A Personalization Method based on Human Factors for Improving Usability of User Authentication Tasks

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

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

Abstract. Aiming to ensure safety of operation to application providers and improve the usability of human computer interactions during authentication, this paper proposes a two-step personalization approach of user authentication tasks based on individual differences in cognitive processing as follows: i) recommend a textual or graphical user authentication mechanism based on the users' cognitive styles of processing textual and graphical information, and ii) recommend a standard or enhanced authentication key strength policy considering the users' cognitive processing abilities. The proposed approach has been applied in a four month ecological valid user study in which 137 participants interacted with a personalized user authentication mechanism and policy based on their cognitive characteristics. Initial results indicate that personalizing the user authentication task based on human cognitive factors could provide a viable solution for balancing the security and usability of authentication mechanisms at the benefit of both application providers and end-users.

Keywords: Individual Differences, Cognitive Styles, Cognitive Processing Abilities, User Authentication, Efficiency, Effectiveness, User Study

1 Introduction

User authentication tasks are performed daily by millions of users to access critical information and services on the World Wide Web. A high number of research works have been proposed aiming to improve the usability and memorability of user authentication mechanisms, and at the same time decrease guessing attacks by malicious software and users [1, 2]. Researchers promote various designs of authentication mechanisms based on text and pictures, biometrics and gestures, password managers and policies [2, 3].

Nevertheless, recent studies have shown that the same security and usability issues of user authentication mechanisms still exist [1, 4]. For example, an increasing number of minimum alphanumeric characters (with a combination of upper-case and low-

er-case letters and special characters) are required by password policies to be entered by users, which hinder the memorability and usability of passwords. On the other hand, users proceed with work-around methodologies to support the memorability of their password key, such as writing down their password, using the same password key for multiple accounts, and thus decreasing the system's security.

Despite the fact that a very high number of user authentication mechanisms have been proposed over the last decade, the majority of today's systems still utilize text-based passwords as their sole means of authentication [4]. The same textual password mechanism and the same password key strength policy is provided to all users, without considering that users do not share common characteristics, cognitive abilities and preferences. In this realm, motivated by theories on individual differences, suggesting that individuals have different cognitive processing abilities and habitual approaches in processing verbal and graphical information, this paper proposes a two-step personalization approach of user authentication tasks based on individual differences in cognitive processing as follows: i) recommend a textual or graphical user authentication mechanism based on the users' cognitive styles of processing textual and graphical information, and ii) provide a personalized authentication key strength policy; standard or enhanced complexity, considering the users' cognitive processing abilities. The proposed approach has been applied in a user study of 137 participants interacting with a personalized user authentication mechanism and policy based on their cognitive processing characteristics.

2 Theoretical Background

2.1 User Authentication

A typical user authentication scenario requires from a legitimate user to provide specific information, used to prove identity or gain access to a resource. User authentication mechanisms consist of three main categories depending on the factors used for authentication: *knowledge-based* require from users to memorize specific information (e.g., password, passphrase, PIN code, sequence of images, etc.) to gain access to a resource, *token-based* require from users to provide a physical object (e.g., credit card) for authentication, and *biometric-based* require from users to reveal their identity based on biometrics (e.g., fingerprint, eye-gaze).

Knowledge-based user authentication mechanisms are currently the most popular mechanisms for authentication, primarily because they are very fast and less expensive to implement compared to token-based and biometric-based mechanisms that require additional hardware and development costs [2]. Researchers have proposed various approaches to improve usability and memorability, such as improving existing recall-based password approaches with recognition of text [5] and enforcing the creation of secure authentication keys through policies [6, 1]. Researchers also promote alternative designs of authentication mechanisms based on images that require users to recall and select pictures as their authentication key [2, 3].

2.2 Individual Differences in Cognitive Processing

Theories of individual differences in cognitive processing aim to describe and explain how individuals differ in cognitive processing abilities and styles. A number of researchers have focused on high-level cognitive processes such as *cognitive styles*, which explain empirically observed differences in mental representation and processing of information [9]. A particularly important cognitive style is the Verbal/Imager dimension that refers to how individuals process information and indicates their preference for representing information verbally, or in mental pictures [9]. *Verbals* prefer and perform more efficiently when hypermedia content is presented in the form of text and are better at recalling acoustically complex text. *Imagers* prefer and perform efficiently when the hypermedia content is provided in a graphical representation.

