Security for Diversity: Studying the Effects of Verbal and Imagery Processes on User Authentication Mechanisms

Marios Belk[1], Christos Fidas[1,2], Panagiotis Germanakos[1,3], George Samaras[1]

[1]Department of Computer Science, University of Cyprus, CY-1678 Nicosia, Cyprus
[2]Interactive Technologies Lab, HCI Group, Electrical and Computer Engineering Department
University of Patras, GR-26504, Patras, Greece
[3]SAP AG, Dietmar-Hopp-Allee 16, 69190 Walldorf, Germany
{belk,christos.fidas,pgerman,cssamara}@cs.ucy.ac.cy

Abstract. Stimulated by a large number of different theories on human cognition, suggesting that individuals have different habitual approaches in retrieving, recalling, processing and storing verbal and graphical information, this paper investigates the effect of such processes with regard to user performance and preference toward two variations of knowledge-based authentication mechanisms. In particular, a text-based password authentication mechanism and a recognition-based graphical authentication mechanism were deployed in the frame of an ecological valid user study, to investigate the effect of specific cognitive factors of users toward efficiency, effectiveness and preference of authentication tasks. A total of 145 users participated during a five-month period between February and June 2012. This recent study provides interesting insights for the design and deployment of adaptive authentication mechanisms based on cognitive factors of users. The results and implications of this paper are valuable in understanding and modeling user interactions with regard to authentication mechanisms.

Keywords: User Authentication, Cognitive Factors, Efficiency, Effectiveness, Preference, Usable Security, Diversity, User Study

1 Introduction

The World Wide Web has become gradually a platform for deployment of complex applications of increased interactivity, as it takes the form of a medium used for complex and important tasks including commercial and governmental transactions, collaborative work, learning and information retrieval. Within this realm, security and privacy issues of interactive systems are considered of paramount importance as it is known that the consequences of a security breach can harm the credibility and legal liability of an organization, decreases users' trust and acceptance, while it exponentially increases maintenance and support costs. In this context, one of the most important and challenging issues is to support users, engaged on tasks related to authentication, through usable computer-human interface designs [1-8].

Nowadays, user authentication over the Internet is achieved primarily with the use of text-based passwords. It is estimated that more than 80% of US and UK companies apply some form of text-based password authentication; in many cases it is their solely method for user authentication [9]. Despite this familiarity factor of users with regard to text-based authentication mechanisms, a considerable amount of research has focused on the design and implementation of graphical authentication schemes. Graphical authentication mechanisms claim to preserve security and improve usability and memorability, as they leverage the vast capacity and capabilities of the human visual memory system [10, 11, 12]. Principally, graphical authentication mechanisms require from a user to enter an authentication key represented by images in a specific sequence. A recent comprehensive review of graphical authentication schemes [13] revealed that numerous ideas have been proposed over the last decade which focus on graphical authentication, and how to address the security and usability issues of text-based passwords, however, few schemes exist that deliver on the original promise of addressing the known problems with text-based passwords since many of the same problems continue to exist. For example, in an early study of Brostoff and Sasse [14], which compared the usability of a text-based password and a recognition-based, graphical authentication mechanism (Passfaces [15]), results demonstrated that although fewer login errors were recorded in graphical authentication than in text-based password interactions, they tended to log in less frequently because the login process was not as efficient as through the text-based password mechanism. A more recent study of Everitt et al. [16] revealed a dramatic decline in memorability and performance when using multiple graphical authentication keys. Also, from a security perspective, the greatest concern of graphical authentication mechanisms is guessing attacks since usable graphical authentication keys usually have a weaker level of security strength than traditional text-based passwords. A study of Stobert et al. [17] indicated that increasing the required authentication key length in graphical authentication mechanisms negatively affects the memorability of the authentication key, and thus, the overall usability of the authentication process.

Graphical authentication schemes can be classified into the following three categories: *Recall-based* authentication mechanisms require that users remember information and reproduce a secret drawing on a static image as their authentication key. Examples include Draw-a-Secret (DAS) [18], its variations [13], YAGP (Yet Another Graphical Password) [19], and Pass-Go [20]. *Cued-recall* authentication mechanisms require users to identify specific locations on a static image and are intended to reduce the memory load on users, since specific cues are utilized in order to assist the recall of information. Examples include PassPoints [21], Persuasive Cued Click Points [22] and gaze-based authentication [23]. *Recognition-based* authentication mechanisms require that users create an authentication key by selecting and memorizing specific images, and then recognize the images among decoys to authenticate. Examples include Passfaces [15], ImagePass [24] and Tiles [25].

A variety of studies have been reported that underpin the necessity for increasing usability of authentication mechanisms [1-8]. The literature reveals many proposals, such as educating and influencing users to create more secure authentication keys [26], improving existing recall-based password approaches with recognition of text

[27], enforcing the creation of secure authentication keys through policies [2, 3], automatically generating secure authentication keys and mnemonic passphrases [28]. Furthermore, password managers [29, 30] have been proposed to minimize users' cognitive load. Nevertheless, ineffective practice of usability in user authentication does not naturally embed the users' characteristics in the design process, and usually adopts a "one-size-fits-all" approach when concerning user authentication designs, ignoring the fact that different users have different characteristics and develop different structural and functional mental models, and thus need individual scaffolding. In this respect, supporting usability of user authentication mechanisms with user-adaptive technologies [31] is based on the promise that understanding and modeling human behavior in terms of structural and functional user requirements related to such security tasks can provide an alternative to the "one-size-fits-all" approach with the aim to improve the system's usability and provide a positive user experience.

