Studying the Effect of Human Cognition on User Authentication Tasks

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

[1]Department of Computer Science, University of Cyprus, CY-1678 Nicosia, Cyprus
[2]SAP AG, Dietmar-Hopp-Allee 16, 69190 Walldorf, Germany
{belk,pgerman,christos.fidas,cssamara}@cs.ucy.ac.cy

Abstract. This paper studies the effect of individual differences in human cognition on user performance in authentication tasks. In particular, a text-based password and a recognition-based graphical authentication mechanism were deployed in the frame of an ecological valid experimental design, to investigate the effect of individuals' different cognitive processing abilities toward efficiency and effectiveness of user authentication tasks. A total of 107 users participated in the reported study during a three-month period between September and November 2012. The results of this recent study can be interpreted under the light of human information processing as they demonstrate a main effect of users' cognitive processing abilities on both efficiency and effectiveness related to authentication mechanisms. The main findings can be considered valuable for future deployment of adaptive security mechanisms since it has been initially shown that specific cognitive characteristics of users could be a determinant factor for the adaptation of security mechanisms.

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

1 Introduction

Over the last decade, the World Wide Web has ingrained itself into everyday life and has contributed to the exponential increase of internet usage since the late 1990s. Its fundamental concept as a medium for collaboration and sharing of information has generated extensive enthusiasm driving many of the world's markets. Within this realm, there is an increasing demand to provide usable and secure interactions to users in various application domains like e-government, e-health, e-learning, e-banking, etc. One of the most important security concerns of Web application providers is to protect their systems from unauthorized access, primarily through user authentication. User authentication over the Internet is primarily achieved with the use of text-based passwords and some suggest that passwords will remain the main means of authentication for the following years [1]. It is estimated that more than 80% of US and UK companies apply some form of text-based password authentication; in many cases it is their solely method for user authentication [2].

Password mechanisms have two main requirements; they need to meet high security standards for keeping malicious users from accessing system accounts, and they need to meet usability standards and provide effective and efficient user interactions. Both are important, and every authentication mechanism is a balancing act between the two [3, 4]. For example, as the password strength increases, its memorability, and thus usability decreases, and vice versa.

The security and usability shortcomings of passwords are many and well-known. For example, passwords are vulnerable to guessing, brute-forcing, and more recently to phishing and keystroke logging, and are typically difficult to remember [5, 1]. The latter is further strengthened with the increasing computational power of today's information systems, by demanding the usage of complex and hard-to-guess passwords. In this context, research on graphical authentication mechanisms has received significant attention lately (see [6] for a recent review) with the aim to improve user memorability, and at the same time decrease guessing attacks by malicious software and users. In graphical authentication mechanisms, human memory is leveraged for visual information in hope of a reduced memory burden that will facilitate the selection and use of more secure authentication keys [6]. Graphical authentication mechanisms principally require from a user to enter an authentication key represented by images in a specific sequence. Examples include among others Draw-a-Secret [7] which is one of the first graphical authentication mechanisms proposed, that requires users to draw their authentication key on a two dimensional grid, Pass-Go [8], where users draw their authentication key using grid intersection points, Gaze-based authentication [9] that supports users in selecting secure gaze-based graphical authentication keys, Passfaces [10] that requires from the user to create an authentication key by selecting and memorizing specific images that illustrate human faces, and then recognize the images among decoys to authenticate, and similarly to Passfaces, ImagePass [11] that utilizes single-object images as the authentication key, instead of human faces, since their study suggested that single-object images are more memorable than abstract images and images that illustrate human faces.

A variety of studies have been reported that underpin the necessity for increasing usability in user authentication mechanisms. An early study in [12], which investigated password memorability of users, underpinned the necessity of usable passwords since results from the study indicated that choosing secure passwords that are memorable has been proven to be a difficult task for many users. Furthermore, a large-scale study of half a million users, which investigated the usage habits of user authentication, supports the need of memorable and secure authentication keys [13]. A more recent study in [14] that investigated the impact of authentication policies on users' productivity and experience, suggested that security policies should be driven by the users' needs helping them to set stronger authentication keys instead of focusing on maximizing their strength.

