Interacting with Computers Advance Access published September 6, 2014

doi:10.1093/iwc/iwu033

A Personalized User Authentication Approach Based on Individual Differences in Information Processing

MARIOS BELK[1,*], CHRISTOS FIDAS[2,3], PANAGIOTIS GERMANAKOS[1,4] AND GEORGE SAMARAS[1]

[1]*Department of Computer Science, University of Cyprus, P.O. Box 20537, 1678 Nicosia, Cyprus*
[2]*Department of Cultural Heritage Management and New Technologies, University of Patras, Patras, Greece*
[3]*Interactive Technologies Lab, HCI Group, University of Patras, Patras, Greece*
[4]*SAP UX – Research, Methods & Communication, SAP AG, Walldorf, Germany*
[*]*Corresponding author: belk@cs.ucy.ac.cy*

An effective user authentication mechanism should embrace both security and usability aspects as its purpose is to ensure safety of operation of online services but as well usability and transparency to its end users. In an attempt to improve the usability and overall experience of user interactions during authentication, this paper proposes an alternative approach of personalizing user authentication tasks based on individual differences in cognitive processing. The presented approach is mainly driven by theories on individual differences in cognitive styles which argue that individuals recall and process textual and graphical information differently. In this realm, the paper presents a 4-month user study in which 153 participants interacted with a personalized user authentication mechanism in an ecological valid context. Analysis of results shows that the presented user authentication approach is a promising alternative to current state of user authentication practices.

RESEARCH HIGHLIGHTS

- We propose an alternative approach of personalizing user authentication tasks based on individual differences in cognitive styles.
- We investigate whether matching the user authentication type to users' cognitive styles has a significant effect on task efficiency and effectiveness.
- We investigate the differences between textual and graphical authentication mechanisms in terms of efficiency, effectiveness and user preference, among users with different cognitive styles.
- Personalizing the user authentication type to users' cognitive styles improves task efficiency and effectiveness.
- Cognitive styles have an effect on users' preference and performance of user authentication tasks.
- Personalizing user authentication tasks based on individual differences in cognitive processing could be a viable alternative to current state of user authentication practices.

Keywords: adaptation and personalization; authentication; user-centred design; user characteristics; user studies

Editorial Board Member: Fabio Paternò

Received 12 March 2014; Revised 11 July 2014; Accepted 31 July 2014

1. INTRODUCTION

In recent years, the security community has come to understand the critical importance of usable security, which is primarily focused on *designing secure systems that people can use* (Cranor and Garfinkel, 2005). There is a growing demand to enhance both the security and the usability aspects of such user interactions, aiming to offer high security standards to application service providers and interaction transparency to

actual users (Biddle *et al.*, 2012; Fidas *et al.*, 2011; Inglesant and Sasse, 2010).

Research on user authentication mechanisms has received significant attention lately with the aim to improve their usability and memorability and, at the same time, decrease guessing attacks by malicious software and users (Biddle *et al.*, 2012; Chiang and Chiasson, 2013; De Luca *et al.*, 2013a, b). Researchers promote various designs of authentication mechanisms based on text and pictures, combinations of text and pictures, password managers and policies, etc. (Biddle *et al.*, 2012; Mihajlov and Jerman-Blazic, 2011; Verma, 2012). Nevertheless, a number of recent studies revealed that user authentication mechanisms still have important usability issues and underpinned the necessity for designing more usable authentication mechanisms (Biddle *et al.*, 2012; Florencio and Herley, 2007; Inglesant and Sasse, 2010). In particular, a large-scale study involving half a million users that investigated the password usage habits supports the need of memorable and secure passwords (Florencio and Herley, 2007). A more recent study by Inglesant and Sasse (2010) that investigated the impact of password policies on users' productivity and experience, suggested that security policies should be driven by the users' needs helping them to set a sufficiently stronger password through guidance and instructions instead of focusing on maximizing password strength through policies.

Ineffective practice of usability in user authentication does not naturally embed the users' individual characteristics in the design process, neglecting the fact that each individual has different characteristics, needs and preferences. In this context, a number of research works have taken into consideration the individuality of users as part of the interaction process and accordingly have investigated the effects of the users' unique characteristics and behaviours on performing the authentication process. Examples include the work of Ma *et al.* (2013) who investigated how individuals with cognitive disabilities (specifically Down syndrome) interact with text-based passwords and graphical authentication mechanisms, and accordingly suggested several design guidelines with the aim to personalize the authentication task. In particular, results suggest that graphical authentication mechanisms could be considered as a possible alternative to text-based passwords for people with Down syndrome since they were able to quickly learn and memorize the graphical authentication key. In addition, results showed that individuals with Down syndrome and other similar types of cognitive disabilities would benefit when Web environments could offer personalized authentication functions that enable the users to select their preferred authentication type. In the same line, results of recent research works have revealed a main effect of users' individual differences on preference and performance of authentication tasks. In particular, a study conducted by Belk *et al.* (2013a) has shown a main effect of users' cognitive-processing abilities on different types of user authentication tasks and the work of Nicholson *et al.* (2013) suggested that personalizing images of graphical authentication mechanisms based on the users' age, gender and culture could maximize memorability. Apart from personalization approaches, other research works have also proposed user authentication mechanisms that focus on user-centred design approaches. Examples include EyePassShapes (De Luca *et al.*, 2009), which is an authentication system that uses a unique eye gesture of the user as the authentication key, the work of Sae-Bae *et al.* (2012) who proposed a gesture-based authentication technique by taking advantage of multi-touch surfaces to combine biometric characteristics of individuals with gestural input, De Luca *et al.* (2013a) who proposed an authentication mechanism, which utilizes how each user performs the input in a pattern-based authentication mechanism for mobile touch-based devices, and the works of Jakobsson *et al.* (2009) and Tamviruzzaman *et al.* (2009) who proposed implicit authentication mechanisms that utilize the users' location to implicitly authenticate the user.

Current state of the art authentication mechanisms provide the same textual or graphical authentication mechanism to all users (Biddle *et al.*, 2012; Zhang *et al.*, 2009), without considering that users might have differences in the way they recall and process information cognitively during user authentication tasks. Driven by theories of individual differences in cognitive processing, suggesting that individuals have differences in recalling and processing textual and graphical information (Riding and Cheema, 1991; Kozhevnikov, 2007), this research work investigates whether personalizing user authentication tasks based on cognitive factors could minimize users' cognitive loads and thus minimize erroneous and inefficient interactions.

The purpose of the paper is 2-fold: (i) to propose an alternative approach of personalizing user authentication tasks based on individual differences in cognitive processing, and accordingly present the main components of a personalized user authentication mechanism and (ii) investigate the added value, in terms of task efficiency, task effectiveness and user preference, of personalizing user authentication tasks (textual and graphical) through a 4-month ecological valid user study.

The paper is organized as follows: in Section 2, we analyse the underlying theory of this work and consequently, in Section 3 we present the research questions. In Section 4, we present the main components of the proposed personalized user authentication mechanism. We then apply the personalization mechanism in the frame of a 4-month ecological valid user study and present the study design, method and developed hypotheses in Section 5. In Section 6 we analyse and interpret the results. In Section 7 we discuss the impact and limitations of the reported research, and finally in Section 8 we conclude the paper and describe promising directions of future work.

2. INDIVIDUAL DIFFERENCES IN COGNITIVE PROCESSING

A significant number of researchers have proposed graphical authentication mechanisms as alternatives to text-based

password mechanisms (Biddle *et al*., 2012; De Luca *et al*., 2013a, b; Mihajlov and Jerman-Blazic, 2011). Graphical authentication mechanisms primarily require users to recall and select pictures as their authentication key, and are considered to improve usability and memorability since they leverage the *picture superiority effect*, claiming that pictures are better recognized and recalled by the human brain than textual information (Nelson *et al*., 1976; Paivio and Csapo, 1973). In this context, graphical authentication mechanisms base their theoretical assumption on the *dual coding theory* (Biddle *et al*., 2012; Paivio, 2006; Paivio and Csapo, 1973) suggesting 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 being processed which are used to organize incoming information that can be acted upon, stored and retrieved for subsequent use. Paivio's dual coding theory explains the picture superiority effect that picture stimuli have an advantage over word stimuli because they are dually encoded; they generate both a verbal and an image code, whereas word stimuli only generate a verbal code. In addition, pictures are mentally represented along with the features being observed and are more perceptually rich than words which lend them an advantage in information processing, whereas text is visually sparse and represented symbolically (e.g. the picture of a football vs. the written word 'football').

On the contrary, several research findings claim that the picture superiority effect does not always hold and is affected by various other factors. Oates and Reder (2010) claim that the picture superiority effect only occurs when a picture affords a meaningful textual label that discriminates it from other pictures (e.g. single-object images like 'basketball', 'car', etc.). Accordingly, as an effort to explain the functioning of the human mind and empirically observed differences in mental representation and processing of information, many researchers have developed theories of individual differences in *cognitive styles* from the perspective of dual coding theory (Riding and Cheema, 1991). Consequently, these works argue that individuals have differences in the way they process and remember textual and graphical information (Riding and Cheema, 1991; Sternberg, 1997; Witkin *et al*., 1977). The work of Riding and Cheema (1991) is considered an important turning point for cognitive styles' research (Peterson *et al*., 2005), which made a survey of ∼30 different cognitive styles and concluded that many of the proposed theories measured a broad style dimension; the Verbal/Imager dimension that refers to how individuals process information and indicates their preference for representing information verbally (Verbals), or in mental pictures (Imagers). Their different characteristics and implications on interactive systems are the following:

Verbals represent the information they read, see or listen in words or verbal associations. They focus their attention externally and are stimulating which is related to their sensory preference, triggered mostly from visual, kinaesthetic, acoustical stimuli, etc. (Liu and Ginther, 1999). Hence, they prefer a stimulating external environment since they perceive it as an extension of themselves. Individuals being Verbals prefer and perform more efficiently when the hypermedia content is presented in the form of text. Verbals also have great reading accuracy and are better at recalling acoustically complex and unfamiliar text (Laing, 2001).