Consequently, a first step toward designing an adaptive user authentication mechanism is to identify which individual characteristics (e.g., knowledge, previous experience, lingual characteristics, cognitive characteristics, etc.) are considered important for adapting such mechanisms. Bearing in mind that human computer interactions with regard to authentication mechanisms are in principal cognitive tasks that embrace to recall and/or recognize, process and store information, we argue that these interactions should be analyzed in more detail under the light of cognitive theories. Accordingly, the purpose of this paper is to investigate whether there is an influence of specific individual characteristics of users targeting on cognitive factors, toward efficiency, effectiveness and user preference of authentication mechanisms.

The rest of the paper is structured as follows: next we present the underlying theory of this work. Furthermore, we describe the context of an empirical study, methods, and developed hypotheses. Thereafter, we analyze and discuss our findings. Finally, we summarize our paper and outline the implications of the reported research.

2 Theoretical Background

One of the most widely accepted theory of human cognition is the Dual Coding Theory [32, 33]. It suggests that visual and verbal information is processed and represented differently and along two distinct cognitive sub-systems in the human mind; the visual and verbal cognitive sub-systems. Each sub-system creates separate representations for information processed which are used to organize incoming information that can be acted upon, stored, and retrieved for subsequent use.

Many psychology studies have reported that pictures are better recognized and recalled by the human brain than textual information, referred as the picture superiority effect [34, 35, 36]. Paivio's Dual Coding Theory explains the picture superiority effect that pictures are more perceptually rich than words which lends them an advantage in information processing. The picture superiority effect might be explained by the fact that pictures are mentally represented along with the features being observed, whereas text is visually sparse and represented symbolically, where symbols might have a different meaning depending on the form of the text, which requires an additional processing for the verbal sub-system. For example, 'X' may represent the Roman numeral 10, or the multiplication symbol [13].

The advantage of the picture superiority effect has led to the design of graphical authentication schemes as a viable alternative to text-based authentication mechanisms aiming to increase efficiency and effectiveness of interactions. In graphical authentication mechanisms, human memory is leveraged for visual information in hope of a reduced memory burden that will facilitate the selection and use of more secure authentication keys [13]. Given also that the current user authentication paradigm expands from login on single desktop computers, to login on smart devices, the added difficultly of typing text-based passwords on small screens has amplified the attention to graphical authentication mechanisms as an alternative to traditional text-based password schemes.

However, several research findings claim that the picture superiority effect does not always hold and is affected by various factors [36, 37, 38]. Oates and Reder [37] claim that the picture superiority effect only occurs when a picture affords a meaningful textual label that discriminates it from other pictures. Results of these studies reveal that abstract pictures are not memorable as single words since the visual stimuli is difficult to identify, and hence, a generation of a consistent textual label is not easy or possible. Robertson and Köhler [38] have further provided evidence that the ability to label a picture affects its processing and memory. Another recent study of Mihajlov and Jerman-Blazic [24], that assessed the memorability rates of abstract, face and single-object images in recognition-based, graphical authentication mechanisms, supports that single-object images have the highest memorability rates in graphical authentication mechanisms, since single-object images can be easily labeled (e.g., "picture of a football"), and thus processed and remembered.

As an effort to explain the aforementioned empirically observed differences in users' mental representation and processing of information, many researchers have developed theories of individual differences in *cognitive style* from the perspective of dual coding theory [39], and consequently, argue that individuals have differences in the way they process and remember information. In particular, individuals may process and organize verbal information more efficiently than visual information, whilst others the opposite [39-44]. Within this context, a number of psychometric tests and questionnaires have been developed that elicit verbal-imagery cognitive style, mainly through self-reported experiences and preferences, and response times on verbal vs. visual aptitude tasks (OSIVQ questionnaire: [41]; VICS test: [42]; CSA test [43]; see also [39, 44] for a review on older questionnaires and psychometric tests). Self-reported questionnaires usually ask the participants to rate their preference toward a verbal versus visual mode of processing. Example ratings would be "I have a photographic memory" or "My verbal skills are excellent" [41]. For the reason that questionnaires showed relatively low internal reliability and poor predictive validity [42, 45], objective measures through the development of psychometric tools have emerged, such as response time in solving cognitive tasks that require verbal or visual processing. In particular, psychometric tools have been proposed that typically require from the participant to provide an answer to text-based or image-based statements. Depending on the response time of each answer, the ratio of means or medians between the verbal and visual statements is computed and further used to classify the participant to a particular group; Verbal or Imager group.

To this end, with the aim to investigate the relation among individual differences in cognitive style, and user authentication mechanisms in terms of efficiency, effectiveness and preference, we next describe an empirical study which entailed a psychometric-based survey for extracting users' cognitive styles, combined with a real usage scenario with two variations of user authentication mechanisms; text-based password and recognition-based, graphical authentication mechanism. Such an endeavor is considered valuable as it entails investigating and modeling human behavior in the context of user authentication tasks. Understanding structural and functional user mental models assists the deployment of usable computer-human interaction designs and workflows, whilst minimizing user cognitive loads, perceptual and learning efforts and erroneous interactions with regard to authentication mechanisms

3 Method of Study

3.1 Procedure

A Web-based environment was developed within the frame of various university courses. During each course enrolment process, students were required to create their authentication key that was used for accessing the courses' material (i.e., course slides, homework exercises) and for viewing their grades. The experimental procedure has been divided in three phases:

- **Phase A:** The type of authentication (text-based password or graphical mechanism) was randomly provided during the enrolment process. At the end of the enrollment process the sample was divided of half of the students having enrolled with a text-based password and the other half having enrolled with a graphical authentication mechanism. The users' interactions during this phase were recorded for a period of one and a half month.
- **Phase B:** After Phase A, the system altered the students' authentication type; students that had enrolled with a text-based password in Phase A were prompted to create a new graphical authentication key and vice versa. The new authentication key would be used for the same period as in Phase A (one and half month). The main aim of Phase B was to engage the whole sample on both authentication mechanisms for the same period of time.
- **Phase C:** After Phase B, the system gave the users the option to choose the preferred authentication type to access the system until the end of the study. In particular, the students were first asked to choose between the two variations of authentication (i.e., text-based password or graphical) for which they had already used in Phase A or Phase B during the semester, and then entered the preferred authentication key. Aiming to avoid the effect of users' familiarity with the previously (Phase B) used authentication mechanism, with regard to preference, the system was available for open access during a one month period (without the presence of any

authentication mechanism, the users could download the learning material without to authenticate themselves).

Controlled laboratory sessions were also conducted throughout the period of the study to elicit the users’ cognitive styles through a psychometric test. With the aim to apply the psychometric tests in a scientific right manner, we conducted several sessions with a maximum of five participants by following the protocol suggested by the inventors of the psychometric tests.

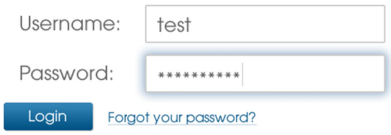
3.2 Users’ Cognitive Style Elicitation

Users’ cognitive styles where elicited by exploiting Riding’s Cognitive Style Analysis test (CSA) [43] since it is considered one of the most credible psychometric tests to elicit cognitive style of users [43, 46]. In particular, we used the CSA test for assessing the Verbal-Imager dimension which indicates an individual‘s tendency to process information verbally or in mental pictures. An individuals’ style on the Verbal-Imager dimension is obtained by presenting a series of 48 questions about conceptual category and appearance (i.e., colour) to be judged by the participants true or false. 24 statements require participants to compare two objects conceptually (e.g., “Are ski and cricket the same type?”, and 24 statements require participants to compare the colour of two objects (e.g., “Are cream and paper the same colour?”).

The psychometric test records the response time of each given answer to the questions and then uses a three-phase algorithm to determine the participant’s cognitive style: i) calculate the average response time on each section (24 questions) of the CSA test, ii) calculate the ratio between the average response times on the verbal (conceptual category) and imagery (appearance) items, and iii) associate the value of each subject’s Verbal-Imager ratio with a style category. A low ratio (<1.02) classifies the participant as a “Verbal”, a high ratio (>=1.02) classifies the participant as an “Imager” [43].

3.3 Authentication Mechanisms used in the Study

One text-based password mechanism and one recognition-based, graphical authentication mechanism were developed. Figure 1 and Figure 2 respectively present the text-based password mechanism and the graphical authentication mechanism used in the study.

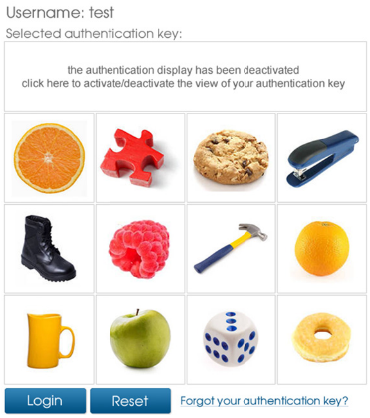


Username: test

Password: **********

Fig. 1. Text-based password mechanism used in the study.

The text-based password mechanism involved alphanumeric and special keyboard characters which could be chosen by the user. A minimum of eight characters including numbers, a mixture of lower- and upper-case letters, and special characters were required to be entered by the users. An additional option for resetting the text-based password was available in case the users forgot their authentication key. In that case, users had to enter their username and a hyperlink was sent to their email that led to a Web-page for resetting their text-based password.



Username: test

Selected authentication key:

the authentication display has been deactivated
click here to activate/deactivate the view of your authentication key

Fig. 2. Graphical authentication mechanism used in the study.

A graphical authentication mechanism that involved single-object images was developed based on the recognition-based, graphical authentication mechanism proposed by Mihajlov and Jerman-Blazic [24]. The choice of this particular graphical authentication mechanism was based on the fact that its theoretical assumption (i.e., single-object images are better memorized and recognized by the human mind) is closely related to the dual coding theory [32, 33], which is considered the basis upon which the Verbal/Imager cognitive styles were developed [39]. During the authentication key creation, users could freely select between eight to twelve images, in a specific sequence out of a random subset of thirty images that were retrieved from a large image database. In case the user was not satisfied with the presented choices, an option to load a different random image subset was available. Repetitions of images were also possible in the sequence (in this case the key length could be longer than twelve images). After the graphical authentication key was created, a fixed image set of sixteen images, containing the user-selected authentication images and system-selected decoy images were permanently attached to the username in order to increase security, since if the decoy images were to change every authentication session, the authentication key could be easily revealed by eliminating the non-repeated images through subsequent sessions [24]. During authentication, a 4 x 4 grid containing the user-selected and system-selected decoy images were presented (Figure 2). The image positions in the selection grid were randomly positioned in each authentication session. Thereafter, users had to select their images in the specific sequence, as entered in the enrolment process in order to get permission for accessing the system. An additional option for resetting the authentication key was also available which was similar to the text-based password reset process.

