Effects of Human Cognitive Differences on Interaction and Visual Behavior in Graphical User Authentication

Marios Belk, Christos Fidas, Christina Katsini, Nikolaos Avouris, George Samaras

Effects of Human Cognitive Differences on Interaction and Visual Behavior in Graphical User Authentication

Marios Belk[1,4], Christos Fidas[2], Christina Katsini[3], Nikolaos Avouris[3], George Samaras[4]

[1]Cognitive UX GmbH, Heidelberg, Germany
belk@cognitiveux.de
[2]Department of Cultural Heritage Management and New Technologies
University of Patras, Greece
fidas@upatras.gr
[3]HCI Group, Department of Electrical and Computer Engineering
University of Patras, Greece
katsinic@upnet.gr, avouris@upatras.gr
[4]Department of Computer Science, University of Cyprus, Nicosia, Cyprus
cssamara@cs.ucy.ac.cy

Abstract. This paper discusses two user studies to investigate whether human cognitive differences affect user interaction and visual behavior within recognition-based graphical authentication tasks. In order to increase external validity, we conducted the studies with separate user samples. In the first study (N=82) which embraced a longitudinal and ecological valid interaction scenario, we examined whether field dependence-independence (FD-I) differences have an effect on their login performance. During the second study (N=51) which embraced an in-lab eye tracking setup, we investigated whether FD-I differences of participants are reflected on their visual behavior during graphical key creation. Analysis of results revealed interaction effects of users' FD-I differences which indicate that such human cognitive differences should be considered as additional human design factors in graphical user authentication research.

Keywords: Human Cognition, Graphical Passwords, Usability, Eye Tracking.

1 Introduction

Graphical passwords have been proposed as viable alternatives to traditional textual passwords since: *a)* they leverage the picture superiority effect, claiming that pictures are better recalled by the human brain than text information [1, 3]; and *b)* they leverage new interaction design capabilities (*e.g.*, selecting images through finger touch on the screen) [1, 4]. Graphical passwords are now being widely adopted in real-life use, *e.g.*, PassFaces [2], Android Pattern Unlock, and Windows 10 Picture Authentication.

Graphical mechanisms can be classified into three primary categories [2, 11]: *recall-based mechanisms* that require users to memorize and draw a secret pattern [5, 6, 7]; *cued-recall-based mechanisms* that require users to identify particular locations on

an image which serve as cues to assist the recall process [8, 9]; and *recognition-based mechanisms* that require users to create a graphical key by memorizing a set of images, and then recognize those among decoys [2, 4, 10].

Recognition-based mechanisms necessitate from humans to perform visual search and visual memory processing tasks, aiming to view, recognize and recall graphical information. Researchers have examined the effects of various individual differences on graphical passwords such as age, gender and language differences [12], cognitive disabilities [13] and verbal/imager style differences [14, 15]. In addition, given that humans do not embrace similarities in visual search strategies and capacity of visual memory, different studies investigated the effects of human memory on various types of graphical passwords [11], image type (*e.g.*, faces *vs.* single-object images) and grid size in recognition-based graphical passwords [4, 33], usage of multiple graphical passwords [16], frequency and interference [17], and image distortion [18, 19].

Research Motivation. Bearing in mind that recognition-based graphical authentication tasks are in principle cognitive tasks which embrace visual search and visual memory processing of graphical information, we further investigate the effects of individual differences in such tasks by adopting Witkin's *field dependence-independence theory (FD-I)* [20, 21]. The FD-I theory suggests that humans have different habitual approaches, according to contextual and environmental conditions, in retrieving, recalling, processing and storing graphical information [20], and accordingly distinguishes individuals as being field dependent and field independent. *Field dependent (FD) individuals* view the perceptual field as a whole, they are not attentive to detail, and not efficient and effective in situations where they are required to extract relevant information from a complex whole. *Field independent (FI) individuals* view the information presented by their visual field as a collection of parts and tend to experience items as discrete from their backgrounds.

With regards to visual search abilities, evidence has shown that FI individuals are more efficient in tasks that entail visual search than FD individuals since they are more successful in dis-embedding and isolating important information from a complex whole [21, 22]. With regards to visual working memory abilities, research has shown that FI individuals have more enhanced working memory abilities than FD individuals since viewing shapes is primarily a visuospatial function, and the cognitive ability of extracting embedded shapes out of a complex whole involves the use of central executive functions, such as monitoring [23].