Imagers represent the information in mental pictures, focus their attention internally and tend to be passive which means they are primarily triggered by their thoughts, memories, etc. (Liu and Ginther, 1999). Imagers prefer and perform more efficiently when the hypermedia content is provided in the combination of graphical and textual representation, but do not perform efficiently when an exclusively verbal representation is provided (Ghinea and Chen, 2008).

A number of psychometric tests and questionnaires have been developed that elicit verbal-imagery cognitive styles, mainly through self-reported experiences and preferences, and response times on verbal and visual aptitude tasks. Self-reported questionnaires usually ask the participants to rate their preference towards a verbal versus visual mode of processing. Example ratings would be *I have a photographic memory* or *My verbal skills are excellent* (Blazhenkova and Kozhevnikov, 2009). For the reason that questionnaires showed relatively low internal reliability and poor predictive validity (McAvinue and Robertson, 2007; Peterson *et al*., 2005), objective measures through the development of psychometric tools have emerged, such as the response time in solving cognitive tasks that require verbal or visual processing and representation. Popular questionnaires and psychometric tests include the OSIVQ questionnaire (Blazhenkova and Kozhevnikov, 2009), the VICS test (Peterson *et al*., 2005) and the CSA test (Riding, 1991). Interested readers are also referred to the works of Riding and Cheema (1991) and Kozhevnikov (2007) for a review on older questionnaires and psychometric tests.

3. RESEARCH QUESTIONS

Based on the theories analysed it becomes evident that a correlation could exist between the efficiency and effectiveness of authentication tasks, and the individuality of users. Accordingly, we suggest that personalizing the user authentication type (textual or graphical) might affect differently, in terms of performance and preference, individuals who have a particular cognitive style of processing and representing more efficiently verbal or graphical information. The high-level goal of this work is to support the usability of user authentication tasks by personalizing the user authentication type (textual password or graphical authentication mechanism) based on the users' individual differences in cognitive styles (Figure 1).

The proposed approach includes the following main challenges (Brusilovsky *et al*., 2007): appropriate *user modelling* dealing with what information is important to be

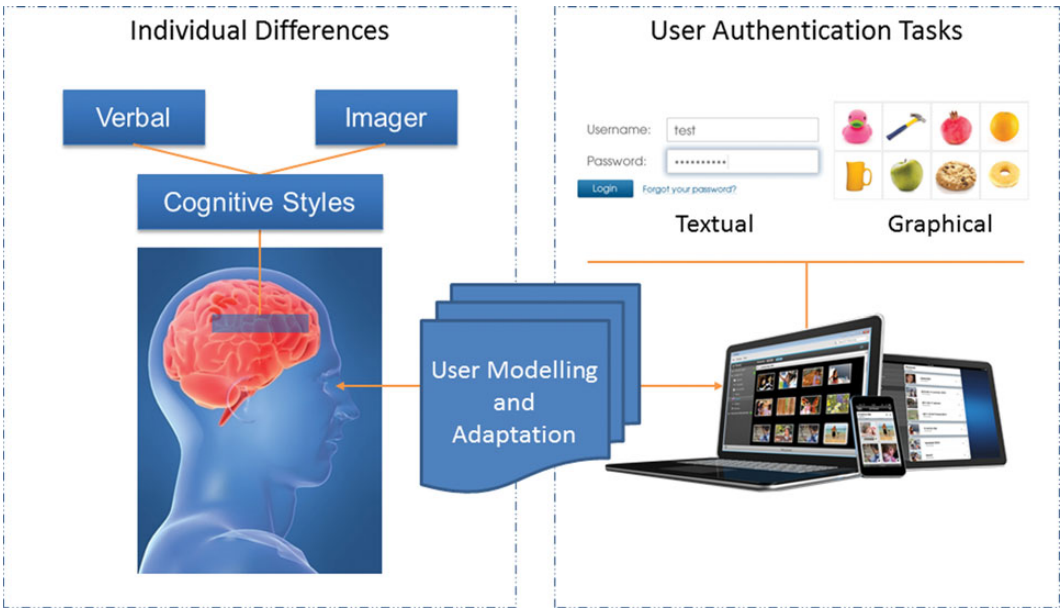

Figure 1. High-level personalization approach in user authentication based on individual differences.

incorporated in the user model and how it can be extracted, and appropriate *adaptation procedures* dealing with what adaptation types and mechanisms are most effective to be performed and how they can be translated into adaptive user interface designs in order to improve the system's usability and to provide a positive user experience.

The following research questions are investigated:

- Does matching the user authentication type to users' cognitive styles have a significant effect on task efficiency and effectiveness?
- What are the differences between the two authentication methods (textual and graphical) regarding efficiency, effectiveness and user preference, among users with different cognitive styles (Verbal or Imager)?

4. PERSONALIZED USER AUTHENTICATION BASED ON COGNITIVE FACTORS

This section presents the main components of the personalized user authentication mechanism. It consists of two main components: the *User Modelling Component* and the *Personalization Component*. The user modelling component is vital for providing personalized user authentication tasks to users. It is responsible to collect and process information about the users that is further utilized by the personalization component to provide a particular type of user authentication: *textual* or *graphical* (Figure 2).

The personalization mechanism is executed only once during user enrolment with an interactive system in which the authentication type (textual or graphical) is mapped to the user account. After enrolment, the user authenticates with the mapped authentication type by first providing his/her username for identification. Figure 3 depicts the workflow of the personalization process of a user authentication mechanism during user enrolment with an interactive system.

4.1. User authentication types

A text-based password mechanism and a recognition-based, graphical authentication mechanism were developed. The two user authentication mechanisms are described next.

4.1.1. Text-based password mechanism

A standard text-based password mechanism was developed in which users can enter alphanumeric and special keyboard characters. A unique username for identification and a minimum of eight characters including numbers, a mixture of lower- and upper-case letters and special characters are required to be entered by the users during password creation. Password characters are hidden as being typed by the users to avoid bystanders reading the password. With the aim to defend against guessing attacks based on transmission sniffers, and brute force attacks at the database level, a cryptographic hash function is utilized that encrypts the given password and transmits it through a secure channel (https), and stored in an encrypted format in the database. In the case of five consecutive incorrect password keys, a CAPTCHA mechanism (von Ahn *et al.*, 2004) is shown to the users to ensure that a human is interacting with the system and not automated software whose purpose is to guess passwords by randomly generating different combinations of password keys. An additional option

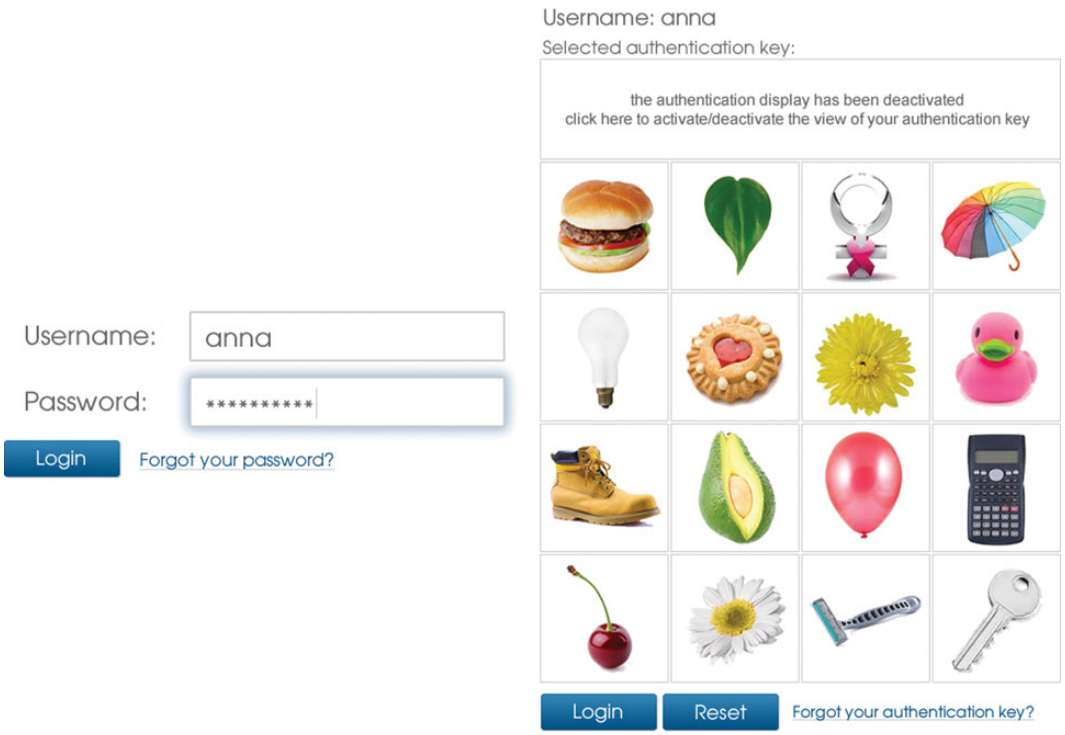

Figure 2. Text-based password (left) and graphical authentication mechanism (right).

for resetting the text-based password is available in case the users forget their authentication key. In that case, users have to enter their username and a hyperlink is then sent to their email that leads to a page for resetting their text-based password.

Finally, with the aim to prevent usage of password managers and autocomplete functions to save the password keys on the users' Web browsers, the following attributes are applied on the HTML form field: (i) the 'autocomplete' attribute of the HTML form element is set to 'off', and (ii) given that the 'autocomplete' attribute is not cross-browser compatible, a random name is generated for the 'name' attribute of the password input field in each session in order to prevent the Web browser from remembering the password key.

4.1.2. Graphical authentication mechanism

A graphical authentication mechanism that involves single-object images was developed based on the recognition-based, graphical authentication mechanism proposed by Mihajlov and Jerman-Blazic (2011). The choice of the graphical authentication mechanism was based on the following reasons: (i) according to the usability evaluation conducted by Mihajlov and Jerman-Blazic (2011), the mean task completion time is more efficient in contrast to other graphical authentication mechanisms that exist in the literature (Biddle *et al*., 2012) and (ii) a number of research works have shown that illustrating single-object images (the type of images that are used in this particular graphical authentication mechanism) facilitates memorability since single-object images can be easily labelled and recognized, in contrast to abstract images and human faces (Chowdhury *et al*., 2013; Mihajlov and Jerman-Blazic, 2011).

