Influences of Users' Cognitive Strategies on Graphical Password Composition

Christina Katsini
HCI Group, ECE Department
University of Patras
26504 Rio, Greece
katsinic@upnet.gr

Nikolaos Avouris
HCI Group, ECE Department
University of Patras
26504 Rio, Greece
avouris@upatras.gr

Christos Fidas
Department of Cultural Heritage Management & 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

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

Permission to make digital or hard copies of part or all 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 third-party components of this work must be honored. For all other uses, contact the Owner/Author. Copyright is held by the owner/author(s).
CHI'17 Extended Abstracts, May 06-11, 2017, Denver, CO, USA
ACM 978-1-4503-4656-6/17/05.
http://dx.doi.org/10.1145/3027063.3053217

Abstract
Recent research reveals interaction effects among human cognitive processing factors, interaction device types and user authentication schemes towards security of user created graphical keys. Aiming to investigate how different visual behaviors of individuals with varying cognitive strategies affect the security aspects of graphical user authentication (GUA) across device types, this paper reports preliminary results of a user study (N=51) on graphical password composition using a recognition-based GUA scheme. Results reveal differences on key strength and complexity, as well as on gaze-based entropies between users with different cognitive strategies, which can be used for the design of user-adaptive GUA schemes.

Author Keywords
Usable Security; Human Cognitive Differences; Graphical User Authentication; Eye Tracking.

ACM Classification Keywords
H.5.2 [Information Interfaces and Presentation]: Graphical user interfaces

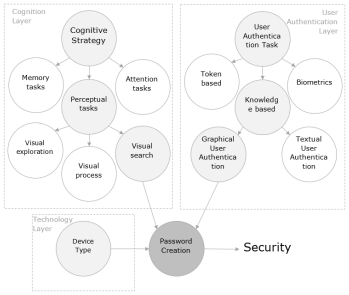

Figure 1. The interplay among human cognitive strategy (*FD-I*), technology factors (*desktop and tablet devices*), and user authentication activity.

Introduction

In the era of mobile, embedded and ubiquitous computing, user authentication remains an important process to ensure that systems and services are accessed by their intended users. Knowledge-based user authentication and particularly textual passwords are currently the most popular authentication schemes [6,10]. However, the application of complex password policies has raised usability and security issues [12], and thus an alternative method, based on graphics, has been proposed; Graphical User Authentication (GUA), which is a widely deployed alternative to textual passwords (e.g., Microsoft Windows Picture Passwords [27]). GUA schemes lie under two major categories: *recall-based* which require users to remember and reproduce a drawing they have drawn before (e.g., DAS [21], Pass-Go [23] and PassPoints [24]); and *recognition-based* which require users to identify and select the target images from a challenge set (e.g., DejaVu [8], PassFaces [5] and ImagePass [15]).

Research on user authentication has become a complex endeavor since it entails several contextual parameters (human and technology specific) that need to be taken into account. From the technology perspective, studies indicate that the device type (e.g., desktop computers, tablets, smart phones) has a main impact on the security aspects of user authentication [26]. From the human perspective, research revealed that individual characteristics of users, such as, users' age [16], gender [7], cognitive disabilities [14], cognitive processing styles and abilities [2,3], affect user authentication performance and preference. From a task execution perspective, research revealed that in decision making tasks, eye movements unfold over the course of the decision process [9], and graphical key creation, as such, is closely related to visual behavior. Thus, it is worth investigating the interplay among human, technology and user authentication activity.

Among a high number of individual characteristics, human cognitive factors, and particularly human cognitive strategies, are considered highly researched and widely applied [1]. A validated and credible cognitive strategy is the *Field Dependence-Independence (FD-I) theory* [25]. FD-I is related to visual search ability as, individuals are classified on their ability to distinguish simple information within complex backgrounds [25], and they are characterized either as *field-dependent (FD)* or *field-independent (FI)*. FD individuals tend to have difficulties on extracting simple information within complex scenes, and follow a more holistic information processing approach, while FI individuals tend to easily separate simple information from complex backgrounds, and are more analytical in information processing tasks [25].