In this context, ineffective practice of usability in user authentication, does not naturally embed the users' characteristics in the design process, and usually adopts a "one-size-fits-all" approach when concerning user authentication designs ignoring the fact that different users have different characteristics and develop different structural and functional mental models, and thus need individual scaffolding. In this respect,

supporting usability of user authentication mechanisms with user-adaptive technologies [15] is based on the promise that understanding and modeling human behavior in terms of structural and functional user requirements related to such security tasks can provide an alternative to the "one-size-fits-all" approach with the aim to improve the system's usability and provide a positive user experience.

Consequently, a first step toward designing an adaptive user authentication mechanism is to identify which individual characteristics (e.g., knowledge, previous experience, lingual characteristics, cognitive characteristics, etc.) are considered important for adapting such mechanisms. Bearing in mind that human computer interactions with regard to authentication mechanisms are in principal cognitive tasks that embrace to recall and/or recognize, process and store information, we suggest that these interactions should be analyzed in more detail under the light of human information processing. In this respect, the purpose of this paper is to investigate whether there is a main effect of specific individual characteristics targeting on cognitive processing abilities (i.e., speed of processing, controlled attention and working memory capacity), toward efficiency and effectiveness of two different types of authentication mechanisms; text-based password and graphical authentication mechanisms.

Such an endeavor is considered valuable for the design and the deployment of more usable computer human interaction processes with the aim to offer adaptive and personalized user authentication mechanisms aiming to assist users to accomplish efficiently and effectively comprehensive and usable authentication tasks. For example, an adaptive authentication mechanism could provide to users a personalized type of authentication mechanism (text-based or graphical) according to their cognitive processing abilities with the aim to improve the efficiency and effectiveness of the authentication task, and minimize users' cognitive load and erroneous interactions.

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

2 Individual Differences in Human Cognition

Human interaction with authentication mechanisms is principally an information processing task consisting of several processing stages [16]. These include perceptual processing of the initial stimulus of the authentication mechanism, cognitive processing to give meaning to this information and further retrieve the memorized authentication key from long-term memory into the working memory system for processing, and finally carrying out the action, which is, the user provides the retrieved authentication key to the authentication form for accessing the system.

Various theories of individual differences in human cognition have been developed with the aim to describe and explain how and why individuals differ in cognitive abilities [17, 18]. In this respect, various researchers attempted to explain the functioning of the human mind in terms of more basic processes, such as *speed of processing, controlled attention* and *working memory capacity* [19]. *Speed of processing* refers to

the maximum speed at which a given mental act may be efficiently executed. In order to elicit speed of processing of individuals, the response time for recognizing a simple stimulus is measured, such as, reading single words or identifying a geometrical figure. In this context, speed of processing indicates the time needed by the human mind to record and give meaning to information; individuals recognizing stimuli faster, are considered more efficient in processing [20, 21].

Controlled attention refers to cognitive processes that can identify and concentrate on goal-relevant information. A classic measure of cognitive control is the Stroop task which requires individuals to name the color in which a word has been printed, while ignoring the word itself [22]. Conflict arises when the color of the word and the word itself are incongruent, e.g., the word "blue" is printed in red color. Individuals must override the dominant aspect of the stimuli (the tendency to read a word) with the processing of their weaker but goal-relevant aspect (the recognition of ink color). In this respect, the difference between the two kinds of measures is taken as an index of inhibition, which is the basic component of controlled attention [20, 22]. People being faster indicating the color of the word tend to have more efficient controlled attention.

Working memory capacity is defined as the maximum amount of information that the mind can efficiently activate during information processing. The conception of working memory grew out of the literature on short-term memory [23, 24] as an empirical model of cognitive functions used for temporarily storing and manipulating information. Enhanced working memory increases the connections and associations that can be built either between the items of the newly encountered information or between this information and information already stored in the long-term memory.

Various research works argue that the aforementioned cognitive processes have an effect on comprehension, learning and problem solving [25, 26]. They are mainly used in mental tasks, such as arithmetic tasks; remembering a number in a multiplication problem and adding that number later on, or creating a new password and using that password later for authentication.

To this end, given that the aforementioned cognitive factors have a main effect in problem solving and other tasks (e.g., individuals with increased working memory capacity accomplish tasks more efficiently), we suggest that such characteristics should be utilized as part of an adaptive interactive system specialized in personalizing user authentication tasks to the cognitive processing abilities of each user. In this respect we further describe the results and findings of a user study that aimed to investigate whether there is a main effect of users' cognitive processing abilities, targeting on speed of processing, controlled attention and working memory capacity, on the efficiency and effectiveness of different types of authentication mechanisms.