During the authentication key creation, users enter a unique username for identification and then can freely select between 8 and 12 images in a specific sequence out of a random subset of 60 images (split into two divisions in the page containing 30 images each) that are retrieved from a large image database. In case the user is not satisfied with the presented choices, an option to load a different image subset is available. Repetitions of images are also possible in the sequence. After the graphical authentication key is created, a fixed image set of 16 images, containing the user-selected authentication images and system-selected decoy images are 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.

During authentication, a 4×4 grid containing the user-selected and system-selected decoy images are presented (Figure 2, right). The image positions in the selection grid are randomly positioned in each authentication session. Thereafter, users have to select their images in the specific sequence, as entered in the enrolment process in order to get permission for accessing the system.

In order to defend against guessing and brute force attacks, a one-time authentication process is utilized as proposed in

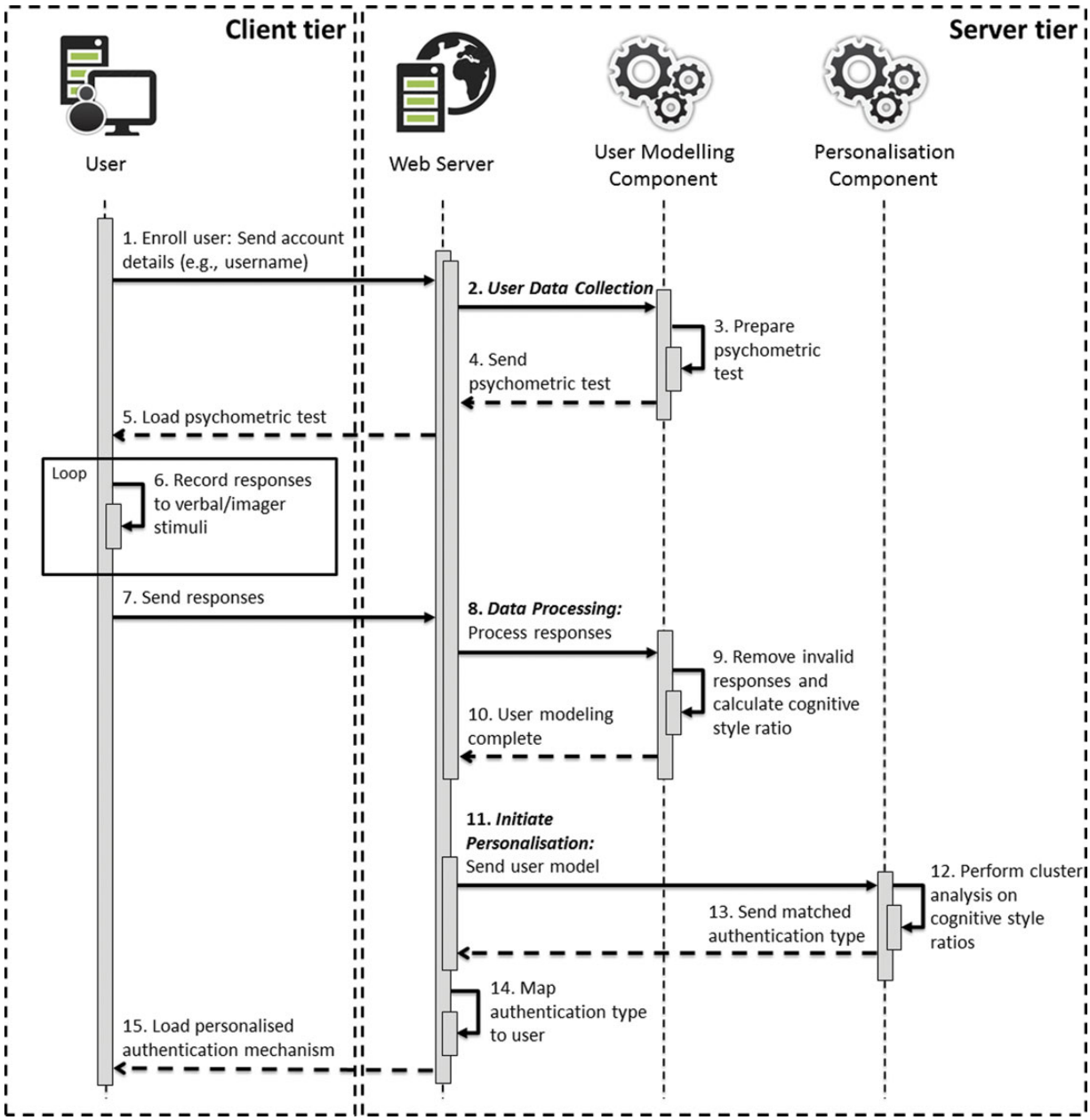

Figure 3. Sequence diagram of the user authentication personalization process during user enrolment.

the work of Mihajlov and Jerman-Blazic (2011). In particular, a random hashed number is assigned to each image and the relation between the image and the hashed number is stored in a temporary record in the database that is valid for a short period of time for the authentication session. In case the user enters five consecutive incorrect authentication keys, the system will run the one-time authentication process again by randomly assigning new random hashed numbers, and the images' positions are randomly changed at the user interface. A secure transmission layer is utilized for communication between the client and the server as in the case of text-based passwords. Finally, the temporary records are deleted from the database in case of a successful authentication session.

Similarly to the text-based password mechanism, in the case of five consecutive incorrect authentication keys, a CAPTCHA mechanism is shown to the users to prevent automated software to guess the authentication key. An additional option for resetting the authentication key is also available which is also similar to the text-based password reset process.

4.2. User modelling component

The user modelling component entails the following phases: *user data collection* and *data processing*, which are considered the basis for offering personalized user authentication tasks.

User data collection: The first step towards adapting and personalizing the user authentication task is to collect data about the users. Users first provide a unique username utilized by the system for user identification as well as basic account information, i.e. full name, gender, age and email. Furthermore, cognitive styles of users are considered the main factor in this work for personalizing the user authentication task. The users' cognitive styles are elicited by exploiting Riding's Cognitive Style Analysis test (CSA) (Riding, 1991; Riding and Cheema, 1991) since it is considered one of the most credible psychometric tests to elicit cognitive styles of users (Kinley *et al*., 2010; Riding and Cheema, 1991). In particular, we developed an online version of 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 users to be true or false. A total of 24 statements require comparing two objects conceptually (e.g. *Are ski and cricket the same type?*). The remaining 24 statements require comparing the colour of two objects (e.g. *Are cream and paper the same colour?*). It is assumed that Verbals respond faster than Imagers in the conceptual types of stimuli because the semantic conceptual category membership is verbally abstract in nature and cannot be represented in visual form (Riding, 1991). On the other hand, it is assumed that Imagers respond faster than Verbals in the appearance statements (colour) since the objects can be readily represented as mental pictures and the information for the comparison can be obtained directly and rapidly from these images (Riding, 1991). The response time and the given answer for each stimulus is recorded and provided to the next phase for data processing.

Data processing: In this phase, all the users' responses to the psychometric test are cleaned from incorrect responses and inconsistencies are resolved in order to be used as input to the personalization component. During the first step of data processing, all users' responses to the psychometric test are examined, and outliers are removed from the dataset. For example, in the case where a user remains idle during a stimulus, the response time and provided answer of that particular stimulus is removed from the dataset. Next, the average response time of all valid and correct responses is calculated on each of the two question types (verbal-type stimuli and imager-type stimuli) of the psychometric test, and then the ratio between the average response times on the verbal (conceptual category) and imagery (appearance) stimuli is calculated. It is assumed that users with a low ratio are considered Verbals, while users with a high ratio are Imagers (Riding, 1991). Algorithm #1 in the Appendix presents the pseudo code of the data processing phase.

4.3. Personalization component

The personalization component performs cluster analysis for grouping users into a specific cognitive style group (Verbal or Imager), that is further mapped to a specific type of authentication (textual or graphical). In particular, cluster analysis is performed to each user's cognitive style ratio, which is calculated in the user modelling component as the fraction of the user's average response time of the verbal stimuli and the average response time of the imagery stimuli. Accordingly, users who have a small value of cognitive style ratio are grouped as Verbals since they are responding faster to the verbal stimuli compared with the imagery stimuli, whereas users who have a large value of ratio are grouped as Imagers since they are responding faster to the imagery stimuli compared with the verbal stimuli. The main aim of this process is to divide the set of users into cluster groups that are different from each other and whose members are similar to each other according to the cognitive style ratios. Users who are grouped as Verbals finally receive a text-based user authentication mechanism and users who are grouped as Imagers receive a graphical user authentication mechanism.

We utilized the k-means clustering algorithm since it is considered one of the most robust and efficient clustering algorithms (Wu *et al*., 2007), and it could yield very good results in our case since the data being processed could be well separated from each other depending on the responses to each cognitive stimuli of the users (Belk *et al*., 2013b; Riding and Cheema, 1991). The k-means clustering algorithm requires a fixed number of k clusters to create before the algorithm runs. Given that the desired groups are known in our case (Verbal and Imager), the algorithm is set to $k = 2$. An important challenge of the algorithm is that initial data points should be assigned as cluster centres and researchers have proposed a number of modified k-means clustering algorithms aiming to effectively select the initial cluster centres to improve the efficiency of the algorithm (Wu *et al*., 2007). In our case, given that the developed psychometric test calculates a cognitive style ratio that indicates the user's tendency on the Verbal–Imager scale (with the lowest and highest cognitive style ratios being, respectively, the most extreme types of Verbals and Imagers), we can easily assign the initial data points as follows: the smallest cognitive style ratio is assigned as the initial cluster centre of the first cluster (representing the initial Verbal cluster) and the largest cognitive style ratio is assigned as the initial cluster centre of the second cluster (representing the initial Imager cluster).