Given that FD and FI individuals differ in terms of visual perceptiveness [11], visual working memory capacity [20] and visual search abilities [1], the motivation of this work lies in increasing our understanding whether and how their differences in visual behavior affect the security aspects of GUA. Therefore, the aim of this work is to investigate the interplay among human cognitive factors (FD-I), technology factors (desktop and table devices), and recognition-based GUA design factors (Figure 1). We consider this as the first step of our greater goal to create user-adaptive GUA schemes that will implicitly elicit the cognitive strategy of the users and assist them in selecting more secure graphical passwords based on their unique individual cognitive strategies.

Figure 2. Graphical user authentication schemes.

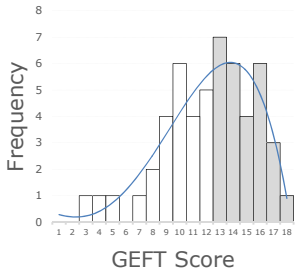

Figure 3. GEFT score normal distribution of participants (Shapiro-Wilk: p=0.156). FIs are highlighted with light-grey color.

Method of Study

Hypotheses

H0₁. there is no significant difference regarding the strength and complexity of the created graphical keys between FD and FI users, by also considering the interaction device type;

H0₂. there is no significant difference regarding the visual search strategy followed for the graphical key creation between FD and FI users, by also considering the interaction device type.

Instruments

HUMAN COGNITIVE FACTOR ELICITATION

Users' field dependence-independence was measured through the Group Embedded Figures Test (GEFT) [18], an accredited and validated paper-and-pencil test [11]. The test measures the user's ability to find common geometric shapes hidden in complex scenes. It consists of 25 items; 7 are used for practice, 18 are used for assessment. Participants are required to identify a given simple figure hidden within a complex pattern by outlining it with a pencil. Based on a widely applied cut-off score [11], participants that solved 11 items or less were classified as FD, whereas participants that solved 12 items and above were classified as FI.

INTERACTION DEVICE TYPES

Two interaction device types were used; *desktop computers* (Intel core i7 with 8GB RAM, 21-inch screen size monitor, Windows 10 operating system, Logitech standard keyboard and mouse) and *tablet touch-based devices* (Samsung P1000 Galaxy). To track users' eye-movements, a *wearable eye tracking device* was used; Tobii Pro Glasses [28] (50 Hz gaze sampling frequency, 4 eye cameras, H.264 1920x1080 pixels at 25 fps).

RECOGNITION-BASED GRAPHICAL AUTHENTICATION SCHEME

A recognition-based GUA scheme was designed and developed following guidelines of well-cited GUA schemes [8,15]. During user enrolment, users created their graphical key by selecting 5 images out of 120 images in a specific order. Each image could only be selected once in a single key. The provided image policy was based on existing approaches and is typical in recognition-based graphical authentication [4,14]. The theoretical entropy of the given policy is 34.41 bits calculated using the following equation [17]:

$$H_{max} = Log_2 K_p \ (1)$$

Participants

We recruited 51 individuals (16 females, 35 males), aged between 18 and 40 (m=29.29, sd=5.76). All participants had prior interaction experience with both device types and none was familiar with any GUA scheme. Based on the users' GEFT scores (Figure 3), 25 participants were classified as FD and 26 participants as FI (m=9.13; sd=3.38; min=3; max=18).

Procedure

The GUA scheme was applied in the frame of an enrolment process of an existing service to increase the ecological validity of the graphical key selection. Guidelines related to the applied policy were provided. Participants first solved the GEFT test and then they enrolled in the service in which they had to create a graphical key. The grid of images was constantly the same for all participants. Half of the participants interacted on a desktop computer and the other half interacted on a mobile touch-based device. The allocation was based on GEFT scores so that the devices were balanced across the FD and FI groups. We

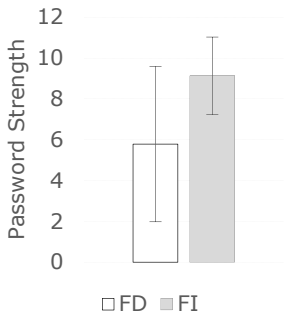

Figure 4. FIs created stronger passwords than FDs (9,124M guesses needed to crack FIs' passwords; 5,781M guesses needed to crack FDs' passwords.