3 Method of Study

3.1 Procedure

A Web-based environment was deployed within the frame of various university courses. Students were required to provide their demographic information during the

enrolment process (i.e., email, age, gender, and department) and create their authentication key that would be used throughout the semester for accessing the courses' material (i.e., course slides, homework) and for viewing their grades. A text-based password and a recognition-based graphical authentication mechanism were utilized as the authentication scheme of the Web-site. The type of authentication mechanism (i.e., text-based password or graphical) was randomly provided during the enrolment process. At the end of the process the sample consisted of 50% of the students having enrolled with a text-based password and 50% of the students having enrolled with a graphical authentication mechanism. In both types of authentication mechanisms, the key created was chosen freely by the user.

The text-based password mechanism (Figure 1) involved alphanumeric and special keyboard characters. A minimum of eight characters including numbers, a mixture of lower- and upper-case letters, and special characters were required to be entered by the users.

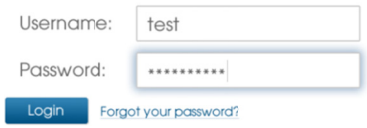

Fig. 1. A text-based password mechanism used during the study

A graphical authentication mechanism (Figure 2) that involved single-object images was developed based on the recognition-based, graphical authentication mechanism proposed in [11]. During the authentication key creation, users had to select between eight to twelve images, in a specific sequence out of a random subset of thirty images that were retrieved from a large image database. After the graphical authentication key was created, a fixed image set of sixteen images, containing the user-selected authentication images and system-selected decoy images were permanently attached to the username in order to increase security, since if the decoy images were to change every authentication session, the authentication key could be easily revealed by eliminating the non-repeated images through subsequent sessions [11]. During authentication a 4 x 4 grid containing the user-selected and system-selected decoy images were presented. Thereafter, users had to select their images in the specific sequence, as entered in the enrolment process in order to get permission for accessing the system.

Both client-side and server-side scripts were developed to monitor the users' behavior during interaction with the authentication mechanisms. In particular, the total time (efficiency) and total number of attempts (effectiveness) required for successfully authenticating were monitored on the client-side utilizing a browser-based logging facility that started recording time as soon the users provided their username, until they successfully completed the authentication process.

Controlled laboratory sessions were also conducted throughout the period of the study to elicit the users' cognitive factors (speed of processing, controlled attention and working memory capacity) through a series of psychometric tests [24, 26]. With the aim to apply the psychometric tests in a scientific right manner, we conducted

several sessions with a maximum of 5 participants by following the protocol suggested by the inventors of the psychometric tests. The psychometric tests utilized in the study are described next.

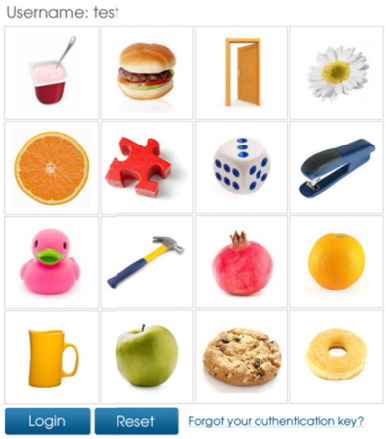

Fig. 2. A graphical authentication mechanism used during the study

Users' Speed of Processing Elicitation Test. A Stroop-like task was devised to measure simple choice reaction time to address speed of processing. Participants were instructed to read a number of words denoting a color written in the same or different ink color (e.g., the word "red" written in red ink color). A total of eighteen words were illustrated to the participant illustrating the words "red", "green" or "blue" either written in red, green or blue ink color. The participants were instructed to press the R keyboard key for the word "red", the G key for the word "green" and the B key for the word "blue". The reaction times between eighteen stimuli and responses onset were recorded and their mean and median were automatically calculated. A filter set at 5000 ms was used to exclude unreasonably slow responses, and wrong responses were also automatically excluded (as suggested in [26]).

