, as assessed by Shapiro-Wilk's test (p<.05). Since the sample sizes in each group are equal, the independent-samples t-test is considered robust under these circumstances. The assumption of homogeneity of variances was violated, as assessed by Levene's test for equality of variances (p<.05). Memory time was significantly longer for culture-intensive users (292.08 ± 27.4) than culture-neutral users (265.4 ± 40.96), a statistically significant difference of 26.68 (95% CI, 8.7 to 44.66), t(50.42)=2.98, p=.004.

As an additional measure of memorability, we recorded the number of password resets per participant. The median number of resets for the culture-intensive group was 0, since most participants did not reset their password, while for the culture-neutral group, the median was 1. A Mann-Whitney U test revealed that the number of resets for the culture-intensive group (6 resets; *mean rank*=36.27) was significantly less than the culture-neutral group (16 resets; *mean rank*=25.9), U=307, z=-2.740, p=.006.

To investigate H_{03}, we ran a Spearman's rank-order correlation to assess the relationship between the time spent to create a graphical password and memorability for both user groups. The analysis showed that there was a positive correlation between time spent to create the password and memorability, rs(61)=.536, p<.001.

Password Strength Differences. To investigate H_{04}, we ran an independent-samples t-test, with the user group (culture-intensive *vs.* culture-neutral) as the independent variable, and the number of guesses needed to crack the password as the dependent variable. The analysis revealed that password strength between the two user groups was not significantly different (t(55.66)=-.266, p=.791); images of the culture-intensive group required 315.08 ± 12.2 million guesses to crack, while images of the culture-neutral group required 324.53 ± 15.2 million guesses to crack.

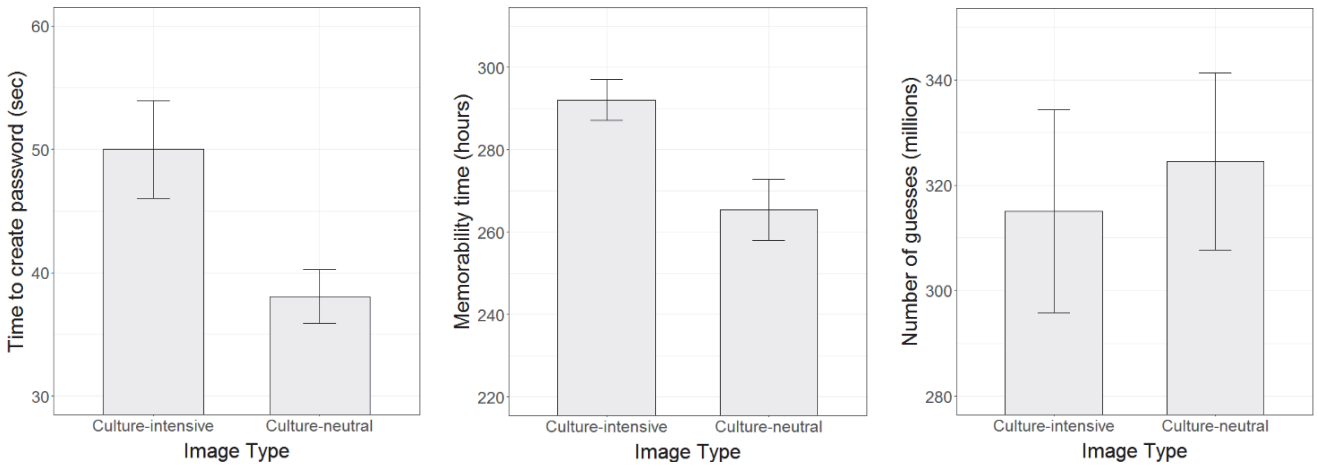

Figure 2: Summary of results; creation time (left), memorability (middle), security (right). Results indicate an increase of time to create the password in the culture-intensive group, which is correlated with memorability, while security was similar across groups.

3 DISCUSSION AND IMPLICATIONS

The results of the study suggest interdependencies between contemporary socio-cultural user memories, the time to create the password and memorability. Hence, it is possible to encourage users towards creating more memorable passwords by providing "best-fit" background images in the graphical password to better process the visual information, and thus trigger deeper information processing and recall. Correlation analyses further indicate that time spent to create the password was positively correlated with memorability, while security analyses showed no significant differences between the groups.