Various researchers also attempted to explain the functioning of the human mind in terms of more elementary cognitive processes. These include the *speed of processing*, which refers to the maximum speed a given mental act may be efficiently executed [7]; *controlled attention*, which refers to cognitive processes to identify and concentrate on goal-relevant information and inhibit attention to irrelevant stimuli [7]; and *working memory capacity*, which is defined as the maximum amount of information the mind can efficiently activate during information processing [8].

3 Motivation and Research Question

Based on the theoretical background, we suggest that the user authentication type (textual or graphical) might affect differently, in terms of performance, individuals that have a particular style of representing and processing information (verbally or visually). In the same line, the added cognitive effort that arises from password policies (e.g., that require users to memorize combinations of upper-case, lower-case, and special characters) might differently affect users with limited or enhanced cognitive processing abilities which are based on the elementary processes of the human mind.

Nowadays, textual passwords are provided to all users neglecting the fact that users might have particular cognitive styles toward processing and representing information in mental pictures (Imagers) and thus might benefit through a different authentication scheme. In addition, the same password policy is provided to all users without considering that users might have limited cognitive processing abilities and will be negatively affected by the added cognitive effort of applying the password policy.

To this end, we suggest that cognitive styles might affect the type of user authentication (textual or graphical), and cognitive processing abilities might affect user performance with different strength levels of authentication policies. In this context, the goal of this work is to improve the usability of user authentication tasks by recommending the "best-fit" user authentication type and policy to users with different cognitive styles and cognitive processing abilities. The following research question is investigated: *Does matching the user authentication type (textual or graphical) and policy (standard or enhanced) to users' cognitive styles and cognitive processing abilities improve task efficiency and effectiveness?*

4 Personalized User Authentication based on Individual Differences in Cognitive Processing

This section presents the main components of the proposed personalized user authentication mechanism. It consists of three main layers; *the user modelling layer*, *the adaptation layer*, and *the user interface layer*.

4.1 User Modelling Layer

The user modelling layer entails the following phases: *user data collection*, *data processing* and *cluster analysis* for eliciting the users' cognitive styles (Verbal or Imager) and cognitive processing abilities (limited or enhanced), that are respectively related to a specific type of authentication (textual or graphical) and policy (standard or enhanced).

User Data Collection. Collecting data of users is the initial step for adapting and personalizing the user authentication task. Cognitive styles and cognitive processing abilities are considered the main factors in this work for personalizing the user authentication task. For eliciting the users' cognitive styles, Riding's Cognitive Style Analysis test (CSA) [9] was utilized that highlights individual differences in verbal or mental representation of information. An individuals' cognitive style is obtained by presenting a series of questions about conceptual category (e.g., *"Are ski and cricket the same type?"*) and appearance (e.g., *"Are cream and paper the same color?"*) to be judged by the users to be true or false. It is assumed that Verbals respond faster than Imagers in the conceptual types of stimuli, whereas Imagers respond faster than Verbals in the appearance statements. The response time and the given answer for each stimulus is recorded and provided to the next phase for data processing.

For eliciting the speed of processing and controlled attention of users, two Stroop-like tasks are used to measure simple choice reaction time of users [7]. The first task requires users to read words denoting a color written in the same or different ink color (e.g., the word "red" written in red ink color), while the second task requires users to recognize the ink color of words denoting a color different than the ink (e.g., the word "green" written in blue ink). The response time and the given answer for each stimulus is recorded and provided to the next phase for data processing. Furthermore, to elicit the users' working memory capacity, a psychometric test was developed that illustrates a series of geometric figures on the screen in which users are required to memorize the figure and then select the same figure among five similar figures. The total number of correct responses indicates the capacity level of working memory that is also provided to the data processing phase.

Data Processing. In this phase, all the users' responses to the psychometric tests are cleaned from invalid responses and inconsistencies are resolved in order to be used as input to the next phase of cluster analysis. During the first step of data processing, all users' responses to the psychometric tests are examined, and outliers are removed

from the dataset. For example, in the case were users remain idle during a stimulus, data about that particular stimulus are removed from the dataset.

Responses of the cognitive style test are processed as follows: the average response time of all valid and correct responses is calculated on each of the two question types (conceptual and appearance) of the psychometric test, and then the ratio between the average response times on the verbal and imagery stimuli is calculated. It is assumed that users with a low ratio are considered Verbals, while users with a high ratio are Imagers.