Users' Controlled Attention Elicitation Test. Similar to the speed of processing elicitation test, a Stroop-like task was devised, but instead of denoting the word itself, participants were asked to recognize the ink color of words denoting a color different than the ink (e.g., the word "green" written in blue ink). A total of eighteen words were illustrated to the participants illustrating the words "red", "green" or "blue" either written in red, green or blue ink color. The participants were instructed to press the R keyboard key for the word written in red ink color, the G key for the word written in green ink color and the B key for the word written in blue ink color. The reaction times between eighteen stimuli and responses onset were recorded and their mean and median were automatically calculated. A filter set at 5000 ms was used to exclude unreasonably slow responses, and wrong responses were also automatically excluded (as suggested in [26]).

Users' Working Memory Capacity Elicitation Test. A visual test was utilized to indicate a user's working memory capacity based on [24]. The test illustrated a geometric figure on the screen and the participant was required to memorize the figure. Thereafter, the figure disappeared and five similar figures were illustrated on the screen, numbered from one to five. The participant was required to provide the number (utilizing the keyboard) of the corresponding figure that was the same as the initial figure. The test consisted of twenty one figures (seven levels of three trials each). As the participant correctly identified the figures of each trial, the test provided more complex figures as the levels increased indicating an enhanced working memory capacity.

3.2 Participants

The study was conducted between September and November 2012 with a total of 107 participants (52 male, 55 female, age 17-26, mean 22). Participants were undergraduate students of Computer Science, Electrical Engineering, Psychology and Social Science departments. A total of 2067 authentication sessions have been recorded during the three-month period.

3.3 Hypothesis

The following hypothesis was formulated for the purpose of our research:

H1. There is significant difference with regard to time (efficiency) and total number of attempts (effectiveness) needed to authenticate through a text-based password mechanism or a recognition-based, graphical authentication mechanism among users with different cognitive processing abilities.

3.4 Analysis of Results

For our analysis, we separated participants into different categories based on their cognitive processing abilities (limited, enhanced) of each cognitive factor (speed of processing, controlled attention, working memory capacity), which are summarized in Table 1.

Table 1. User Groups based on Cognitive Processing Abilities

	Speed of Processing		Controlled Attention		Working Memory Capacity	
	Total	**%**	**Total**	**%**	**Total**	**%**
Enhanced	73	68.2	51	47.7	69	64.5
Limited	34	31.8	56	52.3	38	35.5
Total	107	100	107	100	107	100

User Authentication Efficiency. A one-way analysis of variance (ANOVA) was conducted to examine main effects of authentication type (text-based password vs.

graphical) on the time needed to successfully authenticate. Results revealed that users in general performed significantly faster in the text-based password mechanism compared to the graphical ($F(1,1134)=192.618$, $p<0.001$). Furthermore, a series of two by two factorial analyses of variance were conducted aiming to examine main effects of users' cognitive processing differences (i.e., limited, enhanced) and user authentication type on the time needed to accomplish the authentication task. Figure 3 illustrates the means of performance per cognitive factor group in regard with the speed of processing (SP), controlled attention (CA) and working memory capacity (WMC) dimension, and user authentication type (text-based password and graphical).