3.4 Hypotheses

The following hypotheses were formulated for the purpose of our research:

- ***H_1*.** There is general preference of users toward text-based password mechanisms or recognition-based, graphical authentication mechanisms.
- ***H_2*.** Cognitive styles of users have a main effect on users' preference toward text-based password mechanisms or recognition-based, graphical authentication mechanisms.
- ***H_3*.** There is a significant difference with regard to time (efficiency) and total number of attempts (effectiveness) needed to authenticate through a text-based password mechanism or a recognition-based, graphical authentication mechanism among users belonging to the Verbal and Imager class.

3.5 Participants

A total of 145 people participated in the study between February and June 2012. Participants varied from the age of 17 to the age of 26, with a mean age of 22 and were undergraduate students of Computer Science, Electrical Engineering, Psychology and Social Science departments of the University of Cyprus. The participants' native language was Greek, and had learned English as a second language. A total of 2605 authentications have been recorded during the five-month period, with an average of 19.79 (SD 11.62) logins per participant.

3.6 Data Captured

Both client-side and server-side scripts were developed to monitor the users' behaviour during interaction with the authentication mechanisms. The following data was captured:

- **Performance (Efficiency and Effectiveness):** The total time (efficiency) and total number of attempts (effectiveness) required for successful authentication was monitored on the client-side utilizing a browser-based logging facility that started recording time as soon users entered their username for identification, until they successfully completed the authentication process. Additional performance data included total number of authentication key resets.
- **Preference:** The users' choice between the two variations of authentication during the last one and a half month of the study (Phase C) was used to draw conclusions about their preference toward a particular type of authentication.

Complementary self-reporting data for users' performance and preference toward a particular type of authentication was extracted by conducting semi-structured focus group sessions at the end of the study.

3.7 Analysis of Results

For our analysis, we separated users into two categories based on their cognitive style: Verbal (N=68, f=46.89%), and Imagers (N=77, f=53.1%), which consisted of participants that belong to the Verbal and Imager class, respectively.

Efficiency related to User Authentication. A two by two way factorial analysis of variance (ANOVA) was conducted aiming to examine main effects between the users' cognitive style (i.e., Verbal, Imager) and authentication type (i.e., text-based password vs. graphical) on the time needed to accomplish the authentication task. Figure 3 illustrates the means of performance per cognitive style group and authentication type. In addition, Table 1 summarizes the descriptive statistics of each user group (Verbal and Imager) per authentication type (text-based password and graphical).

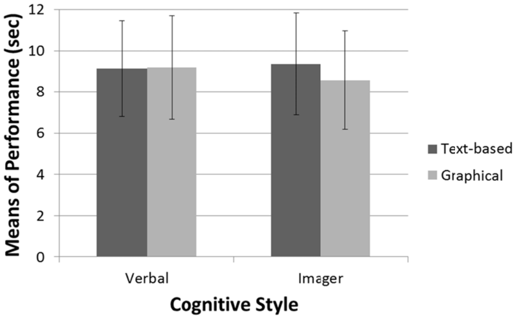


Fig. 3. Means of performance per cognitive style group and authentication type.

The analysis revealed that there is a significant effect on the time needed to accomplish an authentication task with regards to users' cognitive style and authentication type used (F(1,896)=6.635, p=0.01). In particular, users belonging to the Imager class performed faster in graphical authentication than in text-based password authentication mechanisms. In contrast, users belonging to the Verbal class did not perform significantly different in either of the two authentication types (F(1,491)=0.074, p=0.785).

Table 1. Efficiency per cognitive style group and authentication type.

	Verbal		Imager	
	Mean	**Std. Dev.**	**Mean**	**Std. Dev.**
Text-based	9.13	2.31	9.36	2.47
Graphical	9.19	2.50	8.57	2.39

A further comparison between the cognitive style groups revealed that Imagers performed significantly faster in graphical authentication than Verbals (F(1,514)=8.292, p=0.004). However, performance in text-based password mechanisms revealed no significant differences in time since both cognitive style groups performed similarly (F(1,381)=0.838, p=0.361), with Verbals being slightly faster. Given that both types of user groups were more familiar and experienced with text-based passwords, this might explain the fact that no significant differences have been observed in the time to authenticate through the text-based password mechanism. On the other hand, since the familiarity factor has not affected the graphical authentication mechanism, results indicate that the different approach in processing information mentally of each user group (visual approach for Imagers and verbal approach for Verbals) has affected their performance in the graphical authentication mechanism.

Effectiveness related to User Authentication. For each user authentication session, the total number of attempts made for successfully authenticating in each type was recorded. Table 2 summarizes the means of attempts of each user group (Verbal and Imager) per authentication type (text-based password and graphical).

Table 2. Effectiveness per cognitive style group and authentication type.

	Verbal		**Imager**	
	Mean	**Std. Dev.**	**Mean**	**Std. Dev.**
Text-based	1.15	0.40	1.30	0.63
Graphical	1.23	0.50	1.09	0.34

Shapiro-Wilk tests revealed that these distributions do not follow the normal distribution. Regarding the text-based password, although Verbals needed on average less attempts to authenticate, no significant differences were observed between the two user groups, as the Mann-Whitney U test revealed (p=0.183). In the case of graphical authentication, on average, users belonging to the Verbal class needed more attempts to authenticate than the Imager group. The Mann-Whitney U test revealed that the differences between Verbal and Imager user groups were statistically significant (p<0.001). In this respect, Imager users' enhanced ability of processing visual information has positively affected their effectiveness compared to Verbal users. This is further strengthened by the fact that the majority of authentication key resets were initiated by Verbal users for graphical authentication keys. In particular, a total of 7 authentication key resets were initiated by Imagers for graphical authentication mechanisms while in the case of Verbals the number of key resets rose to 24. In case of text-based passwords, a total of 11 password resets were performed; 4 by Imagers and 7 by Verbals.