Considering that cultural characteristics (*e.g.*, societal habits, popular culture, etc.) can be assessed easily through explicit user data collection methods (*e.g.*, during user enrolment), studies like the reported one could drive the design of *cultural-centered adaptive and personalized GUA policies and schemes*. Building on our current work [27, 37, 39, 40], which addresses an optimization problem of assigning "best-fit" user authentication mechanisms based on security and usability attributes, the main results of this work could be transformed into specific context-based recommendation rules and be further applied in a procedure for recommending a specific GUA background image type by considering the users' cultural background.

Like structure-based adaptive policies [38], cultural-based adaptive policies could be considered for helping users who share common cultural characteristics to create more memorable graphical passwords. Simple rule-based mechanisms could be elaborated to serve images related to one's cultural attributes aiming to increase memorability. More sophisticated adaptive policies that would automatically evolve over time by taking advantage of the common behavioral patterns of users sharing a common cultural background (*e.g.*, societal habits, nationality) could be based on collaborative filtering mechanisms. These would suggest images that have been successfully used by existing users (in terms of memorability and security) that share common cultural attributes.

4 CONCLUSIONS AND FUTURE WORK

This paper reports results of a two-week user study that aimed to investigate whether memorability of graphical passwords can be increased through the delivery of contemporary culture-intensive images during password composition. Findings provide evidence about the value of considering image context at the intersection of the user's contemporary culture as an important personalization factor which indicates that improves memorability, while it simultaneously preserves security.

Limitations of the study relate to the selection of two specific background images. Although users tend to choose certain images [26], we have selected two representative images of the most widely used image categories (people [17, 25], scenery [25, 30]). Another limitation relates to the fact that participants belonged to the same culture. Nonetheless, to increase internal validity we recruited participants with the same age, contemporary culture, experiences, etc. to investigate how they interact with a contemporary culture-intensive *vs.* a culture-neutral image in relation to their own culture.

Future work entails conducting inter-cultural studies (*e.g.*, Eastern *vs.* Western cultures), studying the interdependency between users' collective past memories and popular culture, and investigating the influence of other cultural differences on GUA memorability and security, such as cognitive differences (holistic *vs.* analytic) [41, 42], visual behavior [43], etc. Given the global and multi-cultural character of user authentication today, we are optimistic that building cultural-centered adaptive GUA policies and schemes could provide a promising new perspective in GUA research to increase memorability and preserve security.

ACKNOWLEDGMENTS

This paper was partially supported by the project ADVisE, in the frame of the University of Cyprus' internal funded research projects, and the project SUCCESS, funded by the EU Active and Assisted Living Programme (AAL-2016-089).

REFERENCES

[1] Wang, Y., Xia, H., & Huang, Y. (2016). Examining American and Chinese Internet Users' Contextual Privacy Preferences of Behavioral Advertising. In *Proceedings of the 19th ACM Conference on Computer-Supported Cooperative Work & Social Computing* (pp. 539-552). ACM

[2] Lin, J., Benisch, M., Sadeh, N., Niu, J., Hong, J., Lu, B., & Guo, S. (2013). A comparative study of location-sharing privacy preferences in the United States and China. *Personal and ubiquitous computing*, *17*(4), 697-711

[3] Wang, Y., Norice, G., & Cranor, L. F. (2011). Who is concerned about what? A study of American, Chinese and Indian users' privacy concerns on social network sites. In *International Conference on Trust and Trustworthy Computing* (pp. 146-153). Springer, Berlin, Heidelberg

[4] Zhao, C., Hinds, P., & Gao, G. (2012). How and to whom people share: the role of culture in self-disclosure in online communities. In *Proceedings of the ACM 2012 conference on Computer Supported Cooperative Work* (pp. 67-76). ACM

[5] Chaudhary, S., Zhao, Y., Berki, E., Valtanen, J., Li, L., Helenius, M., & Mystakidis, S. (2015). A cross-cultural and gender-based perspective for online security: Exploring knowledge, skills and attitudes of higher education students. *IADIS International Journal on WWW/Internet*, *13*(1)