For the three cognitive processing abilities' tests, a normalization by *Z*-score is conducted on the raw data, since speed of processing and controlled attention measure speed (average in seconds), whereas working memory measures capacity (total of correct responses). The pseudo code for eliciting the cognitive processing abilities is illustrated in Algorithm #1.

Algorithm #1 : Calculate Cognitive Processing Abilities

Input : A set of all users' average response times to the speed of processing test $s = \{ s_1, s_2, ..., t_m \}$, a set of all users' average response times to the controlled attention test $c = \{ c_1, c_2, ..., c_m \}$, and a set of all users' total correct responses to the working memory test $w = \{ w_1, w_2, ..., w_m \}$ where m the total number of users

Output : Cognitive Processing Ability – z

```
1:    procedure Calculate_Cognitive_Processing_Ability(s, c, w)
2:        for i := 1 to m do begin
3:            sop = ( s_i - mean(s) ) / stddev(s);
4:            ca = ( c_i - mean(c) ) / stddev(c);
5:            wmc = ( -1 ) * ( w_i - mean(w) ) / stddev(w);
6:            z_i = ( sop + ca + wmc ) / 3;
7:        end for
8:    end procedure
```

The final *z*-value indicates a user's cognitive processing ability, with a low value indicating an enhanced cognitive processing ability of that user, and a high value indicating a limited cognitive processing ability of that user.

Cluster Analysis. In order to elicit the users' cognitive styles and cognitive processing abilities, cluster analysis is performed to the users' cognitive style ratios and the *z*-values that were calculated in the previous phase, with the aim 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 calculated ratios and *z*-values. Accordingly, in the case of cognitive styles, users having a small value of ratio are grouped as Verbals and users having a large value of ratio are grouped as Imagers. In the case of cognitive processing abilities, small values of *z* are grouped as users having enhanced cognitive processing abilities and large values of *z* are grouped as users having limited cognitive processing abilities.

We utilized the *k*-means clustering algorithm since it is considered one of the most robust and efficient clustering algorithms [10]. 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 or Imager, and limited or enhanced cognitive processing), the algorithm is set to $k = 2$ in both cases. The algorithm initially sets the data point with the smallest value as the first cluster center (Verbal cluster and enhanced cognitive ability cluster) and the data point with the largest value as the second cluster center (Imager cluster and limited cognitive ability cluster). The distance between all other data points and cluster centers is then calculated, and each data point is assigned to the cluster whose distance from the cluster center is minimum of all the cluster centers using the Euclidian distance. New cluster centers are recalculated by measuring the mean of all data points of each cluster. Next, the distances between each data point and newly obtained cluster centers are recalculated in an iterative approach until no data point is reassigned.

4.2 Adaptation Layer

In this layer, based on the user modelling results, a two-step rule-based mechanism is applied to recommend a specific type of authentication and policy as illustrated in Algorithm #2. The applied rules are based on previous studies conducted which revealed an effect of users' cognitive styles and cognitive processing abilities on preference and performance of text-based and graphical user authentication mechanisms [11, 12].

Algorithm #2 : User Authentication Recommendation for a Single User

Input : Cluster group of cognitive styles *vi = { verbal | imager },* cluster group of cognitive processing abilities *cp = { limited | enhanced }*

Output : User authentication type *ua = { textual | graphical },* and authentication policy *p = { standard | enhanced }*

```
1:    procedure Recommendation(vi, cp)
2:        if (vi == verbal) then
3:            ua = textual;
4:        else if (vi == imager) then
5:            ua = graphical;
6:        end if
7:        if (cp == limited) then
8:            p = standard;
9:        else if (cp == enhanced) then
10:           p = enhanced;
12:       end if
13:   end procedure
```

During the first step of personalization, the mechanism recommends a textual password mechanism to Verbals, and a graphical authentication mechanism to Imagers since each type of authentication is best matched to the habitual approach of users' cognitive styles. In the second step, users with limited cognitive processing abilities are provided with a standard policy, whereas users with enhanced cognitive

processing abilities are provided with an enhanced policy. A standard policy in the case of text-based password is considered a password that consists of eight alphanumeric characters, combination of upper-case and lower-case letters and special characters, whereas an enhanced policy needs a minimum of ten characters, entailing the same restrictions as the standard policy. In the case of graphical authentication mechanism, a standard and an enhanced policy respectively requires users to enter eight and ten images as their authentication key.