Preference related to User Authentication. During Phase C, the system provided the option to the users to choose which authentication type to use for accessing the system; either use the current authentication type that was active after Phase B, or use the first authentication type of Phase A. In Table 3 we summarize the users' preferences toward a particular authentication type based on cognitive style. Figure 4 illustrates the total number of authentication sessions in Phase C per cognitive style group.

Table 3. Preference per cognitive style group and authentication type

	Verbal	Imager	Total
Text-based	29	23	52
Graphical	39	54	93
Total	68	77	145

A binomial statistical test was conducted to examine whether there is a general preference relating text-based passwords and graphical authentication mechanisms (H_0: p(text-based password)=0.5 and p(graphical)=0.5). The results revealed that overall, users preferred graphical authentication (p=0.001).

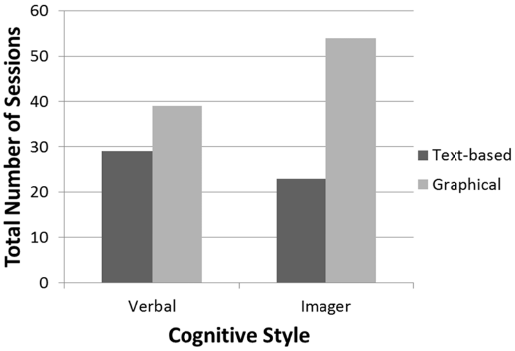


Fig. 4. Users' preference per cognitive style group.

Next, a Pearson's chi-square test was conducted to examine whether there is a relationship between users' cognitive style and their preference toward a specific type of authentication (i.e., text-based password or graphical). The results revealed that in general there is no significant relationship between these two variables (Chi square value=2.563, df=1, p=0.109). Furthermore, examining each cognitive style group individually with respect to preference toward a particular authentication mechanism, it has been identified that users belonging to the Imager class significantly prefer graphical authentication mechanisms (p=0.001). In contrast however, users belonging to the Verbal class do not significantly prefer a particular type of authentication (p=0.275).

3.8 Focus Groups

Semi-structured focus-group sessions were concentrated around the participants' subjective preference and perception of the authentication mechanisms. The question structure of the sessions was focused around the following points: i) which type of authentication the users prefer, ii) which type of authentication was more efficient, iii) which type of authentication was more effective.

The first question for each session was intended to explore the users' preference on authentication mechanisms. The participants were asked to rate their preference toward a particular type of authentication mechanism (text-based password or graphical). A binomial statistical test was conducted to examine whether there is a general preference relating text-based passwords and graphical authentication mechanisms (H_0: p(text-based password)=0.5 and p(graphical)=0.5). The results revealed that overall users preferred graphical authentication (p=0.008) with a total of 89 users preferring graphical authentication mechanisms compared to 56 users who preferred the text-based password mechanism (Table 4).

Table 4. Authentication preference per cognitive style group.

	Verbal	Imager	Total
Text-based	33	23	56
Graphical	35	54	89
Total	68	77	145

A binomial test was conducted separately for each cognitive style group to examine whether a particular cognitive style group prefers specific types of authentication mechanisms. Results revealed that Imagers significantly prefer graphical authentication mechanisms (p=0.001). This supports the aforementioned analysis of results that indicated a significant effect of cognitive style toward preference of authentication mechanisms. In contrast, regarding the Verbal group no clear preference toward text-based passwords or graphical authentication mechanisms was recorded (p=0.904).

As for efficiency and effectiveness of the authentication mechanisms, the participants were asked to rate the efficiency and effectiveness of each mechanism. Table 5 and Table 6 respectively summarize the users' rating regarding efficiency and effectiveness for each authentication type.

Table 5. Authentication efficiency per cognitive style group.

	Verbal	Imager	Total
Text-based	38	33	71
Graphical	30	44	74
Total	68	77	145

A Pearson's chi-square test did not reveal a significant difference in efficiency between the text-based password and graphical authentication mechanism (Chi square value=2.452, df=1, p=0.117). Nevertheless, a noticeable difference in opinions about the efficiency of the two authentication types was observed by participants who belonged to the Verbal class since the majority found the text-based password mechanism more efficient.

Table 6. Authentication effectiveness per cognitive style group.

	Verbal	Imager	Total
Text-based	28	22	50
Graphical	40	55	95
Total	50	95	145

Finally, when asked to rate the difficulty of each authentication type, the majority claimed that graphical authentication mechanisms were easier to recall and recognize the information.

3.9 Validity and Limitations of the Study

With the aim to increase internal validity we recruited a sample of participants that were rather experienced and average than novice users with respect to user authentication and therefore, the research design was setup in order to avoid inference errors. There has also been an effort to increase ecological validity of the research since the user authentication tasks were integrated in a real Web-based system and the participants were involved at their own physical environments without the intervention of any experimental equipment or person. In addition, participants were required to authenticate in the system throughout the semester during real-life tasks (i.e., access their university course's material). Finally, given that future studies will contribute to the external validity of the reported research, we argue that providing personalized user authentication mechanisms, adapted to users' cognitive characteristics, as well as other individual characteristics (e.g., cognitive processing abilities, working memory capacity) could improve the overall user experience with regard to user authentication tasks.