[6] Harbach, M., De Luca, A., Malkin, N., & Egelman, S. (2016). Keep on Lockin'in the Free World: A Multi-National Comparison of Smartphone Locking. In *Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems* (pp. 4823-4827). ACM

[7] Sawaya, Y., Sharif, M., Christin, N., Kubota, A., Nakarai, A., & Yamada, A. (2017). Self-Confidence Trumps Knowledge: A Cross-Cultural Study of Security Behavior. In *Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems* (pp. 2202-2214). ACM

[8] Chiang, H. Y., & Chiasson, S. (2013). Improving user authentication on mobile devices. In *Proceedings of the 15th international conference on Human-computer interaction with mobile devices and services* (pp. 251-260). ACM

[9] Dunphy, P., Heiner, A. P., & Asokan, N. (2010). A closer look at recognition-based graphical passwords on mobile devices. In *Proceedings of the Sixth Symposium on Usable Privacy and Security* (p. 3). ACM

[10] Von Zezschwitz, E., Dunphy, P., & De Luca, A. (2013). Patterns in the wild: a field study of the usability of pattern and pin-based authentication on mobile devices. In *Proceedings of the 15th international conference on Human-computer interaction with mobile devices and services* (pp. 261-270). ACM

[11] Biddle, R., Chiasson, S., & van Oorschot, P. C. (2012). Graphical passwords: Learning from the first twelve years. *ACM Computing Surveys*, *44*(4), 19

[12] Jermyn, I. H., Mayer, A., Monrose, F., Reiter, M. K., & Rubin, A. D. (1999). The design and analysis of graphical passwords. In *Proceedings of the 8th USENIX Security Symposium* (Security '99), USENIX Association

[13] Wiedenbeck, S., Waters, J., Birget, J.C., Brodskiy, A., & Memon, N. (2005). PassPoints: Design and longitudinal evaluation of a graphical password system. *International Journal of Human-Computer Studies*, *63*(1-2), 102-127

[14] Real User Corporation (2004). The Science Behind Passfaces. Technical report.

[15] Mihajlov, M., & Jerman-Blazic, B. (2011). On designing usable and secure recognition-based graphical authentication mechanisms. *Interacting with Computers*, *23*(6), 582-593

[16] Aydın, Ü. A., Acartürk, C., & Çağıltay, K. (2013). The Role of Visual Coherence in Graphical Passwords. In *Proceedings of the Annual Meeting of the Cognitive Science Society*

[17] Alt, F., Schneegass, S., Shirazi, A. S., Hassib, M., & Bulling, A. (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* (pp. 316-322). ACM

[18] Zhao, Z., Ahn, G. J., Seo, J. J., & Hu, H. (2013). On the Security of Picture Gesture Authentication. In *USENIX Security Symposium* (pp. 383-398)

[19] Davis, D., Monrose, F., & Reiter, M. K. (2004). On User Choice in Graphical Password Schemes. In *USENIX Security Symposium* (Vol. 13, pp. 11-11)

[20] Mihajlov, M., Jerman-Blažič, B., & Shuleska, C. A. (2016). Why that picture? discovering password properties in recognition-based graphical authentication. *International Journal of Human–Computer Interaction*, *32*(12), 975-988

[21] Hayashi, E., Dhamija, R., Christin, N., & Perrig, A. (2008). Use your illusion: secure authentication usable anywhere. In *Proceedings of the 4th symposium on Usable privacy and security* (pp. 35-45). ACM

[22] Hayashi, E., Hong, J., & Christin, N. (2011). Security through a different kind of obscurity: Evaluating distortion in graphical authentication schemes. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems* (pp. 2055-2064). ACM

[23] Everitt, K. M., Bragin, T., Fogarty, J., & Kohno, T. (2009). A comprehensive study of frequency, interference, and training of multiple graphical passwords. In Proceedings of the SIGCHI Conference on Human Factors in Computing Systems (pp. 889-898). ACM