To the best of our knowledge, the effects of FD-I towards interaction and visual behavior in recognition-based graphical authentication has not been investigated.

2 Method of Study

2.1 Hypotheses

H1. There are differences in interaction behavior (task efficiency and effectiveness) during graphical login between FD and FI users, by also considering the device type.

H2. There are differences in visual behavior (fixation count and duration) during graphical key selection between FD and FI users, by also considering the device type.

2.2 Research Instruments

Human Cognitive Factor Elicitation Tool. Users' FD-I was measured through the Group Embedded Figures Test (GEFT) [24] which is a widely accredited and validated paper-and-pencil test [21, 22]. The test measures the user's ability to find common geometric shapes in a larger design. The GEFT consists of 25 items; 7 are used for practice, 18 are used for assessment. In each item, a simple geometric figure is hidden within a complex pattern, and participants are required to identify the simple figure by drawing it with a pencil over the complex figure. Based on a widely-applied cut-off score [22], participants that solve 11 items and less are classified as FD, participants that solve 12 items and above are classified as FI.

Eye Tracking Device. A wearable eye tracking device was used; Tobii Pro Glasses 2 [25], which has 4 eye cameras and a 100Hz gaze sampling frequency.

Recognition-based Graphical Authentication Mechanism. A recognition-based graphical authentication mechanism was designed and developed following guidelines of well-cited graphical schemes; Passfaces [2], DejaVu [10] and ImagePass [4]. During user enrolment, users created their authentication key by selecting a fixed number of 5 single-object images out of 120 images in a specific order. The same image could not be selected multiple times in a single key. The provided policy was based on existing approaches and is typical in recognition-based graphical authentication [1, 13].

Interaction Devices. The graphical authentication mechanism was deployed on two types of devices; *desktop computers* (Intel core i7 with 8GB RAM, 21-inch monitor, standard keyboard/mouse) and *mobile touch-based devices* (Samsung P1000 Galaxy, with a 7'' screen size and Apple iPad 3, with a 9.5'' screen size). In both device types, the grid of images was visible in a single screen view without requiring scrolling.

2.3 Procedure

In order to thoroughly investigate the effects of FD-I, we conducted two user studies with separate user samples; Study A investigated FD-I effects on *graphical login performance over time*, and Study B investigated FD-I effects on *visual behavior during graphical password creation*.

Study Design A. The graphical authentication mechanism was applied in the frame of a University laboratory course in which students would authenticate through a login form for accessing their daily course's material (*i.e.*, daily lab exercise). Main aim was to increase ecological validity since students would use the authentication mechanism as part of a real-life laboratory course. The study lasted for four months based

on a between-subjects study design. The first month was dedicated for classifying the participants into FD and FI groups. Several controlled laboratory sessions were conducted in which users solved the GEFT. Then, participants created their graphical key and further interacted with the graphical authentication mechanism to access their course material throughout the semester (three months). Half of the participants interacted on desktop computers and the other half interacted on mobile touch devices. The allocation was based on both FD and FI groups so that the devices were balanced across user groups. To control the frequency of access and prevent user interactions with other types of devices, the users' IP addresses were monitored so that they would access the authentication mechanism only through the devices located at the laboratory room. The users' interactions with the authentication mechanism were recorded for three months (two sessions per week; a maximum twenty-four sessions for each user). Client-side and server-side scripts were developed that measured the total time to login (seconds) for each user session and the number of attempts required to login.

Study Design B. The graphical authentication mechanism was applied in the frame of an enrolment/registration process of a real-life service in order to increase ecological validity. The study was conducted in a quiet room in the lab where each participant was asked to sit in front of a computer at about 40 cm away from the screen. Initially, the participants were introduced to the procedure of the study and familiarized with the eye tracking equipment. Participants wearing glasses were allowed to wear the eye tracking equipment on top of their glasses. Participants first solved the GEFT aiming to classify them into FD and FI groups. Next, participants enrolled in the service in which they had to create a graphical key through the graphical authentication mechanism. The grid of images was constantly the same for all participants. Since the participants were not familiar with recognition-based graphical mechanisms, we provided guidelines related to the applied policy and participants were free to ask any questions before proceeding with the key creation task. Half of the participants interacted on a desktop computer and the other half interacted on a mobile touch device. The allocation was based on both FD and FI groups so that the devices were balanced across groups. Raw eye tracking data were recorded, *i.e.*, fixation count and duration.