The limitations of the reported study are related to the fact that participants were only university students with an age between 17 to 26 years, and shared common cultural backgrounds. Given that Asian-type alphabets are primarily processed by the visual cognitive sub-system, in contrast to the Western-type alphabets that are primarily processed by the verbal cognitive sub-system [47], cognitive styles might have affected differently the user performance and preference of the authentication mechanisms in case participants had knowledge of non-Western-type languages. In addition, carrying out a single assessment of users' cognitive style might not fully justify the users' classification into specific cognitive-based groups since individuals might be influenced by other circumstances over time such as emotions, urgency, etc. Finally, the results might be affected by the fact that the two types of authentication mechanisms diverge in term of user interface since the text-based password keys are entered through keyboard clicks, while the graphical keys are entered through mouse clicks on the images.

To this end, future studies need to be conducted with a greater sample of varying profiles, cultures and ages, as well as investigate the effect of contextual factors (i.e., user device) in combination with cognitive styles of users in order to reach to more concrete conclusions about the effect of individuals' cognitive style on their performance and preference related to authentication mechanisms. In addition, considering that in real life, users have to memorize multiple authentication keys [16], another important aspect for investigation is to study the effect of cognitive styles on user performance and preference when using multiple text-based password and graphical authentication mechanisms over time.

4 Conclusions

The purpose of this paper is to present results of an ecological valid user study which was designed with the aim to investigate whether there is a main effect of specific individual characteristics of users targeting on cognitive styles, towards performance and preference of two complementary types of user authentication mechanisms (text-based and graphical). Such an endeavor is considered valuable for the design and the deployment of more usable computer-human interaction processes with the aim to offer personalized and adaptive authentication mechanisms aiming to assist users to accomplish efficiently and effectively comprehensive and usable authentication tasks. For the purpose of this research we have designed a three phase experimental study which entailed a credible psychometric-based test for eliciting users' cognitive style based on the dual coding theory that suggests two sub-cognitive systems for processing and representing verbal and visual information in parallel threads.

The results of this paper can be interpreted under the light of this theory as they demonstrate a main effect of cognitive styles on both performance and preference related to authentication mechanisms. Regarding performance, results revealed that users of the Imager class performed faster in graphical authentication than in text-based password authentication, whereas users of the Verbal class did not authenticate significantly faster in either of the two authentication types. Furthermore, Imagers performed significantly faster in graphical authentication than Verbals did, however in the case of text-based passwords performance of both cognitive style groups was not considerably different, with Verbals being slightly faster than Imagers. An interpretation of this result can be based on the fact that all users were more familiar and experienced interacting with text-based passwords, hence no significant difference was observed between the Verbal and the Imager. On the other hand, since the familiarity factor did not affect the graphical authentication mechanism, we have observed that the visual approach of processing and organizing information of the Imagers has positively affected their performance compared to the Verbals.

Regarding effectiveness (i.e., total number of attempts), we conclude that both authentication mechanisms were effective in use throughout the study. Nevertheless, both number of attempts and number of authentication key resets reveal that graphical authentication mechanisms have positively affected user belonging to the Imager class as they needed significantly less attempts and key resets in graphical authentication mechanisms compared to Verbal users.

Finally, participants in general preferred graphical authentication mechanisms. Results also demonstrate that users categorized in the Imager group significantly prefer graphical authentication mechanisms. A possible interpretation of this result might be based on the novelty effect of graphical authentication. However, results suggest that if this would be the main factor that influences users' preference then it would be observed across all user groups regardless their cognitive style, which in the current sample is not the case, since users categorized into the Verbal group did not significantly prefer a particular authentication type.

Based on the presented results which embrace objective quantitative data (captured data during experimentations) as well as subjective qualitative self-reporting data (focus group studies), we argue that following a user-centered design methodology, it is necessary that designers of authentication mechanisms should clearly bear in mind individual differences of users while interacting with the system. Currently, there is a strong underlying design assumption that text-based passwords are the most comprehensive way for user authentication [48]. The results of this study suggest enhancing current authentication mechanisms aiming to embrace both text-based and recognition-based, graphical authentication mechanisms. As the results suggest, such an approach would have many positive implications from a usability and user experience point of view since, recommending authentication mechanisms, personalized to the users’ cognitive style (especially in the case of Imagers, as results indicate) would increase the users’ memorability and information processing efficiency of the authentication key, and thus improve task completion efficiency and effectiveness, and user satisfaction. At the same time, graphical authentication mechanisms provide similar security protection levels as text-based passwords from a service provider point of view, taking into consideration that they are encrypted properly on the service provider database layer and submitted securely on the transmission layer [24, 13]. On the other hand, from a user’s point of view, they entail similar threats as text-based authentication mechanisms with regard to guessing (e.g., brute-force attacks) or capturing attacks (e.g. shoulder surfing, malware, phishing attacks, etc.) [24].

A practical implication of this work could be either to allow a user to explicitly declare the preferred authentication mechanism or by implicitly recommend the “best-fit” authentication mechanism based on historical usage data of the user in regard with efficiency and effectiveness of authentication tasks, or based on user interactions with a psychometric-based, cognitive style elicitation test. A more sophisticated architecture solution could be based on a recommendation engine as part of an adaptive system specialized on user authentication tasks aiming to extract from interaction data, the individuals’ characteristics by use of statistical means.

Studies like the reported one can be useful for improving usable security on the World Wide Web through adaptivity in user interface designs with regard to authentication mechanisms, aiming to organize and present information and functionalities related with security tasks in an adaptive format to diverse user groups, by using different levels of abstractions through appropriate interaction styles, terminology, information presentation and user modeling techniques.