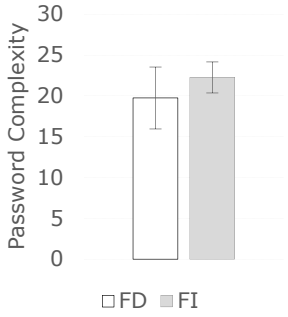

Figure 5. FIs created more complex passwords than FDs (FI: 22.254 ± 1.927; FD: 19.731 ± 3.807) according to Sun et al. [22] equation.

also conducted a qualitative post-study survey asking participants on the strategies they followed during password key creation.

Analysis of results and interpretations

The analysis of the results focuses on understanding the influence of cognitive strategies on the security aspects of graphical password composition. We first report the security analysis of the created passwords, in terms of password strength and complexity as security metrics. Next, we report a gaze-based security analysis, as FDs and FIs differ in terms of visual search behavior, reflecting on the number of items fixated on [19]. Finally, we report a supportive qualitative analysis of the approaches followed by FDs and FIs to create graphical passwords.

Graphical key strength and complexity analysis of the selected keys

To measure the password strength, we used a brute-force approach (i.e., check of all possible password combinations of GUA passwords comprising of five unique images starting from the upper left of the grid and traversing it row by row). The practical strength was measured in terms of number of guesses needed to crack each password. The data were not normally distributed across all independent variables, and thus we performed the non-parametric Independent-Samples Mann-Whitney U Test for each independent variable (cognitive strategy and device type). The Independent-Samples Mann-Whitney U Test met all assumptions and revealed a statistically significant difference in practical password strength between the different cognitive strategies, p=0.038, with a mean password strength 9,124M for FIs and 5,781M for FDs (Figure 4). No effect was revealed for different device types.

To measure the per-user password complexity we used Sun et al.'s equation, as it focuses on graphical user authentication schemes [22]:

$$PS_p = S_p \times \log_2(L_p + I_p + O_p) \quad (2)$$

Where S_p is the length of the graphical key; L_p is the physical length of the key, I_p is the total number of intersections; and O_p is the number of overlaps of the password pattern. The higher the score, the more complex the password is. We performed a two-way ANOVA to examine the effect of cognitive strategy and device type on the per-user password complexities. All assumptions were met (i.e., there were no outliers; PS_p was distributed normally; PS_p variance was homogenous). There was a main effect of cognitive strategy on passwords' complexities across device types (F=5.501, p=0.023, *partial* η^2=0.109), with FIs having created more complex passwords than FDs (*FI*: 22.254 ± 1.927; *FD*: 19.731 ± 3.807), as depicted in Figure 5. No main effect of device type, nor any interaction with cognitive strategy were revealed.

Security analysis based on the eye-movement behavior during key composition

Our gaze-based security analysis is based on the gaze-based key-pool K_p of each participant (i.e., the total images each participant fixated on, rather than the total images of the grid). Based on this, we calculated the gaze-based entropy H_A (i.e., the entropy calculated based on the gaze-based key-pool explained previously) using equation (1). We performed a two-way ANOVA to examine the effect of cognitive strategy

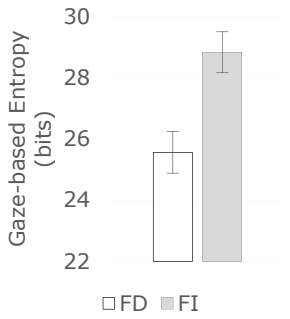

Figure 6. FIs fixated on more images than FDs (FI: 28.83 ± 0.67; FD: 25.56 ± 0.68), and thus they had a greater gaze-based key-pool available.