[24] Chiasson, S., Biddle, R., & van Oorschot, P. C. (2007). A second look at the usability of click-based graphical passwords. In *Proceedings of the 3rd symposium on Usable privacy and security* (pp. 1-12). ACM

[25] Dunphy, P., & Yan, J. (2007). Do background images improve draw a secret graphical passwords?. In *Proceedings of the 14th ACM conference on Computer and communications security* (pp. 36-47). ACM

[26] Wiedenbeck, S., Waters, J., Birget, J. C., Brodskiy, A., & Memon, N. (2005). Authentication using graphical passwords: Effects of tolerance and image choice. In P*roceedings of the 2005 symposium on Usable privacy and security* (pp. 1-12). ACM

[27] Katsini, C., Fidas, C., Raptis, G. E., Belk, M., Samaras, G., & Avouris, N. (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* (p. 87). ACM

[28] Raptis, G. E., Katsini, C., Belk, M., Fidas, C., Samaras, G., & Avouris, N. (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* (pp. 164-173). ACM

[29] 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

[30] Zhao, Z., Ahn, G. J., & Hu, H. (2015). Picture gesture authentication: Empirical analysis, automated attacks, and scheme evaluation. *ACM Transactions on Information and System Security (TISSEC)*, *17*(4), 14

[31] van Oorschot, P. C., & Thorpe, J. (2011). Exploiting predictability in click-based graphical passwords. *Journal of Computer Security*, *19*(4), 669-702

[32] Zachary Pace (2011). Signing in with a picture password. Retrieved from https://blogs.msdn.microsoft.com/b8/2011/12/16/signing-in-with-a-picture-password

[33] Thorpe, J., & van Oorschot, P. C. (2007). Human-Seeded Attacks and Exploiting Hot-Spots in Graphical Passwords. In *USENIX Security Symposium* (Vol. 8, pp. 1-8)

[34] Perazzi, F., Krähenbühl, P., Pritch, Y., & Hornung, A. (2012). Saliency filters: Contrast based filtering for salient region detection. In *Computer Vision and Pattern Recognition (CVPR), 2012 IEEE Conference on* (pp. 733-740). IEEE

[35] Stobert, E., & Biddle, R. (2013). Memory retrieval and graphical passwords. In *Proceedings of the symposium on usable privacy and security* (p. 15). ACM

[36] Sadovnik, A., & Chen, T. (2013). A visual dictionary attack on Picture Passwords. In *Image Processing (ICIP), 2013 20th IEEE International Conference on* (pp. 4447-4451). IEEE

[37] Belk, M., Fidas, C., Germanakos, P., & Samaras, G. (2017). The interplay between humans, technology and user authentication: A cognitive processing perspective. *Computers in Human Behavior*, *76*, 184-200

[38] Segreti, S.M., Melicher, W., Komanduri, S., Melicher, D., Shay, R., Ur, B., Bauer, L., Christin, N., Cranor, L.F. and Mazurek, M.L. (2017). Diversify to Survive: Making Passwords Stronger with Adaptive Policies. In *Symposium on Usable Privacy and Security (SOUPS)*

[39] Fidas, C., Hussmann, H., Belk, M., & Samaras, G. (2015). iHIP: Towards a user centric individual human interaction proof framework. In *Proceedings of the 33rd Annual ACM Conference Extended Abstracts on Human Factors in Computing Systems* (pp. 2235-2240). ACM

[40] Belk, M., Germanakos, P., Fidas, C., & Samaras, G. (2014). A personalization method based on human factors for improving usability of user authentication tasks. In *Proceedings of the International Conference on User Modeling, Adaptation, and Personalization* (pp. 13-24). Springer

[41] Varnum, M. E., Grossmann, I., Kitayama, S., & Nisbett, R. E. (2010). The origin of cultural differences in cognition: *The social orientation hypothesis. Current directions in psychological science*, *19*(1), 9-13

[42] Engelbrecht, P., & Natzel, S. G. (1997). Cultural variations in cognitive style: Field dependence vs field independence. *School Psychology International*, *18*(2), 155-164

[43] Nisbett, R. E., & Masuda, T. (2003). Culture and point of view. *Proceedings of the National Academy of Sciences*, *100*(19), 11163-11170