2.4 Participants

In Study A, 82 individuals (40 females, 42 males) participated in the study, ranging in age from 18 to 25 (m=20.46; sd=3.82). Based on their scores on the GEFT; 39 participants (47.5%) were FD; 43 participants (52.5%) were FI. In Study B, 51 individuals (16 females, 35 males), ranging in age from 18 to 40 (m=29.29; sd=5.76), participated in the study. Based on the users' scores on the GEFT, 25 participants (49%) were FD; 26 participants (51%) were FI. All participants had prior interaction experience with desktop and mobile devices. No participant was familiar with recognition-based graphical authentication and the GEFT. All participated voluntarily and could opt out any time they wished. To avoid bias, no details were provided about the research.

3 Analysis of Results

3.1 Interaction Behavior Analysis during Graphical Login (H_1)

We compared the *time to login* (task efficiency) and the *number of attempts* (task effectiveness) to successfully login based on 1854 recorded login sessions[1].

Task Efficiency. For time to login, we performed a mixed effects analysis[2]. As fixed effects, we entered the interaction device type (desktop and mobile) into the model, and as random effects, we used subjects to account for non-independence of measures (24 sessions). To account for multiple testing, we adjusted the alpha level with the Dunn-Sidak correction and accordingly report the corrected *p*-values in the analysis[3]. *P*-values were obtained by likelihood ratio tests of the full model with the effect in question against the model without the effect in question [29]. Visual inspection of residual plots revealed that linearity and homoscedasticity were violated. Thus, we performed a log transformation on the dependent variable (time to login), and further inspected residual plots, histograms and Q-Q plots of the residuals, indicating that there were no obvious deviations from linearity, homoscedasticity and normality. In the analyses, we report descriptive statistics and comparisons based on the non-transformed data, whereas significance testing is performed on the transformed data. Figure 1 illustrates the login time per device type across all the sessions of the study.

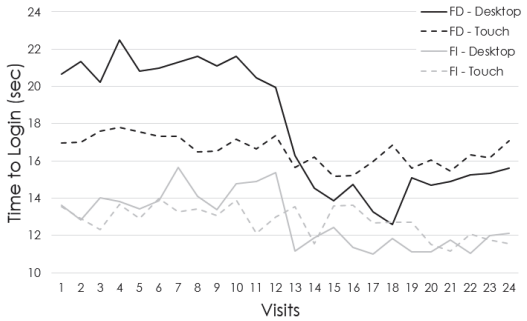

Fig. 1. Login time comparisons between FD and FI users over the three-month study [32].

The analysis revealed that users' FD-I affected the time needed to login ($\chi^2(1)=20.599$, $p<.001$), as FI users were overall significantly faster in completing the login task than FD users. On desktop interactions, FI users were faster than FD users by 5.4 seconds ± 1.01 (standard errors (*SE*)), while on touch interactions, FI users were again faster by 3.74 seconds ± .99. The main effect of device type on time needed to login is not significant, nor is the interaction between FD-I and device. The analysis also revealed a main effect of session trials on the time to successfully login indicating that time to login improves as users gain more experience ($\chi^2(1)=205.36$,

[1] For a more detailed analysis on the users' interactions and feedback, please see [32]
[2] For the analysis, we used *R* [26] with the *lme4 package* [27]
[3] Using the *dunn.test package* in *R* [28]

p<.001). FD users recorded the highest times on both desktop and touch devices throughout the 24 sessions compared to FI users. Nevertheless, while FD users needed more time to login than FI users in the initial sessions, as they gained experience, time difference between FD-FI users notably decreased (Figure 1).

Task Effectiveness. The number of sessions with failed attempts was counted. A session is considered as failed in case the participant needed more than one attempt to successfully login. Over the span of 24 sessions for each user, we entered a flag indicating whether the session was a successful or a failed attempt. We performed a mixed logistic regression with the task effectiveness (successful *vs.* failed) as the dependent variable. The independent variables were used as fixed effects (FD-I, device type), and the subjects as random effects. Among 1854 sessions, 288 attempts failed (15.53% overall error rate). Most failed sessions were caused by FD users (80 failed attempts in desktop and 90 failed attempts in touch devices). FI users recorded 71 failed attempts in desktop and 47 failed attempts in touch devices (Table 1). However, the analysis revealed that these differences were not significant ($\chi^2(1)=5.06$, $p=.17$).

Table 1. Failed attempts (out of 1854 sessions) per FD-I group and device type.