and device type on the gaze-based entropy. All assumptions were met (i.e., there were no outliers; H_A was distributed normally; H_A variance was homogenous). The gaze-based entropy of FDs and FIs differed significantly, regardless of the device type used (F=11.98, p=0.001, *partial* η^2=0.203). FIs had greater gaze-based entropy than FDs (*FI*: 28.83 ± 0.67; *FD*: 25.56 ± 0.68), as depicted in Figure 6. In particular, FI users fixated on significantly more images than FD users and thus, the entropies indicated that FI users had more chances of creating more secure passwords than FD users since they used a bigger key pool to select their images. No main effect of device type, nor any interaction with cognitive strategy were shown.

Qualitative analysis

To further provide supportive insights for the conclusions drawn from the security analysis we performed a qualitative analysis on the user interviews' data. After completing the task, participants were asked on the strategy they followed to create their graphical passwords. FDs reported creating their authentication keys in a random way based on images that caught their attention or images related to things they like. In addition, quite often they reported of not reading the instructions and being unaware of the GUA policy. As a result, they had difficulties in remembering the selected key when they were asked to login immediately after registering and most FD users answered negatively in the question of whether they would remember their graphical key after one month.

On the other hand, FI users took more time to read the instructions carefully, browse the images and select their authentication keys. Their selection strategy was mainly based on their daily routine and included images related to their hobbies. Others created stories starting with an image they liked and associated the order with the stories they made up. The majority of FIs were positive that they would remember the created keys after one month, and most of them did not face any difficulty with remembering their key when they were asked to login immediately after registration.

Interpretation of results

The analysis of results allows us to draw conclusions in regards to the effect of FD-I during graphical key creation. Security analysis of the selected graphical passwords revealed statistically significant differences in strength and complexity for individuals of different cognitive strategy groups. However, no effect was revealed regarding the device type. Gaze-based security analyses revealed that individuals who follow different cognitive strategies fixated on statistically significant different number of images, which is reflected on the gaze-based entropy. In all cases, FI individuals created more secure passwords than FDs, in terms of password strength, complexity, and gaze-based entropy.

The quantitative findings are related to the qualitative data derived from participants' interviews. FI individuals reported that they selected their passwords on stories they made reflecting their hobbies, daily interests, etc. They tended to look for specific images to fill their stories, following an analytical approach. On the other hand, FD individuals reported that they selected images that caught their attention at first sight, in a random order, without making associations between the selected images. In contrast to FI individuals, FD individuals tended to follow a more holistic approach to create graphical passwords.

Implications for further research

In this paper, we reported an analysis on the security aspects of a recognition-based GUA scheme framed by individual differences in human cognitive strategies. The analysis revealed that FI users created more strong and complex graphical keys and they fixated on more images than FD users. This is related to the differences of the search strategies of the two groups. Replicating this study with recall-based GUA schemes, such as Microsoft Windows Picture Passwords [27], will allow us to further understand the effects of FD-I on GUA schemes. The study should be expanded to include login tasks in the long term to understand any burdens when using GUA schemes and accordingly provide guidelines for design.

Our findings emphasize that people, depending on their cognitive strategy, create less secure keys than others, i.e., FD users follow a more random approach when selecting graphical passwords, while FI users, due to their analytical approach of visual search, scan a bigger part of the image grid to find images that complete the story they use to create their passwords. This behavioral difference necessitates the use of intelligent ways of guiding users to select more secure graphical passwords, by assisting them to scan the entire image grid through adjusting the GUA interface based on the individual cognitive strategies. Such methods would ensure that the practical entropy of the selected graphical passwords would be closer to the theoretical.

Given that this study revealed a main effect of individual cognitive strategies on GUA tasks, a deeper analysis of the eye tracking data could suggest metrics for classifying users based on their cognitive strategy. In particular, these metrics could be used to train machine learning systems and perform implicit elicitation of the users' cognitive strategies based on their eye movement behavior in real time. A user-adaptive system would then provide the most suitable interaction interface for each target group, especially when it comes to the extremes of groups, where holistic or analytical eye-gaze behaviors are expected to be more prominent.