4.3 User Interface Layer

In this layer, depending on the decision made in the previous phase, either a textual password or graphical authentication mechanism is communicated to the user interface. The two user authentication mechanisms are described next.

Text-based Password Mechanism. A standard text-based password mechanism was utilized in which users can enter alphanumeric and special keyboard characters. A minimum of eight or ten characters (depending on the policy) including numbers, a mixture of lower-case 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.

Graphical Authentication Mechanism. A graphical authentication mechanism that involves single-object images was developed based on the recognition-based, graphical authentication mechanism proposed in [3]. During the authentication key creation, users can freely select a minimum of eight or ten images (depending on the policy), in a specific sequence out of a random subset of thirty images that are retrieved from a large image database. After the graphical authentication key is created, a fixed image set of sixteen images, containing the user-selected authentication images and system-selected decoy images are permanently attached to the username in order to increase security. During authentication, a four by four grid containing the user-selected and system-selected decoy images are presented. 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 authentication key creation process for accessing the system.

From a security point of view, text-based passwords and graphical authentication mechanisms provide similar security protection levels if they are encrypted properly on the service provider database layer and submitted securely on the transmission layer [2, 3]. Accordingly, aiming to defend against guessing attacks based on transmission sniffers, and brute force attacks at the database level, a cryptographic hash function is utilized in both authentication mechanisms that encrypts the given authentication key and transmits it through a secure channel (https), and stored in an encrypted format in the database. Furthermore, text-based and graphical authentication mechanisms entail similar threats with regard to guessing attacks on the client's side. Regarding capturing attacks (e.g., malware, phishing attacks, etc.), graphical authentication mechanisms are more immune than text-based passwords since additional spy-

ing software is needed to capture the screen as the user types. On the other hand, graphical authentication mechanisms are more vulnerable to shoulder surfing attacks and social engineering since the nature of the images used (single-object images) allows being easily described and thus easier to share with other users.

5 Experimental Evaluation

In this section we present and discuss our observations and experiences of applying the personalized user authentication mechanism in the frame of a four month ecological valid user study in which users interacted with personalized user authentication mechanisms based on their cognitive styles and cognitive processing abilities.

5.1 Sampling and Procedure

A total of 137 individuals participated in the study (54 males, 83 females, age 17-22) during September and December 2013, and were undergraduate students of Psychology and Social Science Departments. A Web-based system was applied within the frame of university courses. The user enrolment process was divided into two phases: i) participants were required to provide their demographic information (i.e., email, age, gender, and department) and interact with the developed online psychometric tests for eliciting their cognitive styles and cognitive processing abilities, ii) and participants created their authentication key that was used for accessing the courses' material (i.e., course slides, homework exercises) and for viewing their grades. During each course enrolment process, the personalization mechanism recommended a specific type of authentication (text-based password or graphical authentication mechanism) and authentication policy (standard or enhanced) based on the cluster each user was assigned according to the user modelling and adaptation process.

In order to investigate the added value of personalizing the user authentication task based on the users' cognitive styles and cognitive processing abilities, a matched and a mismatched condition was randomly assigned to the decision rules aiming to divide the sample into two groups; the one group being assigned a personalized user authentication mechanism (the matched condition that entailed the recommended user authentication mechanism), and the other group being assigned with a non-personalized user authentication mechanism (the mismatched condition that entailed the opposite type of user authentication to the one suggested by the system). The allocation was based on the users' cognitive characteristics so that the conditions were balanced across all user groups. Participants were not aware whether they were receiving a personalized or a non-personalized authentication mechanism.

Client-side and server-side scripts were developed to monitor the users' behaviour during interaction with the user authentication mechanism. In particular, the total time required for successful authentication (task efficiency) was recorded from the time users entered their username for identification, until they successfully completed the authentication process, as well as the total attempts required for successful authentication for each session (task effectiveness).

5.2 Hypotheses

The following hypotheses were formulated:

H1. The time needed (efficiency) to successfully authenticate through a personalized user authentication mechanism is reduced compared to a non-personalized mechanism.

H2. The total number of attempts (effectiveness) to successfully authenticate through a personalized user authentication mechanism is reduced compared to a non-personalized mechanism.