Overall	Desktop-FD	Touch-FD	Desktop-FI	Touch-FI
288	80	90	71	47
Total	**170**		**118**	

3.2 Visual Behavior Analysis during Graphical Key Creation (H_2)

Given that the graphical password creation embraces per se visual search analysis and comprehension, we analyzed the visual behavior of FD-I users, in terms of *fixation count* (the number of times a user looked at a specific image) and *fixation duration* (the number of milliseconds each fixation lasted) for each image in the grid. Accordingly, we analyzed the visual behavior of users: *a)* focusing on all the images of the image grid during key creation; and *b)* on the chosen images of the graphical key.

Cumulative Visual Behavior during Graphical Key Creation. To study the effect of FD-I on visual behavior during graphical key creation, a two-way MANOVA was run with two independent variables (FD-I and device type) and three dependent variables (total fixated images, mean fixation count and mean fixation duration per image). There was a linear relationship between the dependent variables, and no evidence of multicollinearity. There were no univariate and no multivariate outliers in the data. Data were normally distributed. There was homogeneity of covariance matrices and variances. Table 2 shows the cumulative fixation count and duration per group.

Analysis revealed a statistically significant main effect of FD-I on the combined dependent variables ($F(3,45)=4.393$, $p=.009$, *partial* $\eta^2=.227$). Further analysis of the main effects revealed a statistically significant difference between FD-I for desktop interactions on the total fixated images ($F(1,47)=4.728$, $p=.035$, *partial* $\eta^2=.091$), and touch interactions on the total fixated images ($F(1,47)=8.323$, $p=.006$, *partial*

η^2=.150). FI users fixated on significantly more images than FD users. A statistically significant difference between FD-I for desktop interactions on the fixation count was revealed (F(1,47)=4.760, p=.034, *partial* η^2=.092), with FI users having a significantly larger fixation count than FD users. However, the difference was not significant for touch interactions (F(1,47)=.676, p=.415, *partial* η^2=.014). No significant differences were found between FD-I for desktop and touch interactions on fixation duration.

Table 2. Cumulative fixation count and duration per FD-I group and device type.

Median	Desktop-FD	Desktop-FI	Touch-FD	Touch-FI
# of images fixated	40	***56.36***	39	***61.08***
Fixation count	1.50	***2.07***	2.46	2.25
Fixation duration	.41	.55	.61	.58

Visual Behavior per Selected Image of the Graphical Key. We performed a similar analysis as the previous focusing on the fixation count and duration of each image that was selected for the graphical key. All assumptions were met for conducting the test. We run a two-way repeated measures MANOVA test with two independent variables (FD-I and device type), and two dependent variables (fixation count and duration per selected image in the graphical key). Table 3 summarizes the median fixation count and duration of the selected images of the graphical key.

Table 3. Median fixation count and duration for selected images in the graphical key.

Median	Desktop-FD	Desktop-FI	Touch-FD	Touch-FI
Fixation count	2.00	2.16	2.1	2.69
Fixation duration	1.32	1.43	1.58	2.39

There was a statistically significant effect of FD-I on the combined dependent variables (F(4,44)=3.164, *Wilks'* Λ=.777, p=.023), with FI users fixating more time on the selected images than FD users. The interaction effect between FD-I and device type was not statistically significant (F(1,44)=.990, *Wilks'* Λ=.917, p=.083).

4 Discussion of Main Findings

Finding 1 – FD-I differences affect task login efficiency over time in graphical passwords across device types. FI users needed significantly less time to complete the graphical login task compared to FD users over the whole period of the three-month study (supporting H_1). From a theoretical point of view, given that FI users have enhanced analytical abilities and dis-embedding skills, and an enhanced visual working memory in contrast to FD users [23], FI users might have been positively affected in graphical login tasks since the images are processed through the visual working memory sub-system.

Finding 2 – FD-I differences affect task login effectiveness over time in graphical passwords. FI users needed less attempts to complete the graphical login task compared to FD users (supporting H_1). This can be due to the stimuli and interaction

design of the graphical mechanism, *i.e.*, in the case of graphical login, homogeneous objects and structure are illustrated to the users, in which the surrounding framework might dominate the perception of the aiming items. Accordingly, when FD users interact with these stimuli, they might find it difficult to locate the information they are seeking because other information might mask what they are looking for. In contrast, FI users find it easier to recognize and select the essential information from its surrounding field due to improved dis-embedding skills and visual search abilities [21].