Conclusion

This paper revealed that cognitive strategies of users have a main effect on the generated key strength and complexity of recognition-based GUA schemes. Users' cognitive strategies are reflected on the number of fixated images during key creation with the gaze-based entropy of FIs being significantly greater than the gaze-based entropy of FDs. Bearing in mind that recent research attempts [13] are trying to incorporate novel authentication schemes based on eye tracking methods and users' gaze patterns, studies like the reported one provide valuable insights for further understanding the complexity and interplay among users' high-level cognitive strategies, and eye gaze behavior within graphical authentication tasks. In addition, the study indicates that socio-cognitive theories, like the FD-I theory, can be considered as applicable analysis frameworks which are necessary within nowadays complex computation realms.

Acknowledgements

We would like to thank all the volunteers that took the time to participate in our study.

References

1. Charoula Angeli, Nicos Valanides, and Paul Kirschner. 2009. Field dependence–independence and instructional-design effects on learners' performance with a computer-modeling tool. *Computers in Human Behavior* 25, 6: 1355–1366. http://dx.doi.org/10.1016/j.chb.2009.05.010.
2. Marios Belk, Christos Fidas, Panagiotis Germanakos, and George Samaras. 2013. Security for Diversity: Studying the Effects of Verbal and Imagery Processes on User Authentication Mechanisms. In 442–459. http://dx.doi.org/10.1007/978-3-642-40477-1_27.
3. Marios Belk, Christos Fidas, Panagiotis Germanakos, and George Samaras. 2015. A Personalized User Authentication Approach Based on Individual Differences in Information Processing. *Interacting with Computers* 27, 6: 706–723. http://dx.doi.org/10.1093/iwc/iwu033.
4. Robert Biddle, Sonia Chiasson, and P.C. Van Oorschot. 2012. Graphical passwords. *ACM Computing Surveys* 44, 4: 1–41. http://dx.doi.org/10.1145/2333112.2333114.
5. 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!*. Springer London, London, 405–424. http://dx.doi.org/10.1007/978-1-4471-0515-2_27.
6. Sonia Chiasson, Alain Forget, Elizabeth Stobert, P. C. van Oorschot, and Robert Biddle. 2009. Multiple password interference in text passwords and click-based graphical passwords. *Proceedings of the 16th ACM conference on Computer and communications security - CCS '09*, ACM Press, 500. http://dx.doi.org/10.1145/1653662.1653722.
7. Darren Davis, Fabian Monrose, and Michael K Reiter. 2004. On User Choice in Graphical Password Schemes. *In 13th USENIX Security Symposium*.
8. Rachna Dhamija and Adrian Perrig. 2000. Deja Vu-A User Study: Using Images for Authentication. *USENIX Security Symposium*, 4.
9. Kerstin Gidlöf, Annika Wallin, Richard Dewhurst, and Kenneth Holmqvist. 2013. Using Eye Tracking to Trace a Cognitive Process: Gaze Behaviour During Decision Making in a Natural Environment. *Journal of Eye Movement Research* 6, 1. http://dx.doi.org/dx.doi.org/10.16910/jemr.6.1.3.
10. C. Herley and P. Van Oorschot. 2012. A Research Agenda Acknowledging the Persistence of Passwords. *IEEE Security & Privacy Magazine* 10, 1: 28–36. http://dx.doi.org/10.1109/MSP.2011.150.
11. Jon-Chao Hong, Ming-Yueh Hwang, Ker-Ping Tam, Yi-Hsuan Lai, and Li-Chun Liu. 2012. Effects of cognitive style on digital jigsaw puzzle performance: A GridWare analysis. *Computers in Human Behavior* 28, 3: 920–928. http://dx.doi.org/10.1016/j.chb.2011.12.012.
12. Saranga Komanduri, Richard Shay, Patrick Gage Kelley, et al. 2011. Of passwords and people. *Proceedings of the 2011 annual conference on Human factors in computing systems - CHI '11*, ACM Press, 2595. http://dx.doi.org/10.1145/1978942.1979321.
13. Dachuan Liu, Bo Dong, Xing Gao, and Haining Wang. 2015. Exploiting Eye Tracking for Smartphone Authentication. In *Lecture Notes in Computer Science (LNCS)*. 457–477. http://dx.doi.org/10.1007/978-3-319-28166-7_22.
14. Yao Ma, Jinjuan Feng, Libby Kumin, and Jonathan Lazar. 2013. Investigating User Behavior for Authentication Methods. *ACM Transactions on Accessible Computing* 4, 4: 1–27. http://dx.doi.org/10.1145/2493171.2493173.
15. Martin Mihajlov and Borka Jerman-Blažič. 2011. On designing usable and secure recognition-based graphical authentication mechanisms. *Interacting with Computers* 23, 6: 582–593. http://dx.doi.org/10.1016/j.intcom.2011.09.001.
16. James Nicholson, Lynne Coventry, and Pam Briggs.