5.3 Analysis of Results

Clustering Results. The cluster analysis of the user modelling mechanism separated users into clusters based on their cognitive style ratios and cognitive processing *z*-values (Table 1). The main goal of the clustering algorithm was to minimize variability within the clusters and maximize variability between the clusters based on the ratios and *z*-values. The evaluation was focused on how similar the ratio and *z*-value of a particular user is to another user of the same cluster, and how different the ratio and *z*-value of users in clusters from the ones of the other cluster.

Table 1. Descriptive statistics of the ratios and *z*-values in each cluster.

Cognitive Styles				**Cognitive Processing Abilities**			
Cluster 1 (Verbals)		**Cluster 2 (Imagers)**		**Cluster 1 (Enhanced)**		**Cluster 1 (Limited)**	
Mean (SD)	**N**	**Mean (SD)**	**N**	**Mean (SD)**	**N**	**Mean (SD)**	**N**
0.84 (0.13)	77	1.25 (0.09)	60	-0.93 (0.56)	89	1.04 (0.49)	48

Two independent-samples t-tests were conducted to determine mean differences on the cognitive style ratios between the generated cluster groups (Verbal/Imager) as well as the mean differences on the cognitive processing abilities *z*-values between the enhanced and limited cognitive processing cluster groups. Homogeneity of variances was violated in the case of cognitive styles, as assessed by Levene's test for equality of variances (cognitive styles: p=0.032; cognitive processing abilities: p=0.216). In this respect a Welch t-test was conducted for unequal variances of data.

Results indicated that there were significant differences among cognitive style ratios and among *z*-values between the clusters (cognitive styles: $t(128.892)=-20.694$, $p<0.001$; cognitive processing abilities: $t(135)=-20.193$, $p<0.001$), indicating that the user modelling procedure grouped the users into different clusters effectively, and could be thus safely used in the main data analysis.

User Authentication Efficiency. An independent-samples t-test was used to determine mean differences on the time needed to solve the personalized and non-personalized user authentication mechanism. Accordingly, if cognitive styles and cognitive processing abilities are of any importance, these two groups should have statistically significant different scores.

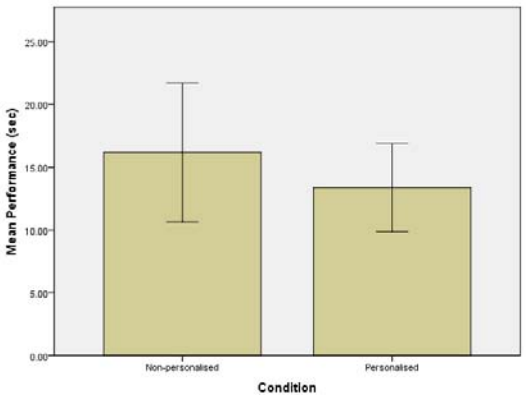

Fig. 1. Means of performances per condition.

Data were normally distributed for both personalized and non-personalized data, as assessed by visual inspection of Normal Q-Q Plots. The assumption of homogeneity of variances was violated, as assessed by Levene's test for equality of variances (p=0.001). In this respect a Welch t-test was conducted that can accommodate unequal variances of data.

The analysis revealed that interactions with personalized user authentication mechanisms were more efficient (M=13.39, SD=1.75) than non-personalized user authentication mechanisms (M=16.19, SD=2.77). These results were statistically significant (t(2028.138)=-29.996, p=0.03). Figure 1 illustrates the means of performances of each condition. Accordingly, the results indicate that individual differences in cognitive processing could be a determinant factor on the adaptation of user authentication mechanisms as they improve task completion efficiency and supports Hypothesis #1.

User Authentication Effectiveness. Effectiveness was measured by the total number of attempts made for successfully authenticating in each condition. A Mann-Whitney U test was run to determine if there were differences in total attempts between the personalized and the non-personalized condition. Distributions of these attempts were not similar, as assessed by visual inspection (Figure 2). Total attempts for personalized user authentication interactions (*mean rank* = 1031.92) were significantly less compared to non-personalized user authentication interactions (*mean rank* = 1452.27) indicating that the personalized user authentication interactions improved task effectiveness, supporting Hypothesis #2. These results were statistically significantly different (U=517699, z=-14.898, p=0.01).