Algorithm #2 in the Appendix presents our modified version of the k-means clustering algorithm. The algorithm initially sets the data point with the smallest ratio value as the first cluster centre (Verbal cluster) and the data point with the largest ratio

value as the second cluster centre (Imager cluster), i.e. $k = 2$. The distance between all other data points and cluster centres are then calculated, and each data point is assigned to the cluster whose distance from the cluster centre is the minimum of all the cluster centres using the Euclidian distance. New cluster centres are recalculated by measuring the mean of all data points of each newly created cluster. Next, the distances between each data point and the newly obtained cluster centres are recalculated in an iterative approach until no data point is reassigned.

Finally, when the two clusters are created, the mechanism maps a textual authentication mechanism to the users who are grouped in the first cluster which contains lower values of cognitive style ratio (Verbals), whereas a graphical authentication mechanism is provided to users who are grouped in the second cluster which contains higher values of cognitive style ratio (Imagers). For future user interactions with the system, each user accesses the system through the mapped user authentication mechanism. In case no information about the cognitive styles of users is available (either because the user did not perform the psychometric test or all of his/her interactions with the psychometric test were invalid), the system provides the option to the user to choose the preferred user authentication type.

5. STUDY DESIGN

In this section we present the method of applying the personalized user authentication mechanism in the frame of a 4-month ecological valid user study in which users interacted with two different types of user authentication tasks that were recommended by the developed personalization mechanism.

5.1. Procedure

The Web-based personalization mechanism was applied within the frame of various university courses. The user modelling and personalization process was divided in two phases during users' enrolments:

Phase A—User modelling: Controlled laboratory sessions were conducted at the beginning of the study aiming to elicit the users' cognitive styles through the psychometric test. With the aim to apply the psychometric test in a scientific right manner, we conducted several sessions with a maximum of 10 participants by following the protocol suggested by the inventors of the psychometric tests. Participants initially created their basic user profile by providing explicitly their username and personal information (i.e. email, age, gender) through an online form, and then interacted with the developed online psychometric test to elicit their cognitive styles. For the purpose of the study, in order to proceed with Phase B, all participants interacted first with the user modelling component in order to elicit the cognitive style ratios of all users and further perform the cluster analysis in Phase B for mapping each authentication type to users based on the generated clusters.

Phase B—Personalization: Participants created their authentication key that was used for accessing the courses' material (i.e. course slides, homework exercises) and for viewing their grades throughout the semester. In this phase, the personalization mechanism mapped a specific type of authentication (text-based password or graphical authentication mechanism) based on the cluster each user was assigned according to his/her responses to the psychometric test in Phase A. The clustering algorithm was applied on an existing representative sample of 800 undergraduate students of the same university whose cognitive styles were elicited in past user studies of the authors. The mapped user authentication mechanism was then utilized by the user for authenticating in the system throughout the semester.

In order to investigate the added value of personalizing the user authentication task based on the users' cognitive styles, a matched and a mismatched condition was randomly assigned to the decision rules so that half of the participants would interact with a personalized user authentication mechanism (matched condition) and half of the participants would interact with a non-personalized user authentication mechanism (mismatched condition). For example, in case of a matched condition, the user would receive the authentication mechanism as recommended by the personalization mechanism, whereas a mismatched condition would provide the opposite type of user authentication to the one suggested by the system. The allocation was based on the users' cognitive styles so that the conditions were balanced across all cognitive style groups.

The users' interactions were recorded for a period of 3 months. After this period, aiming to engage all participants with both types of user authentication mechanisms (textual and graphical), during the last month of the study, the system provided the opposite type of user authentication mechanism to all users (users who initially interacted with a personalized mechanism were prompted by the system to create a non-personalized mechanism, and vice versa). The interactions during the last month were intended only to provide experience to users regarding the opposite type of user authentication mechanism and further elicit their preference towards a particular authentication type.

5.2. User data

Both quantitative and qualitative data about the users was collected. Quantitative data were collected through client-side and server-side scripts that monitored the users' behaviour during interaction with the user authentication mechanisms. In particular, we developed client-side scripts at the user interface level for measuring the time needed to login by the users, whereas server-side scripts for handling and counting login errors. The following measurements were captured:

Task efficiency: Task efficiency for each participant was evaluated based on the total time spent to enroll (registration) and time spent to login. Login time for each participant was measured as the median time of all successful sessions for each of the conditions (Chowdhury

et al., 2013). Since the study was conducted in an ecological valid context, users performed the tasks at their own physical environment; we used the median time since it is robust against outliers (e.g. when a user receives a phone call while authenticating). Recording time started on page load until they successfully completed the user authentication task.

Task effectiveness: Task effectiveness for each participant was evaluated based on the login success rate and total number of authentication key resets for each of the conditions. Login success rate was calculated by dividing the total number of successful authentication sessions with the total number of all authentication sessions of each user. A session is considered as successful in this case when the user successfully logins at first attempt. A session is considered as non-successful when a user needs more than one attempt to authenticate. For example, for a specific session, if the user made four attempts to authenticate (the first three attempts failed, and the fourth one succeeded), this session is considered as a non-successful session.

User preference: Qualitative data were collected at the end of the study through semi-structured focus groups to elicit the users' subjective preference and perceptions regarding the interactions they had with the user authentication mechanisms.

5.3. Participants

The study was conducted with a total of 153 participants (43.79% male, 56.21% female, age 17–22 years). Participants were undergraduate students of Psychology and Social Science Departments. The sample included users who were rather experienced and average than novice users with respect to user authentication and therefore, the research design was set up in order to avoid inference errors. Furthermore, the participants were familiar and experienced with textual password mechanisms prior to the study since all of them were using at least one password protected online account, and they had no experience with recognition-based, graphical authentication mechanisms.

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).

5.4. Hypotheses

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

H_1—Efficiency: The login time needed to successfully authenticate through a personalized user authentication mechanism is improved compared with the non-personalized user authentication mechanism, considering also various main effects and interactions with respect to cognitive styles of users.

H_2—Effectiveness: The success rate of a personalized user authentication mechanism is increased compared with the non-personalized user authentication mechanism, considering also various main effects and interactions with respect to cognitive styles of users.

H_3—Preference: Verbal and Imager users prefer a particular type of user authentication that is closer to their habitual approach of cognitive processing and representation.

6. ANALYSIS OF RESULTS

We performed several descriptive and inferential statistical analyses to investigate the added value of personalizing user authentication tasks based on users' cognitive styles. The analysis investigates the impact of cognitive styles on task efficiency, task effectiveness and user preference of different types of user authentication tasks. The reported analysis of task efficiency and effectiveness contains user interactions of the initial 3 months of the study, excluding the user interactions of the last month that were intended only to provide experience to users regarding the opposite type of user authentication.

Given the between-subjects study design, we used the independent-samples t-test and the analysis of variance (ANOVA) test, where appropriate, aiming to investigate interaction effects between cognitive styles of users and user authentication types on the time spent on user enrolment (registration), time spent on login and success rate. The Mann–Whitney U-test was used in cases we wanted to investigate the differences between ordinal data (authentication key requests) and the χ^2 test was used to examine whether the participants prefer a specific authentication method over the other in terms of preference and perceived usability. We next analyse and discuss findings of each measure.

6.1. Clustering results

The cluster analysis separated users into two clusters based on their cognitive style ratios: Verbals ($n = 70$, $f = 45.8\%$) and Imagers ($n = 83$, $f = 54.2\%$), which consisted of participants who belong to the Verbal and Imager class, respectively. The main goal of the clustering algorithm was to minimize variability within the clusters and maximize variability between the clusters based on the users' cognitive style ratios. The analysis and evaluation was focused on how different the cognitive style ratios of users were between the two clusters. An independent-samples t-test was conducted to determine mean differences on the cognitive style ratios between the two created cluster groups (Table 1). There was homogeneity of variances, as assessed by Levene's test for equality of variances ($P = 0.728$). Results indicated that there were significant differences among cognitive style ratios between the two clusters ($t(151) = 23.761$, $P < 0.001$), indicating that the personalization mechanism grouped effectively the users into

two different clusters, and could be thus safely used in the main data analysis.

6.2. Descriptive statistics

A total of 153 user accounts have been created during the enrolment phase. The participants' university identity was utilized as their username which was seven characters long for all users. Regarding the text-based authentication key, the minimum length was 8 characters, while the maximum length was 12 for all users ($M = 8.49$, $SD = 1.188$). Regarding the graphical authentication key, the minimum length was 8 images, while the maximum length was 10 for all users ($M = 8.16$, $SD = 0.491$), with the majority of participants using an 8-image graphical authentication key. A two-by-two factorial ANOVA was run to determine whether there were differences in the key length between Verbal and Imager users per user authentication type. The test revealed that there were no significant differences in the key length between Verbals and Imagers in both text-based and graphical authentication types ($F(1, 153) = 0.567$, $P = 0.453$).

During the authentication key creation phase, Verbal users spent on average 35.85 s ($SD = 9.20$) to successfully create a text-based password key, while Imagers spent on average 36.04 s ($SD = 9.65$). Regarding the graphical authentication key creation, Verbals spent on average 87.01 s ($SD = 25.17$) to successfully create a graphical authentication key, while Imagers spent on average 79.55 s ($SD = 28.19$). A two-by-two way factorial ANOVA did not reveal significant differences with regard to time spent for creating an authentication key between Verbals and Imagers and user authentication type ($F(1, 153) = 1.387$, $P = 0.241$).

Table 1. Descriptive statistics of the cognitive style ratios in each cluster.

Cluster 1—Verbals			Cluster 2—Imagers		
Mean	Std. Dev.	*n*	Mean	Std. Dev.	*n*
0.77	0.1	70	1.2	0.11	83

Finally, a total of 5535 authentication sessions have been recorded during the 3-month period, with a mean of 33.75 ($SD = 13.62$) logins per participant.