2013. Age-related performance issues for PIN and face-based authentication systems. *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems - CHI '13*, ACM Press, 323. http://dx.doi.org/10.1145/2470654.2470701.

17. L. O'Gorman. 2003. Comparing passwords, tokens, and biometrics for user authentication. *Proceedings of the IEEE* 91, 12: 2021–2040. http://dx.doi.org/10.1109/JPROC.2003.819611.

18. Philip K Oltman, Evelyn Raskin, and Herman A Witkin. 1971. *Group embedded figures test*. Consulting Psychologists Press Palo Alto, CA.

19. George E Raptis, Christos A Fidas, and Nikolaos M Avouris. 2016. Using Eye Tracking to Identify Cognitive Differences: A Brief Literature Review. *20th Pan-Hellenic Conference in Informatics*. http://dx.doi.org/10.1145/3003733.3003762.

20. Kent A. Rittschof. 2010. Field dependence–independence as visuospatial and executive functioning in working memory: implications for instructional systems design and research. *Educational Technology Research and Development* 58, 1: 99–114. http://dx.doi.org/10.1007/s11423-008-9093-6.

21. Aviel D Rubin, Ian Jermyn, Alain Mayer, Fabian Monrose, and Michael K Reiter. 1999. The design and analysis of graphical passwords. *8th USENIX Security Symposium*.

22. Chen Sun, Yang Wang, and Jun Zheng. 2014. Dissecting pattern unlock: The effect of pattern strength meter on pattern selection. *Journal of Information Security and Applications* 19, 4–5: 308–320. http://dx.doi.org/10.1016/j.jisa.2014.10.009.

23. Hai Tao and Carlisle Adams. 2008. Pass-Go: A Proposal to Improve the Usability of Graphical Passwords. *IJ Network Security* 7, 2: 273–292. http://dx.doi.org/10.6633/IJNS.200809.7(2).18.

24. 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, 1–2: 102–127. http://dx.doi.org/10.1016/j.ijhcs.2005.04.010.

25. H. A. Witkin, C. A. Moore, D. R. Goodenough, and P. W. Cox. 1975. Field-Dependent and Field-Independent Cognitive Styles and Their Educational Implications. *ETS Research Bulletin Series* 1975, 2: 1–64. http://dx.doi.org/10.1002/j.2333-8504.1975.tb01065.x.

26. Emanuel von Zezschwitz, Alexander De Luca, and Heinrich Hussmann. 2014. Honey, I shrunk the keys. *Proceedings of the 8th Nordic Conference on Human-Computer Interaction Fun, Fast, Foundational - NordiCHI '14*, ACM Press, 461–470. http://dx.doi.org/10.1145/2639189.2639218.

27. Windows 10 sign in options. Retrieved January 11, 2017 from http://www.thewindowsclub.com/windows-10-sign-options.

28. Tobii Pro Glasses 2. Retrieved January 8, 2017 from http://www.tobiipro.com/product-listing/tobii-pro-glasses-2/.