Acknowledgements. We would like to thank all the participants of the study for their time and qualitative feedback in the frame of the focus group sessions. The work is co-funded by the PersonaWeb project under the Cyprus Research Promotion Foundation (ΤΠΕ/ΠΛΗΡΟ/0311(ΒΙΕ)/10), and the EU projects Co-LIVING (60-61700-98-009) and SocialRobot (285870).

5 References

1. Shay, R., Kelley, P., Komanduri, S., Mazurek, M., Ur, B., Vidas, T., Bauer, L., Christin, N., Cranor, L.: Correct Horse Battery Staple: Exploring the Usability of System-assigned Passphrases. In: ACM Symposium on Usable Privacy and Security, Article 7, 20 pages. ACM Press, New York, NY (2012)
2. Komanduri, S., Shay, R., Kelley, P., Mazurek, M., Bauer, L., Christin, N., Cranor, L., Egelman, S.: Of Passwords and People: Measuring the Effect of Password-composition Policies. In: ACM International Conference on Human Factors in Computing Systems, pp. 2595-2604, ACM Press, New York, NY (2011)
3. Inglesant, P., Sasse A.: The True Cost of Unusable Password Policies: Password use in the Wild. In: ACM International Conference on Human Factors in Computing Systems, pp. 383-392. ACM Press, New York, NY (2010)
4. Florencio, D., Herley, C.A.: Large-scale Study of Web Password Habits. In: ACM International Conference on World Wide Web, pp. 657-666. ACM Press, New York, NY (2007)
5. Adams, A., Sasse, A.: Users are not the Enemy: Why Users Compromise Security Mechanisms and How to Take Remedial Measures. J. Communications of the ACM 42(12), 40-46 (1999)
6. Shay, R., Komanduri, S., Kelley, P., Leon, P., Mazurek, M., Bauer, L., Christin, N., Cranor, L.: Encountering Stronger Password Requirements: User Attitudes and Behaviors. In: ACM Symposium on Usable Privacy and Security, Article 2, 20 pages. ACM Press, New York, NY (2010)
7. Bonneau, J., Herley, C., van Oorschot, P., Stajano, F.: The Quest to Replace Passwords: A Framework for Comparative Evaluation of Web Authentication Schemes. In: IEEE Symposium on Security and Privacy, pp. 553-567, IEEE Computer Society, Washington, DC (2012)
8. LeBlanc, D., Forget, A., Biddle, R.: Guessing Click-based Graphical Passwords by Eye Tracking. In: IEEE International Conference on Privacy, Security and Trust, pp. 197-204. IEEE Computer Society, Washington, DC (2010)
9. Zhang, J., Luo, X., Akkaladevi, S., Ziegelmayer, J.: Improving Multiple-password Recall: An Empirical Study. J. Information Security 18(2), 165-176 (2009)
10. Angeli, A.D., Coventry, L., Johnson, G., Renaud, K.: Is a Picture Really Worth a Thousand Words? Exploring the Feasibility of Graphical Authentication Systems. J. Human-Computer Studies 63(1-2), 128-152 (2005)
11. Everitt, K.M., Bragin, T., Fogarty, J., Kohno, T.A.: Comprehensive Study of Frequency, Interference, and Training of Multiple Graphical Passwords. In: ACM International Conference on Human Factors in Computing Systems, pp. 889-898. ACM Press, New York, NY (2009)
12. Tullis, T.S., Tedesco, D.P., McCaffrey, K.E.: Can Users Remember their Pictorial Passwords Six Years Later. In: ACM International Conference on Human Factors in Computing Systems, pp. 1789-1794. ACM Press, New York, NY (2011)

13. Biddle, R., Chiasson, S., van Oorschot, P.: Graphical Passwords: Learning from the First Twelve Years. J. ACM Computing Surveys 44(4), 41 pages (2012)
14. Brostoff, S., Sasse, M.A.: Are Passfaces More Usable than Passwords: A Field Trial Investigation. In: BCS International Conference on People and Computers, pp. 405-410, British Computer Society, UK (2000)
15. Passfaces Corporation. The science behind Passfaces, `http://www.passfaces.com/enterprise/resources/whitepapers.htm`
16. Everitt, K., Bragin, T., Fogarty, J., Kohno, T.: A Comprehensive Study of Frequency, Interference, and Training of Multiple Graphical Passwords. In: ACM International Conference on Human Factors in Computing Systems, pp. 889-898. ACM Press, New York, NY (2009)
17. Stobert, E., Forget, A., Chiasson, S. van Oorschot, P., Biddle, R.: Exploring Usability Effects of Increasing Security in Click-based Graphical Passwords. In: ACM International Conference on Computer Security Applications Conference, pp. 79-88. ACM Press, New York, NY (2010)
18. Jermyn, I., Mayer, A., Monrose, F., Reiter, M., Rubin, A.: The Design and Analysis of Graphical Passwords. In: USENIX Security Symposium, pp. 1-1. USENIX Association, Berkley, CS (1999)
19. Gao H., Guo X., Chen X., Wang L., Liu X. YAGP: Yet Another Graphical Password Strategy. In: IEEE International Conference on Computer Security Applications, pp. 121-129. IEEE Computer Society, Washington, DC (2008)
20. Tao, H., Adams, C.: Pass-Go: A Proposal to Improve the Usability of Graphical Passwords. J. Network Security 7(2), pp. 273-292 (2008)
21. Wiedenbeck, S., Waters, J., Birget, J., Brodskiy, A., Memon, N.: Authentication Using Graphical Passwords: Effects of Tolerance and Image Choice. In: ACM Symposium on Usable Privacy and Security, pp. 1-12. ACM Press, New York, NY (2005)
22. Chiasson, S., Forget, A., Biddle, R., van Oorschot, P.: Influencing Users Towards Better Passwords: Persuasive Cued Click-Points. In: BCS International Conference on People and Computers, pp. 121-130. British Computer Society, UK (2008)
23. Bulling A., Alt F., Schmidt A.: Increasing the Security of Gaze-based Cued-recall Graphical Passwords using Saliency Masks. In: ACM International Conference on Human Factors in Computing Systems, pp. 3011-3020. ACM Press, New York, NY (2012)
24. Mihajlov, M., Jerman-Blazic, B.: On Designing Usable and Secure Recognition-based Graphical Authentication Mechanisms. J. Interacting with Computers 23(6), 582-593 (2011)
25. Nicholson, J., Dunphy, P., Coventry, L., Briggs, P., Olivier, P.A.: Security Assessment of Tiles: a New Portfolio-based Graphical Authentication System. In: ACM International Conference on Human Factors in Computing Systems (Ext. Abstracts), pp. 1967-1972. ACM Press, New York, NY (2012)
26. Forget, A., Chiasson, S., van Oorschot, P., Biddle, R.: Improving Text Passwords Through Persuasion. In: ACM International Symposium on Usable Privacy and Security, pp. 1-12. ACM Press, New York, NY (2008)
27. Wright, N., Patrick, A., Biddle, R.: Do You See Your Password?: Applying Recognition to Textual Passwords. In: ACM International Symposium on Usable Privacy and Security, Article 8, 14 pages. ACM Press, New York, NY (2012)
28. Kuo, C., Romanosky, S., Cranor, L.: Human Selection of Mnemonic Phrase-based Passwords. In: ACM International Symposium on Usable Privacy and Security, pp. 67-78. ACM Press, New York, NY (2006)