Finding 3 – FD-I differences affect visual behavior during graphical password creation. FI users fixated cumulatively on more images across device types, and had a significantly higher fixation count on desktop computers than FD users. In addition, an analysis per selected image has shown that FI users fixated more time on their chosen images than FD users across device types (supporting H_2). Since FI users are analytical and pay attention to details through deeper processing of visual information [20-23], hence they spent more time to process the images in the grid during and prior selection. Such a behavior could have an effect on memorability, in favor of FI users who, as analyzed in Finding 1 and Finding 2, had an increased efficiency and effectiveness in login time and attempts compared to FD users. In addition, FD users fixated on, and selected from a smaller subset of the image grid than FI users, thus affecting practical security entropy of the graphical authentication scheme as shown in [30].

5 Design Implications and Conclusion

The findings underpin the value of considering human cognitive differences as a design factor, in both design and run-time, to avoid deploying graphical authentication schemes that unintentionally favor a specific group based on the designer's decisions.

From a designer's perspective, all findings underpin the value for versatility in the design and development of graphical authentication schemes by taking into account human cognitive differences in information processing. Currently, human cognitive characteristics are not considered as human design factors of graphical user authentication schemes and thus we hope that our work will inspire similar research endeavors (*e.g.*, see the approach discussed in [32] on how human cognitive factors can be incorporated in personalized user authentication schemes). Furthermore, since FI users tend to scan the whole grid of images prior selecting their key, while FD users tend to scan a smaller subset prior selecting their key, an intelligent mechanism could assist FD-I users to reach an improved equilibrium between security and usability, *e.g.*, by illustrating multiple, smaller grids of images to FD users. In addition, low-level eye metrics (fixation count and duration on specific areas of interests) could be used at run-time for user classification and modeling (*e.g.*, [31]), to scaffold users during graphical key creation tasks.

A limitation of the eye tracking study relates to its limited ecological validity which is inherent to the nature of in-lab experiments that was necessary to run the eye tracking setup. Another limitation concerns that only one particular graphical authentication mechanism was investigated although a variety of other genres and mechanisms exist (*e.g.*, Windows 10 Picture Authentication, Android Pattern Unlock, etc.).

References

1. Biddle, R., Chiasson, S., & van Oorschot, P. (2012). Graphical passwords: Learning from the first twelve years. *ACM Computing Surveys, 44*(4), 41 pages.
2. Passfaces Corporation (2009). The Science Behind Passfaces. White paper, http://www.passfaces.com/enterprise/resources/white_papers.htm.
3. Paivio, A., & Csapo, K. (1973). Picture superiority in free recall: Imagery or dual coding? *Cognitive Psychology, 5*(2), 176-206.
4. Mihajlov, M., & Jerman-Blazic, B. (2011). On designing usable and secure recognition-based graphical authentication mechanisms. *Interacting with Computers, 23*(6), 582-593.
5. Jermyn, I., Mayer, A., Monrose, F., Reiter, M., & Rubin, A. (1999). The design and analysis of graphical passwords. In *Proceedings of the USENIX Security Symposium (Security 1999)*, USENIX Association.
6. Gao, H., Guo, X., Chen, X., Wang, L., & Liu, X. (2008). YAGP: Yet Another Graphical Password Strategy. In *Proceedings of the Conference on Computer Security Applications*, IEEE Computer Society, 121-129.
7. Tao, H., & Adams, C. (2008). Pass-Go: A proposal to improve the usability of graphical passwords. *Network Security, 7*(2), 273-292.
8. Wiedenbeck, S., Waters, J., Birget, J., Brodskiy, A., & Memon, N. (2005). Authentication using graphical passwords: Effects of tolerance and image choice. In *Proceedings of the Symposium on Usable Privacy and Security (SOUPS 2005)*, ACM Press, 1-12.
9. Chiasson, S., Forget, A., Biddle, R., & van Oorschot, P. (2008). Influencing users towards better passwords: Persuasive cued click-points. In *Proceedings of the Conference on People and Computers*, British Computer Society, 121-130.
10. Dhamija, R., & Perrig, A. (2000). DejaVu: A user study using images for authentication. In *Proceedings of the USENIX Security Symposium*, USENIX Association.
11. Stobert, E., & Biddle, R. (2013). Memory retrieval and graphical passwords. In *Proceedings of the Symposium on Usable Privacy and Security (SOUPS 2013)*, ACM Press, article 15, 14 pages.
12. Nicholson, J., Coventry, L. & Briggs, P. (2013). Age-related performance issues for PIN and face-based authentication systems. In *Proceedings of Conference on Human Factors in Computing Systems (CHI 2013)*, ACM Press, 323-332.
13. Ma, Y., Feng, J., Kumin, L., & Lazar, J. (2013). Investigating user behavior for authentication methods: A comparison between individuals with Down syndrome and neurotypical users. *ACM Transactions on Accessible Computing, 4*(4), Article 15, 27 pages.
14. Belk, M., Fidas, C., Germanakos, P., & Samaras, G. (2013). Security for diversity: Studying the effects of verbal and imagery processes on user authentication mechanisms. In *Proceedings of the Conference on Human-Computer Interaction (INTERACT 2013)*, Springer-Verlag, 442-459.
15. Belk, M., Fidas, C., Germanakos, P., & Samaras, G. (2015). A personalized user authentication approach based on individual differences in information processing. *Interacting with Computers, 27*(6), Oxford University Press, 706-723.
16. Chowdhury, S., Poet, R., & Mackenzie, L. (2013). A comprehensive study of the usability of multiple graphical passwords. In *Proceedings of the Conference on Human-Computer Interaction (INTERACT 2013)*, Springer-Verlag, 424-441.
17. Everitt, K., Bragin, T., Fogarty, J., & Kohno, T. (2009). A comprehensive study of frequency, interference, and training of multiple graphical passwords. In *Proceedings of the Conference on Human Factors in Computing Systems (CHI 2009)*, ACM Press, 889-898.