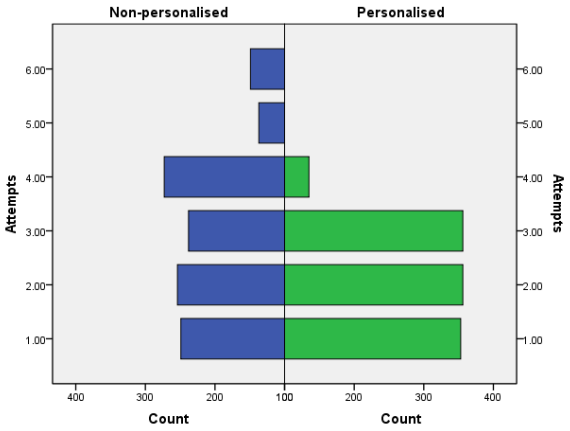

Fig. 2. Total attempts to successfully authenticate in each condition.

6 Conclusions

The paper proposed a personalization approach for supporting the design and deployment of usable and secure user authentication tasks, driven primarily by the need to define more effective and efficient user-centered design techniques related to such tasks. The proposed approach was realized in a prototype Web-based system that provided personalized user authentication mechanisms based on individual differences in cognitive styles and cognitive processing abilities.

Our research revealed that personalizing the user authentication type (textual or graphical) and authentication policy to users' cognitive styles and cognitive processing abilities improves task performance, both in terms of task efficiency and effectiveness. These findings are consistent with previous studies that revealed an effect of human cognitive factors on task efficiency and effectiveness of user authentication [11, 12], and translating these findings into adaptation rules was at some extent successful. Limitations of the study include the limited sample size and participants of non-varying profiles (e.g., undergraduate students and age). In this context, bearing in mind that cognitive processing characteristics of users change and decline over time, the suggested approach could have stronger effects on older adults [13]. Although it is interesting and promising that results yielded statistical significant results, further studies need to be conducted in order to reach to more concrete conclusions about the added value and the effects of personalizing user authentication tasks based on individual differences in cognitive processing.

Acknowledgements. The work is co-funded by the PersonaWeb project under the Cyprus Research Promotion Foundation (ΤΠΕ/ΠΛΗΡΟ/0311(ΒΙΕ)/10), and the EU projects SocialRobot (285870) and Miraculous-Life (611421).

7 References

1. Inglesant, P., Sasse, A.: The True Cost of Unusable Password Policies: Password use in the Wild. In: ACM SIGCHI International Conference on Human Factors in Computing Systems, pp. 383-392. ACM Press, New York, NY (2010)
2. Biddle, R., Chiasson, S., van Oorschot, P.: Graphical Passwords: Learning from the First Twelve Years. J. ACM Computing Surveys, 44, 4, Article 19 (2012)
3. Mihajlov, M., Jerman-Blazic, B.: On Designing Usable and Secure Recognition-based Graphical Authentication Mechanisms. J. Interacting with Computers 23, 6, 582-593 (2011)
4. Zhang, J., Luo, X., Akkaladevi, S., Ziegelmayer, J.: Improving Multiple-password Recall: An Empirical Study. J. Information Security 18, 2, 165-176 (2009)
5. 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)
6. 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)
7. Stroop, J.R. Studies of Interference in Serial Verbal Reactions. J. Experimental Psychology 18, 643-662 (1935)
8. Baddeley, A.: Working Memory: Theories, Models, and Controversies. J. Annual Review of Psychology 63, 1-29 (2012)
9. Riding, R., Cheema, I.: Cognitive Styles – An Overview and Integration. J. Educational Psychology 11(3-4), 193-215 (1991)
10. Wu, X., Kumar, V., Quinlan, J., Ghosh, J., Yang, Q., Motoda, H., McLachlan, G., Ng, A., Liu, B., Yu, P., Zhou, Z., Steinbach, M., Hand, D., Steinberg, D.: Top 10 Algorithms in Data Mining. J. Knowledge Information Systems, 14, 1, 1-37 (2007)
11. Belk, M., Fidas, C., Germanakos, P., Samaras, G.: Security for Diversity: Studying the Effects of Verbal and Imagery Processes on User Authentication Mechanisms. In: IFIP TC13 Conference on Human-Computer Interaction, pp. 442-459. Springer, Heidelberg (2013)
12. Belk, M., Germanakos, P., Fidas, C., Samaras, G.: Studying the Effect of Human Cognition on User Authentication Tasks. In: International Conference on User Modeling, Adaptation, and Personalization, pp. 102-113, Springer, Heidelberg (2013)
13. Schaie, W.: Developmental Influences on Adult Intelligence: The Seattle Longitudinal Study (2nd ed.), New York, NY: Oxford University Press (2013)