29. Halderman, J.A., Waters, B., Felten, E.: Convenient Method for Securely Managing Passwords. In: ACM International Conference on World Wide Web, pp. 471-479. ACM Press, New York, NY (2005)
30. Chiasson, S., van Oorschot, P.C., Biddle, R.A.: Usability Study and Critique of Two Password Managers. In: USENIX Security Symposium, pp. 1-16. USENIX Association, Berkley, CA (2006)
31. Brusilovsky, P., Kobsa, A., Nejdl, W.: The Adaptive Web: Methods and Strategies of Web Personalization. Springer, Heidelberg (2007)
32. Paivio, A.: Mind and Its Evolution: A Dual Coding Theoretical Approach. Lawrence, Erlbaum, Mahwah, NJ (2006)
33. Paivio, A., Csapo, K.: Picture Superiority in Free Recall: Imagery or Dual Coding? J. Cognitive Psychology 5(2), 176-206 (1973)
34. Anderson, J.R.: Cognitive Psychology and its Implications: Seventh Edition. Worth Publishers, NY (2009)
35. Ally, B.A., Budson, A.E.: The Worth of Pictures: Using High Density Event Related Potentials to Understand the Memorial Power of Pictures and the Dynamics of Recognition Memory. J. NeuroImage 35, 378-395 (2007)
36. Brady, T.F., Konkle, T., Alvarez, G.A., Oliva, A.: Visual Long-term Memory has a Massive Storage Capacity for Object Details. J. National Academy of Sciences 105(38), 14325-14329 (2008)
37. Oates, J.M., Reder, L.M.: Memory for Pictures: Sometimes a Picture is not Worth a Single Word. Successful Remembering and Successful Forgetting: A Festschrift in Honor of Robert A. Bjork. J. Psychological Press, 447-462 (2010)
38. Robertson, E.K., Köhler, S.: Insights from Child Development on the Relationship between Episodic and Semantic Memory. J. Neuropsychologia 45(14), 3178-3189 (2007)
39. Riding, R., Cheema, I.: Cognitive Styles – An Overview and Integration. J. Educational Psychology 11(3-4), 193-215 (1991)
40. Peterson, E., Rayner, S., Armstrong, S.: Researching the Psychology of Cognitive Style and Learning Style: Is There Really a Future?. J. Learning and Individual Differences 19(4), 518-523 (2009)
41. Blazhenkova, O., Kozhevnikov, M.: The New Object-Spatial-Verbal Cognitive Style Model: Theory and Measurement. J. Applied Cognitive Psychology 23(5), 638-663 (2009)
42. Peterson, E., Deary, I., Austin, E.: A New Reliable Measure of Verbal-Imagery Cognitive Style. J. Personality and Individual Differences 38, 1269-1281 (2005)
43. Riding, R.: Cognitive Styles Analysis. Learning and Training Technology, Birmingham, UK (2001)
44. Kozhevnikov, M.: Cognitive Styles in the Context of Modern Psychology: Toward an Integrated Framework of Cognitive Style. J. Psychological Bulletin 133(3), 464-481 (2007)
45. McAvinue, L.P., Robertson, I.H.: Measuring Visual Imagery Ability: A Review. J. Imagination, Cognition and Personality 26, 191-211 (2007)
46. Kinley, K., Tjondronegoro, D., Partridge, H.: Web Searching Interaction Model based on User Cognitive Styles. In: ACM International Conference of SIGCHI Australia on Computer-Human Interaction, pp. 340-343. ACM Press, New York, NY (2010)
47. Tavassoli, N.: Temporal and Associative Memory in Chinese and English. J. Consumer Research 26(2), 170-181 (1999)
48. Herley, C., van Oorschot, P.: A Research Agenda Acknowledging the Persistence of Passwords. J. Security and Privacy 10(1), 28-36 (2012)