18. Hayashi, E., Dhamija, R., Christin, N., & Perrig, A. (2008). Use your illusion: Secure authentication usable anywhere. In *Proceedings of the Symposium on Usable Privacy and Security (SOUPS 2008)*, ACM Press, 35-45.
19. Hayashi, E., Hong, J., & Christin, N. (2011). Security through a different kind of obscurity: Evaluating distortion in graphical authentication schemes. In *Proceedings of the Conference on Human Factors in Computing Systems (CHI 2011)*, ACM Press, 2055-2064.
20. Witkin, H.A., Moore, C.A., Goodenough, D.R., & Cox, P.W. (1977). Field-dependent and field-independent cognitive styles and their educational implications. *Educational Research, 47*(1), 1-64.
21. Angeli, C., Valanides, N., & Kirschner, P. (2009). Field dependence-independence and instructional-design effects on learners' performance with a computer-modeling tool. *Computers in Human Behavior, 25*(6), 1355-1366.
22. Hong, J., Hwang, M., Tam, K., Lai, Y., & Liu, L. (2012). Effects of cognitive style on digital jigsaw puzzle performance: A GridWare analysis. *Computers in Human Behavior, 28*(3), 920-928.
23. Rittschof, K. A. (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.
24. Witkin, H.A., Oltman, P., Raskin, E., & Karp, S. (1971). *A manual for the embedded figures test*. Palo Alto, CA: Consulting Psychologists Press.
25. Tobii Pro Glasses 2. Accessed online September 19, 2016. http://www.tobiipro.com/product-listing/tobii-pro-glasses-2/#Specifications
26. R Core Team (2015). *R: A language and environment for statistical computing*. R Foundation for Statistical Computing, Vienna, Austria. https://www.R-project.org/.
27. Bates, D., Maechler, M., Bolker, B., & Walker, S. (2015). Fitting linear mixed-effects models using lme4. *Journal of Statistical Software, 67*(1), 1-48.
28. Dinno, A. (2015). *dunn.test: Dunn's Test of Multiple Comparisons Using Rank Sums*. R package version 1.3.1. http://CRAN.R-project.org/package=dunn.test
29. Winter, B., & Grawunder, S. (2012). The phonetic profile of Korean formality. *Journal of Phonetics, 40*, 808-815.
30. Katsini, C., Fidas, C., Belk, M., Avouris, N., & Samaras, G. (2017). Influences of users' cognitive strategies on graphical password composition. In *Extended Abstracts of the Conference on Human Factors in Computing Systems (CHI 2017)*, ACM Press, 2698-2705.
31. Raptis, G., 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 Conference on User Modeling, Adaptation and Personalization (UMAP 2017)*, ACM Press (to appear)
32. 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* (to appear)
33. Belk, M., Pamboris, A., Fidas, C., Katsini, C., Avouris, N., & Samaras, G. (2017). Sweet-spotting security and usability for intelligent graphical authentication mechanisms. In *Proceedings of the Conference on Web Intelligence (WI 2017)*, ACM Press (to appear)