6.3. User authentication efficiency

Task efficiency was evaluated based on user enrolment time and login time. We distinguished login time and performed several analyses as follows: (i) overall login time spent from page load, including entering username for user identification until entering the authentication key, (ii) time spent to enter the username, (iii) time spent to enter the authentication key (i.e. from entering the first character/image to last character/image) and (iv) mean time between character/image inputs of the authentication key. Table 2 summarizes the login time measures per cognitive styles group and user authentication type.

6.3.1. Overall login time

Overall login time was measured as the time starting from page load until successfully entering the user authentication key. This includes entering the username for user identification and entering the authentication key but also includes the overall cognitive processing performed by the user based on the rest stimuli included in the page. We initially aim to investigate whether the proposed personalization approach has improved the user authentication task in terms of overall time spent to login. Accordingly, an independent-samples *t*-test was performed to determine mean differences on the time needed to authenticate through the personalized and non-personalized user authentication mechanism. The analysis revealed that interactions with personalized user authentication mechanisms were more efficient ($M = 12.86$, $SD = 1.26$, $SE = 0.14$) than non-personalized user authentication mechanisms ($M = 14.36$, $SD = 1.05$, $SE = 0.12$). These results were statistically significant ($MD = 1.51$, $t(151) = 7.982$, $P < 0.01$). Figure 4 illustrates the means of performances for each condition.

Furthermore, a two-by-two way factorial ANOVA was conducted aiming to examine main effects and interactions between the users' cognitive styles (i.e. Verbal and Imager) and authentication type (i.e. text-based and graphical) over the time needed to successfully authenticate. Figure 5 illustrates

Table 2. Login time measures.

	Verbals		Imagers	
Time spent	Textual (p)	Graphical (np)	Textual (np)	Graphical (p)
Overall login	12.54 (1.52)	14.46 (0.61)	14.28 (1.31)	13.14 (0.91)
Username	1.79 (0.83)	1.59 (0.89)	1.73 (0.88)	1.84 (0.84)
First to last	9.26 (1.48)	11.17 (0.58)	10.98 (1.31)	9.84 (0.91)
Between clicks	1.08 (0.07)	1.37 (0.05)	1.31 (0.05)	1.2 (0.06)

p, personalized condition; np, non-personalized condition.

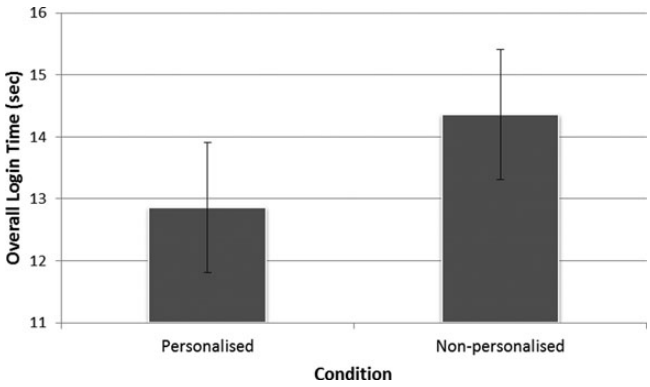

Figure 4. Means of overall login time per personalization condition.

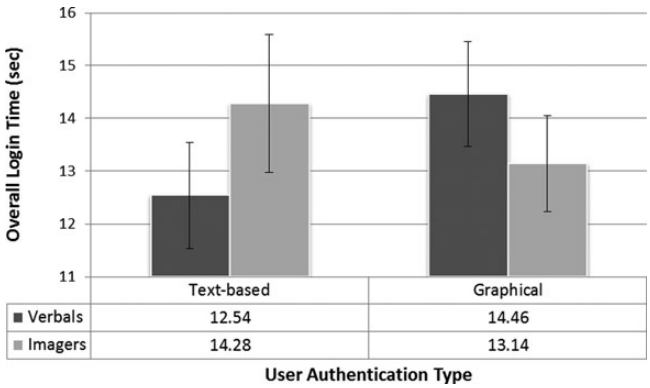

Figure 5. Means of overall login time per cognitive style group and authentication type.

the means of performances of each cognitive style group and authentication types.

The analysis revealed an interaction effect between cognitive styles and authentication type on the time to authenticate ($F(1, 153) = 67.546$, $P = 0.001$). A pairwise comparison between cognitive style groups revealed that Verbals performed significantly faster with text-based passwords (personalized condition) with a mean of 12.54 seconds compared with Imagers that had a mean of 14.28 s ($MD = 1.746$, $SE = 0.263$; $F(1, 149) = 44.123$, $P < 0.01$). Similarly, in the case of user interactions with the graphical authentication mechanism, significant differences were observed with Imagers having a mean of 13.14 s (the graphical authentication mechanism being the personalized condition for Imagers), compared with Verbals who had a mean of 14.46 s ($MD = 1.318$, $SE = 0.264$; $F(1, 149) = 24.850$, $P < 0.01$). Finally, a pairwise comparison between authentication types revealed that in the case of Verbals the mean difference login time ($MD = 1.92$) between the text-based and graphical authentication mechanism was larger, compared with Imagers ($MD = 1.143$). This may be due to the fact that the personalized condition for Verbals (text-based passwords) was also affected by the familiarity factor since users were more experienced with textual passwords, in contrast to Imagers that received a graphical authentication mechanism as a personalized condition. Nevertheless, both cases indicate that for both user types, the personalized condition significantly improves task efficiency compared with the non-personalized condition.

To this end, the results can be interpreted under the light of cognitive styles as they demonstrate a main effect on task efficiency. Given the natural ability and preference of users processing more efficiently textual or graphical information (Riding and Cheema, 1991), the results indicate that these cognitive processing characteristics could be a determinant factor on the personalization of user authentication mechanisms as they improve task completion efficiency of user authentication which supports Hypothesis #1.

6.3.2. Username time

Username was entered by the users for user identification and was utilized by the personalization mechanism to provide the given type of user authentication. A two-by-two way factorial ANOVA revealed that the user authentication type (text-based and graphical) and cognitive styles (Verbal and Imager) did not have an interaction effect on time to enter the username ($F(1, 153) = 1.144$, $P = 0.287$). In addition, given that the username length was the same for all users (seven characters long university identity number), such a result was rather expected.

6.3.3. Time from first to last character/image input

A sub-analysis regarding the time for entering the user authentication key from first to last character/image was analysed with the aim to investigate the differences in authentication key recall time between cognitive style groups and authentication types. A two-by-two factorial ANOVA was conducted using cognitive styles (Verbal and Imager) and user authentication type (text-based and graphical) as independent variables, and the time to enter the authentication key (from first to last character/image input) as the dependent variable. The analysis revealed that there was a statistically significant interaction between cognitive styles and user authentication type on the time to enter the authentication key ($F(1, 153) = 68.860$, $P < 0.001$). Such a result is in line with the overall login time analysis (Section 6.3.1) which further supports Hypothesis #1 and that individual differences in cognitive styles affect task efficiency of particular types of authentication mechanisms.

6.3.4. Learning effects on task efficiency

The impact of trials was analysed on the overall login time aiming to investigate whether learning effects exist and whether they correlate with the authentication type and cognitive styles. The analysis compared login times that were grouped by months (3) and grouped by weeks (12). A repeated measures analysis of variance test was conducted using participants' cognitive styles (Verbal and Imager) and user authentication type (text-based

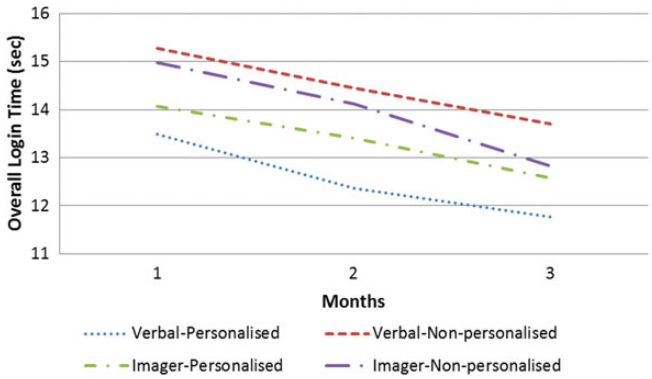

Figure 6. Means of overall login time per cognitive style group and authentication type over 3 months.

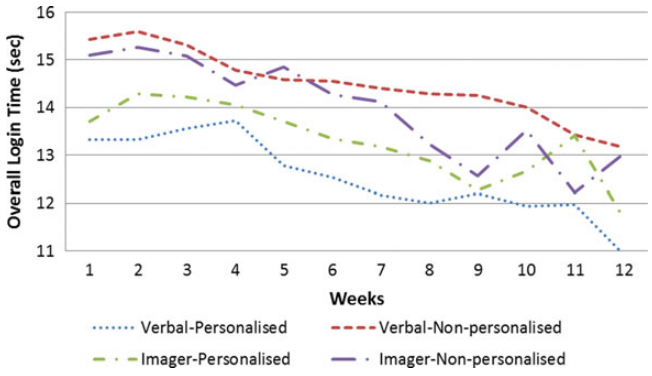

Figure 7. Means of overall login time per cognitive style group and authentication type over 12 weeks.

and graphical) as independent variables and the time spent on login as the dependent variable. Two separate analyses were performed comparing the times per month (3) and per week (12). Figures 6 and 7, respectively, illustrate the mean login times on a monthly basis and on a weekly basis for both cognitive style groups using the two authentication types.

In both statistical tests, results suggest that users spent significantly less time to login as they gain experience with the authentication mechanisms (monthly: $F(2, 149) = 158.975$, $P < 0.01$; weekly: $F(2, 149) = 27.610$, $P < 0.01$). Furthermore, in both analyses, learning effects did not correlate with cognitive styles nor user authentication type as the trend was observed for both user groups and authentication types (monthly: $F(2, 149) = 1.292$, $P = 0.278$; weekly: $F(2, 149) = 1.391$, $P = 0.184$).

In the monthly comparison we have observed a decline of login time throughout the 3 months for all users, with all cognitive style groups having steady differences, i.e. Verbals who received a personalized condition were every month faster at login, followed by Imagers with a personalized condition and then, respectively, with Imagers and Verbals who received a non-personalized condition. Furthermore, the weekly comparison has shown that all users had an increase in time to login from first to second week, especially in the case of users interacting with a graphical authentication mechanism. This might be interpreted based on the fact that users were not familiar with this kind of authentication type. Nevertheless, over time we observe that time to login with graphical authentication mechanisms decreases over time. Also, interactions of Verbals who received a personalized condition spent the lowest time throughout all the 12 weeks.

6.4. User authentication task effectiveness

Task effectiveness was evaluated based on the login success rate and the total number of authentication key reset requests. We also examine the impact of trials on success rate over time.

6.4.1. Success rate of login

User authentication effectiveness was measured in terms of success rate. The analysis compared the effectiveness between the personalized and non-personalized user authentication interactions. Overall, the majority of user sessions were completed at first attempt in both conditions. However, in the case of non-personalized user interactions, a higher number of attempts were recorded. In particular, an independent-samples t-test showed that there is a statistically significant difference between the two conditions ($t(151) = -9.602$, $P < 0.01$) which indicates that the proposed personalization method significantly affects the success rate of user authentication. In particular, personalized user authentication interactions had a mean success rate of 89.77% ($SD = 4.28$), whereas non-personalized user authentication interactions had a mean success rate of 82.67% ($SD = 4.83$). The results suggest that personalized user authentication tasks have an improved success rate compared with non-personalized user authentication tasks which supports Hypothesis #2.

Furthermore, a two-by-two way factorial ANOVA was conducted using cognitive styles (Verbal and Imager) and user authentication type (text-based and graphical) as independent variables and the user authentication success rate as the dependent variable. Figure 8 illustrates the success rate per cognitive style group and authentication type.

Results revealed a main interaction effect between cognitive styles and user authentication type on the success rate ($F(2, 153) = 122.523$, $P < 0.01$). A pairwise comparison between Verbals and Imagers revealed that Verbals were significantly more effective than Imagers in text-based passwords ($MD = 2.613$, $SE = 0.912$; $F(1, 149) = 8.208$, $P = 0.005$). In the case of graphical authentication, a higher mean difference in the success rate was observed between Imagers and Verbals, with Imagers being significantly more effective when authenticating through graphical authentication mechanisms ($MD = 11.703$, $SE = 0.917$; $F(1, 149) = 169.865$, $P = 0.001$).

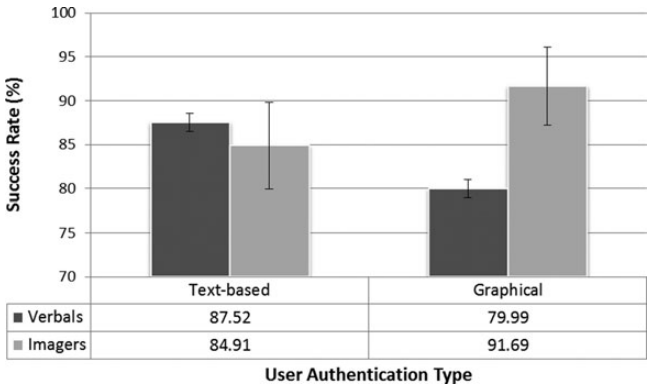

Figure 8. Success rate per cognitive style group and authentication type.

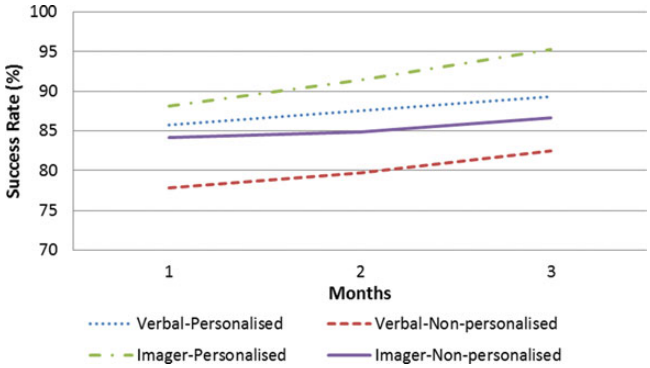

Figure 9. Success rate per cognitive style group and authentication type over 3 months.

6.4.2. *Learning effects on task effectiveness*

Similar to the task efficiency analysis, the impact of trials was investigated on the success rate aiming to investigate whether learning effects exist and whether they correlate with the authentication type and cognitive styles. The analysis compared success rates that were grouped by months (3) and grouped by weeks (12). A repeated measures analysis of variance test was conducted using participants' cognitive styles (Verbal and Imager) and user authentication type (text-based and graphical) as independent variables and the success rate as the dependent variable. Two separate analyses were performed comparing the times per month (3) and per week (12). Figures 9 and 10, respectively, illustrate the mean success rates on a monthly basis and on a weekly basis for both cognitive style groups using the two authentication types.

In both statistical tests, results suggest that users made less errors on login as they gain experience with the authentication mechanisms (monthly: $F(2, 149) = 468.358$, $P < 0.01$; weekly: $F(2, 149) = 129.594$, $P < 0.01$). Furthermore, the analysis revealed an interaction effect between cognitive styles and user authentication type on the success rate (monthly: $F(2, 149) = 9.217$, $P < 0.01$; weekly: $F(2, 149) = 5.217$, $P < 0.01$).

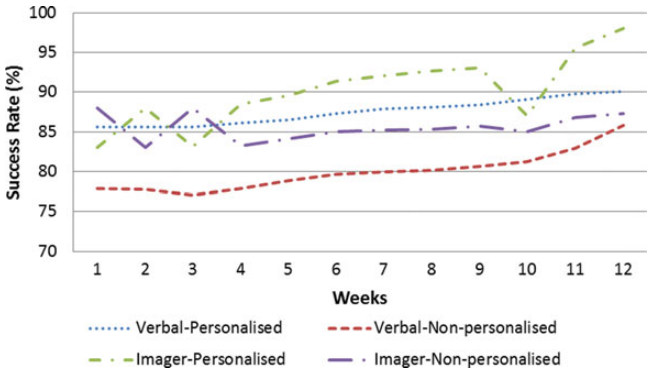

Figure 10. Success rate per cognitive style group and authentication type over 12 weeks.

The monthly comparison revealed that the success rates were steadily increasing every month with Imagers interacting with the personalized condition having the highest success rate, followed by Verbals with personalized condition and then, respectively, Verbals with non-personalized and Imagers with non-personalized conditions. The weekly comparison revealed that Verbals who received a non-personalized condition (graphical) had the lowest success rate throughout the 12 weeks. Also in the case of Verbals (in both conditions) the success rate steadily increased over time, with the personalized condition (text-based) having higher success rates in every week compared with the non-personalized condition (graphical). On the other hand, in the case of Imagers the success rates between the two conditions were changing during the initial 4 weeks. After the 4 weeks, however, Imagers who received a personalized condition had higher success rates in every week until the end of the study. These results reveal that in the case of Verbals, the personalized condition improves success rates through each week of the study, whereas in the case of Imagers, initial trials did not reveal clear differences between success rates; however, with more trials Imagers had significantly higher success rates compared with the non-personalized condition.

6.4.3. *Authentication key resets*

The number of authentication key resets was counted. Table 3 summarizes the total number of authentication key requests per cognitive styles group and condition. We conducted the rank-based non-parametric Mann–Whitney U-test to determine whether there were differences in authentication key requests between personalized and non-personalized conditions. The test revealed no significant differences in the number of authentication key requests between the groups ($U = 1$, $z = -0.775$, $P = 0.439$).

In both cognitive style groups, the majority of users requested to reset their graphical authentication key. A Mann–Whitney U-test was conducted to determine whether there were differences in the number of authentication key requests between the two user authentication conditions. The test revealed no

Table 3. Authentication key requests.

	Verbals		Imagers		
	Textual (p)	Graphical (np)	Textual (np)	Graphical (p)	Total
Month 1	1	4	0	3	8
Month 2	3	5	4	4	17
Month 3	2	3	3	5	13
Total	6	13	7	12	38

p, personalized condition; np, non-personalized condition.

significant differences in the number of authentication key requests between the two groups ($U = 0$, $z = -1.549$, $P = 0.121$). Although the number of authentication key requests could be an indicator for user authentication effectiveness, based on the reported results no safe conclusions can be drawn whether there is an interaction effect between users' cognitive styles and authentication condition on the number of authentication key requests.

6.5. Focus groups

Focus-group sessions were concentrated around the participants' subjective preference and perception based on the authentication-based interactions they had during the study. As mentioned in the Procedure Section, during the last month of the study, users were provided with the opposite user authentication type with the aim to engage all the participants with both authentication conditions and further elicit their preference towards a particular type of authentication. The users' performance interactions (efficiency and effectiveness) during the last month were not utilized in the previous analysis of results and were intended only to provide experience to users about the opposite user authentication type.

Six focus-group interviews took place after the end of the study, each group containing 10 participants, with equal number of Verbals and Imagers in each group (5). The focus groups followed a semi-structured process based on predetermined questions that lasted ∼20 min. Audio recordings and examiner notes were used to collect the participants' data. All participants of the focus groups were asked to rank the two authentication methods based on the following aspects: (i) the type of authentication that the users prefer, (ii) the type of authentication that was more efficient, (iii) the type of authentication that was more effective and (iv) the type of authentication that was more memorable. Example questions were *Which authentication type needed less attempts to complete?*, *Which authentication type do you prefer?*, *Which authentication key type was easier to remember?* For each question, participants ranked the two authentication methods with 1 and 2 to represent their first and second choices. Table 4 lists the number of participants who chose a specific method as their first choice for each factor.

Table 4. Participants who chose a specific authentication type as their first choice for each evaluation factor.

	Verbals		Imagers	
	Textual (p)	Graphical (np)	Textual (np)	Graphical (p)
1. Preference	17	13	*9*	*21*
2. Efficiency	*23*	*7*	*11*	*19*
3. Effectiveness	14	16	13	17
4. Memorability	12	18	*6*	*24*

Numbers in italic revealed significant differences between the two methods for each factor. p, personalized condition; np, non-personalized condition.

Factor 1—Authentication preference: There is a statistical significant association between cognitive styles and authentication preference (*Chi square value* $= 4.344$, $df = 1$, $P = 0.037$). Significant differences were observed in the case of Imagers, with 21 Imagers choosing the graphical authentication mechanism as their first choice, while 9 choosing textual passwords. On the other hand, 17 Verbal users preferred textual passwords with a considerable number (13) preferring the graphical authentication mechanism. As participants commented, their preference was based on the novelty factor of graphical authentication mechanisms as an interesting alternative to existing textual passwords. However, results suggest that if novelty would be the main factor that influences users' preference then it would be observed across all user groups regardless of their cognitive style, which in the current sample is not the case, since users categorized in the Verbal group did not significantly prefer a particular authentication type, providing support for Hypothesis 3.

Factor 2—Authentication efficiency: Similarly, there is a statistical significant association between cognitive styles and perceived efficiency (*Chi square value* $= 9.774$, $df = 1$, $P = 0.002$). 19 Imagers thought that the graphical authentication mechanism (personalized) was the most efficient, while 11 chose the textual password. 23 Verbals chose textual passwords (personalized), compared with seven that chose the graphical authentication mechanism. Such a result further supports the quantitative results which revealed that task efficiency was improved in the personalized condition for both cognitive style groups.

Factor 3—Authentication effectiveness: There was no significant association between cognitive styles and perceived effectiveness (*Chi square value* $= 0.067$, $df = 1$, $P = 0.795$). This might be based on the fact that the majority of users authenticated successfully at first attempt, making it difficult to compare the effectiveness of one of the two authentication mechanisms.

Factor 4 - Authentication Memorability: There is no statistical significant association between cognitive styles and memorability (*Chi square value* $= 2.857$, $df = 1$, $P = 0.091$) since the graphical authentication mechanism was rated as more memorable for both user groups. 24 over 6 Imagers and 18 over 12 Verbals chose the graphical authentication mechanism. We observe that a considerable number of Verbals perceived the textual password mechanism as more memorable. It is also worth mentioning that

users commented that memorability of the graphical authentication mechanism increased even more after several sessions.

7. IMPORTANCE AND LIMITATIONS OF THE STUDY

This section discusses the importance of the reported research and limitations of the study.

7.1. Importance of personalizing user authentication tasks

Taken into consideration that user authentication tasks are performed on every moment worldwide by millions of users it becomes evident that having a usability flaw in such human computer interaction cycles, or even not considering usability issues while designing them, results in unacceptable trade-offs for the users in terms of time and money. Thus, embracing usability aspects in designing usable user authentication mechanisms has become nowadays a necessity (Biddle *et al*., 2012; Inglesant and Sasse, 2010; Florencio and Herley, 2007).

User authentication (text, image) is primarily a human information processing task. While user authentication mechanisms are becoming less usable due to the increasing strength of authentication key policies (Inglesant and Sasse, 2010), and users demand new approaches that will adapt according to their individual characteristics (Belk *et al*., 2013a; Ma *et al*., 2013; Nicholson *et al*., 2013), the main impact of the presented research is that it provides an alternative point of view in delivering personalized user authentication mechanisms to users.

Results of the study demonstrate that the proposed approach could be considered as an alternative to current user authentication practices, since user interactions with personalized user authentication tasks were improved in terms of task efficiency and effectiveness. In addition, analysis of results demonstrated several interaction effects between cognitive styles of users on task performance and user preference towards different types of user authentication types. In particular, this study provides evidence that individual differences in cognitive processing have a main impact on users' performance and preference of user authentication tasks and accordingly suggests enhancing current user authentication mechanisms aiming to embrace both text-based and graphical authentication mechanisms. Such an approach would have many positive implications from a usability and user experience point of view since, recommending authentication mechanisms (textual or graphical), personalized to the users' cognitive styles has a positive impact on the users' memorability and information processing efficiency of the authentication key, and thus improves task completion efficiency and effectiveness, and user satisfaction. At the same time, graphical and textual authentication mechanisms provide similar security protection levels taking into consideration that they are encrypted properly on the service provider database layer and submitted securely on the transmission layer (Biddle *et al*., 2012; Mihajlov and Jerman-Blazic, 2011). Furthermore, as presented in sub-section 4.1.2, the authentication key space of the two authentication mechanisms is similar, given that users may choose 8–12 characters/images out of 60+ characters/images during enrolment. On the user layer, the graphical authentication mechanism might have a smaller key space due to the 4×4 grid of images which is smaller compared with the text-based password mechanism; however, possible attackers at the user layer are prevented through several security measures that are applied on the graphical authentication mechanism as proposed by Mihajlov and Jerman-Blazic (2011), such as the one-time authentication process, the five consecutive login trials policy and the CAPTCHA mechanism.

7.2. Limitations of the study

Limitations of this study are based on the fact that the user study included a rather limited sample with non-varying profiles (e.g. age). Although the results revealed an observable main effect of cognitive factors on user authentication task performance, we are aware that these findings must be repeatedly confirmed. A practical limitation of this work would be the prerequisite of users conducting the psychometric test during enrolment with the system which might be rather time consuming for users. In addition, initialization issues of the clustering mechanism exist for future wide-scale deployment of the proposed mechanism which are out of the scope of this paper. Nevertheless, we suggest that implicit user modelling approaches could be utilized as the ones suggested in the works of Chen and Liu (2008) and Belk *et al*. (2013b) that aim to implicitly elicit the users' cognitive styles based on the navigation behaviour of users. Finally, the reported work was conducted on a particular user authentication mechanism, which may not be considered as representative of all possible security mechanisms. Still, the integration of individual differences of users seems to be viable in the context of usable security, but should be further tested in other security mechanisms. In this respect, future work includes applying the approach on different security mechanisms such as CAPTCHA (von Ahn *et al*., 2004). For example, given that different types of CAPTCHA mechanisms exist in the literature which includes text recognition, image recognition and speech recognition (Shirali-Shahreza *et al*., 2013), adapting the type of CAPTCHA; provide either a text-recognition or image-recognition CAPTCHA based on the preferred or more effective way of users' cognitive processing could improve task usability and overall user experience.

8. CONCLUSIONS AND FUTURE WORK

The paper proposed an alternative, to current state of the art, authentication mechanism aiming to personalize user

authentication tasks based on individual differences in cognitive styles. The proposed approach was applied in a real-life Web environment that provided personalized user authentication mechanisms based on the users' cognitive styles. For the purpose of this research we have designed an ecological valid user study which entailed a credible psychometric-based test for eliciting users' cognitive styles and a real usage scenario of users interacting with the personalized user authentication mechanism for a period of 4 months. The results revealed that matching the user authentication type (textual or graphical) to users' cognitive styles improves user performance, and user satisfaction in terms of preference. Both Verbals and Imagers who were interacting with personalized conditions were significantly more efficient and effective than those who interacted with non-personalized conditions. These findings are consistent with the theories of cognitive styles that are referred in our approach, and it seems that the challenging task of translating these theories into adaptation rules was at some extent successful. Furthermore, results also yielded several interaction effects between cognitive styles and user authentication types on user performance in terms of efficiency and effectiveness of tasks. In particular, the research underpins that Verbal users authenticate more efficiently and effectively with text-based passwords than graphical authentication mechanisms, whereas Imager users the opposite.

In general we suggest that more user-centred design approaches are necessary to understand the human behaviour in such tasks and to design, develop and deploy more usable authentication mechanisms. The proposed approach could also have strong implications on older adults whose cognitive processing characteristics are limited and decline over time (Schaie, 2013). In this context, future research prospects include conducting further user studies with other samples like older adults as well as investigate the impact of other cognitive factors (e.g. working memory capacity) on user authentication interactions with the aim to strengthen the validity of the reported results and increase our understanding about the effects of users' cognitive processing factors on preference and performance related to user authentication. Furthermore, bearing in mind that users experience their context and environment in different manners and perspectives (Kozhevnikov, 2007; Riding and Cheema, 1991), and given that users interact through heterogeneous devices (e.g. desktop computers, mobile touch-based devices), future work is to further extend the user model including additional cognitive styles of users who describe the users' behaviour in various contexts of use. In particular, the Wholist/Analyst dimension (Kozhevnikov, 2007; Riding and Cheema, 1991) is another accredited and widely known cognitive style dimension that refers to how individuals organize information and indicates a preference of structuring information as a whole to get the big picture and experiencing surroundings of the environment in a relative passive and global manner (Wholists), or structuring the information in detail and experiencing surroundings in an active manner and with an internal perspective (Analysts). Accordingly, changing the device/surrounding during interaction (desktop computer or mobile touch-based device) might affect differently users who experience surroundings and situations differently (holistically or analytically). Such an attempt requires to investigate whether differences exist between the two authentication methods (textual and graphical) regarding efficiency, success rate and user preference, among users with different cognitive styles (Verbal or Imager and Wholist or Analyst), interacting with different types of devices (desktop computers or mobile touch-based devices).

We envision that results of the reported research would provide important insights to practitioners for designing more usable and user-centric authentication mechanisms, and researchers to understand human factors and behaviour within such tasks. The importance of user authentication task usability in current and future deployed eServices and applications for the society is considered to be of paramount importance on the economical but also on the user acceptance layer, since more usable security interactions, in less misuse and support costs, contribute to a more positive user acceptance for almost all citizens.

ACKNOWLEDGEMENTS

The work is co-funded by the PersonaWeb project under the Cyprus Research Promotion Foundation (ΤΠΕ/ΠΛΗΡΟ/0311(BIE)/10) and the EU project SocialRobot (285870). We also thank all the students who participated in the user study and for their valuable feedback and support.

REFERENCES

Belk, M., Fidas, C., Germanakos, P. and Samaras, G. (2013a). Security for Diversity: Studying the Effects of Verbal and Imagery Processes on User Authentication Mechanisms. In Proc. IFIP INTERACT 2013, pp. 442–459. Springer, Berlin, Heidelberg.

Belk, M., Papatheocharous, E., Germanakos, P. and Samaras, G. (2013b). Modeling users on the World Wide Web based on cognitive factors, navigation behaviour and clustering techniques. Syst. Softw., 86(12), 2995–3012.

Biddle, R., Chiasson, S. and van Oorschot, P. (2012). Graphical passwords: learning from the first twelve years. ACM Comput. Surv., 44, 41 pages.

Blazhenkova, O. and Kozhevnikov, M. (2009). The new object-spatial-verbal cognitive style model: theory and measurement. Appl. Cogn. Psychol., 23, 638–663.

Brusilovsky, P., Kobsa, A. and Nejdl, W. (2007). The Adaptive Web: Methods and Strategies of Web Personalization. Springer, Berlin, Heidelberg.

Chen, S. and Liu, X. (2008). An integrated approach for modeling learning patterns of students in Web-Based instruction: a cognitive style perspective. ACM Trans. Comput.-Hum. Interact., 15, 1–28.

Chiang, H. and Chiasson, S. (2013). Improving User Authentication on Mobile Devices: A Touchscreen Graphical Password. In Proc.

ACM MobileHCI 2013, pp. 251–260. ACM Press, New York, NY, USA.

Chowdhury, S., Poet, R. and Mackenzie, L. (2013). A Comprehensive Study of the Usability of Multiple Graphical Passwords. In Proc. IFIP INTERACT 2013, pp. 424–441. Springer, Berlin, Heidelberg.

Cranor, L. and Garfinkel, S. (2005). Security and Usability. O'Reilly Media, Inc.

De Luca, A., Denzel, M. and Hussmann, H. (2009). Look into My Eyes!: Can You Guess My Password?. In Proc. ACM SOUPS 2009, Article 7, 12 pages. ACM Press, New York, NY, USA.

De Luca, A., Hang, A., Brudy, F., Lindner, C. and Hussmann, H. (2013a). Touch Me Once and I Know It's You! Implicit Authentication Based on Touch Screen Patterns. In Proc. ACM CHI 2012, pp. 987–996. ACM Press, New York, NY, USA.

De Luca, A., von Zezschwitz, E., Nguyen, N., Maurer, M., Rubegni, E., Scipioni, M. and Langheinrich, M. (2013b). Back-of-Device Authentication on Smartphones. In Proc. ACM CHI 2013, pp. 2389–2398. ACM Press, New York, NY, USA.

Fidas, C., Voyiatzis, A. and Avouris, N. (2011). On the Necessity of User-Friendly CAPTCHA. In Proc. ACM CHI 2011, pp. 2623–2626. ACM Press, New York, NY, USA.

Florencio, D. and Herley, C.A. (2007). Large-Scale Study of Web Password Habits. In Proc. ACM WWW 2007, pp. 657–666. ACM Press, New York, NY, USA.

Ghinea, G. and Chen, S.Y. (2008). Measuring quality of perception in distributed multimedia: Verbalizers vs. imagers. Comput. Hum. Behav., 24, 1317–1329.

Inglesant, P. and Sasse, A. (2010). The True Cost of Unusable Password Policies: Password Use in The Wild. In Proc. ACM CHI 2010, pp. 383–392. ACM Press, New York, NY, USA.

Jakobsson, M., Shi, E., Golle, P. and Chow, R. (2009). Implicit Authentication for Mobile Devices. In Proc. USENIX HotSec 2009, pp. 9–9. USENIX Association, Berkeley, CA, USA.

Kinley, K., Tjondronegoro, D. and Partridge, H. (2010). Web Searching Interaction Model Based on User Cognitive Styles. In Proc. ACM OZCHI 2010, pp. 340–343. ACM Press, New York, NY, USA.

Kozhevnikov, M. (2007). Cognitive styles in the context of modern psychology: toward an integrated framework of cognitive style. Psychol. Bull., 133, 464–481.

Laing, M. (2001). Teaching learning and learning teaching: an introduction to learning styles. New Front. Educ., 31, 463–475.

Liu, Y. and Ginther, D. (1999). Cognitive styles and distance education. J. Dist. Learn. Admin., 2, Article 5.

Ma, Y., Feng, J., Kumin, L. and Lazar, J. (2013). Investigating user behavior for authentication methods: a comparison between individuals with Down syndrome and neurotypical users. ACM Trans. Access. Comput., 4, article 15, 27 pages.

McAvinue, L.P., Robertson, I.H. (2007). Measuring visual imagery ability: a review. Imagin. Cogn. Pers., 26, 191–211.

Mihajlov, M. and Jerman-Blazic, B. (2011). On designing usable and secure recognition-based graphical authentication mechanisms. Interact. Comput., 23(6), 582–593.

Nelson, D.L., Reed, U.S. and Walling, J.R. (1976). Pictorial superiority effect. Exp. Psychol. Hum. Learn. Memory, 2, 523–528.

Nicholson, J., Coventry, L. and Briggs, P. (2013). Age-Related Performance Issues for Pin and Face-Based Authentication Systems. In Proc. ACM CHI 2013, pp. 323–332. ACM Press, New York, NY, USA.

Oates, J.M. and Reder, L.M. (2010). 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, pp. 447–462. Psychological Press.

Paivio, A. and Csapo, K. (1973). Picture superiority in free recall: imagery or dual coding? Cognitive Psychol., 5, 176–206.

Paivio, A. (2006). Mind and Its Evolution: A Dual Coding Theoretical Approach. Lawrence Erlbaum Associates, Mahwah, NJ.

Peterson, E., Deary, I. and Austin, E. (2005). A new reliable measure of verbal–imagery cognitive style. Pers. Indiv. Differ., 38, 1269–1281.

Riding, R. (1991). Cognitive Style Analysis—Research Administration. Learning and Training Technology, Birmingham, UK.

Riding, R. and Cheema, I. (1991). Cognitive styles—an overview and integration. Educ. Psychol., 11, 193–215.

Sae-Bae, N., Ahmed, K., Isbister, K. and Memon, N. (2012) Biometric-Rich Gestures: A Novel Approach to Authentication on Multi-Touch Devices. In Proc. ACM CHI 2012, pp. 977–986. ACM Press, New York, NY, USA.

Schaie, W. (2013). Developmental Influences on Adult Intelligence: The Seattle Longitudinal Study (2nd edn). Oxford University Press, New York, NY.

Shirali-Shahreza, S., Penn, G., Balakrishnan, R. and Ganjali, Y. (2013). SeeSay and HearSay CAPTCHA for Mobile Interaction. In Proc. ACM CHI 2013, pp. 2147–2156. ACM Press, New York, NY, USA.

Sternberg, R.J. (1997). Thinking Styles. Cambridge University Press, New York.

Tamviruzzaman, M., Ahamed, S.I., Hasan, C.S. and O'brien, C. (2009). ePet: When Cellular Phone Learns to Recognize Its Owner. In Proc. ACM SafeConfig Workshop 2009, pp. 13–18. ACM Press, New York, NY, USA.

Verma, P. (2012) icAuth: Image-Color Based Authentication System. In Proc. ACM IUI 2012, pp. 329–330. ACM Press, New York, NY, USA.

von Ahn, L., Blum, M. and Langford, J. (2004). Telling humans and computers apart automatically. Commun. ACM, 47, 56–60.

Witkin, H.A., Moore, C.A., Goodenough, D.R. and Cox, P.W. (1977). Field-dependent and field-independent cognitive styles and their educational implications. Educ. Res., 47, 1–64.

Wu, X. *et al*. (2007). Top 10 algorithms in data mining. Knowl. Infor. Syst., 14, 1–37.

Zhang, J., Luo, X., Akkaladevi, S. and Ziegelmayer, J. (2009). Improving multiple-password recall: an empirical study. Infor. Secur., 18, 165–176.

APPENDIX

Algorithm #1: Data processing of responses for a single user

Input : A set of correct responses (seconds) to the verbal stimuli $t = \{t_1, t_2, \ldots, t_m\}$ and a set of correct responses (seconds) to the visual stimuli $v = \{v_1, v_2, \ldots, v_n\}$, where m and n are the total number of correct answers to the stimuli of each set, respectively

Output : Cognitive style ratio of the user—cs

```
1:  procedure Calculate_Cognitive_Style_Ratio(t, v)
2:      sum_t = 0; sum_v = 0;
3:      for i := 1 to m do begin
4:          sum_t += t_i;
5:      end for
6:      for i := 1 to n do begin
7:          sum_v += t_i;
8:      end for
9:      avg_t = sum_t / m;
10:     avg_v = sum_v / n;
11:     cs = avg_t / avg_v;
12: end procedure
```

Algorithm #2: Modified K-means clustering

Input : A set of users' cognitive style ratios obtained from the psychometric tests $cs = \{cs_1, cs_2, \ldots, cs_n\}$, a set of cluster centres (cognitive style ratios) $v = \{v_1, v_2, \ldots, v_k\}$ and $k = 2$ the total number of clusters to create (Verbal and Imager clusters)

Output : A set of $clusters = \{c_1, c_2, \ldots, c_k\}$

```
1:  procedure Cluster_Users(cs, v, k)
2:      v_1 = min(cs); v_2 = max(cs);
3:      Do
4:          reiterate = false;
5:          for i := 1 to n do begin
6:              if (|cs_i − v_1| > |cs_i − v_2|) then
7:                  if (cs_i ∈ c_1) then
8:                      remove_from_cluster(cs_i, c_1);
9:                      assign_to_cluster(cs_i, c_2);
10:                     reiterate = true;
11:                 end if
12:             else
13:                 if (cs_i ∈ c_2) then
14:                     remove_from_cluster(cs_i, c_2);
15:                     assign_to_cluster(cs_i, c_1);
16:                     reiterate = true;
17:                 end if
18:             end if
19:         end for
20:         for i := 1 to k do begin
21:             x = count(c_i);
22:             sum = 0;
23:             for j := 1 to x do begin
24:                 sum += c_i[j];
25:             end for
26:             v_i = sum/x;
27:         end for
28:     while (reiterate);
29: end procedure
```