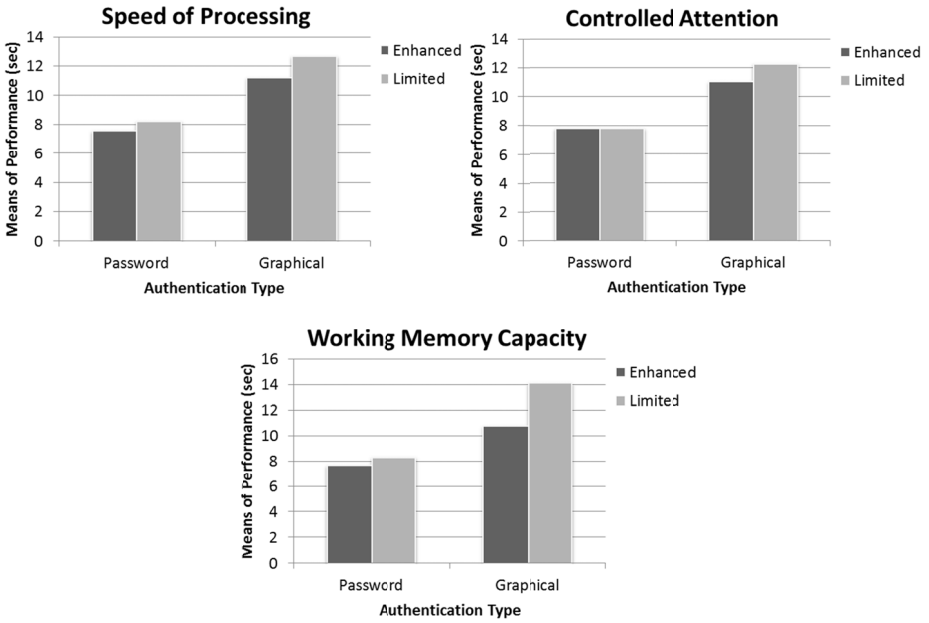

Fig. 3. Means of Performance for Speed of Processing (top left), Controlled Attention (top right) and Working Memory Capacity (bottom) User Groups

The main observation based on all three graphs is that users with enhanced cognitive processing abilities performed significantly faster in the graphical authentication mechanism than users with limited cognitive processing abilities (*SOP Group*: $F(1,496)=8.981$, $p=0.003$; *CA Group*: $F(1,496)=7.269$, $p=0.007$; *WMC Group*: $F(1,496)=45.199$, $p<0.001$). On the other hand, no significant differences in text-based password performances between the two user groups (limited vs. enhanced) were observed. An interpretation of this result might be based on the fact that all users were more familiar and experienced interacting with text-based passwords, hence no significant differences were observed between the limited and enhanced user groups across all three cognitive factors. However, since the familiarity factor did not affect the graphical authentication mechanism, we have observed that the users' enhanced ability of processing information has positively affected their performance compared to users with limited cognitive processing abilities.

Furthermore, a between authentication type comparison revealed that users with enhanced working memory capacity did not perform significantly different between the text-based password and the graphical authentication mechanism. Given the fact that pictures are visually and aesthetically richer than plain text, from a user-adaptation point of view, this result suggests providing graphical authentication mechanisms to users with enhanced working memory capacity with the aim to provide a positive user experience during user authentication [11].

User Authentication Effectiveness. For each user authentication session the total number of tries made for successfully authenticating in each type was recorded. Tables 2 summarize the means of tries across all three cognitive processing groups (i.e., SP, CA, WMC groups) per authentication type (text-based password and graphical). Regarding the text-based password authentication mechanism, on average, users with limited cognitive processing abilities needed more tries to authenticate than the enhanced group. The Mann-Whitney test revealed that the differences between limited and enhanced speed of processing users was statistically significant ($p=0.002$), whereas for the controlled attention group ($p=0.67$) and the working memory capacity group ($p=0.7$) the differences were not significant. In the case of graphical authentication, users with limited speed of processing and controlled attention needed on average less attempts than the enhanced user group, however with no statistically significant differences as the Mann-Whitney test revealed (*SOP:* $p=0.72$; *CA:* $p=0.12$; *WMC:* $p=0.21$).

Table 2. Means of Tries per User Group

	Speed of Processing		**Controlled Attention**		**Working Memory Capacity**	
	Enhanced	**Limited**	**Enhanced**	**Limited**	**Enhanced**	**Limited**
Password	1.14	1.55	1.29	1.34	1.31	1.54
Graphical	1.29	1.12	1.33	1.15	1.18	1.30

A between authentication type comparison, revealed that as our sample increased there was a growing tendency of users with limited cognitive processing abilities, toward solving graphical authentication mechanisms more effective than text-based passwords. The Mann-Whitney test revealed that users with limited speed of processing and limited working memory capacity needed less attempts in graphical authentication than text-based password authentication, with statistical significant differences (*SOP:* $p=0.006$; *WMC:* $p=0.047$). Taking into consideration that a graphical authentication mechanism is from a memory recall point of view a less demanding cognitive task than a password (recall through recognition vs. recall of information), an interpretation of this result can be based on the fact that graphical authentication mechanisms leverage human memory for visual information [6] and thus users with decreased speed of processing and working memory capacity needed less attempts in graphical authentication than in text-based passwords since the images illustrated helped them recognize and recall their authentication key.

4 Conclusions

The overarching aim of this work was to increase our understanding and knowledge on supporting usable security interaction design through user modeling, and adaptivity in user interface designs aiming to assist users to accomplish efficiently and effectively comprehensive and usable authentication tasks. In this respect, a three-month ecological valid user study was designed which entailed credible psychometric-based tests for eliciting the users' cognitive processing abilities (speed of processing, controlled attention, working memory capacity) and two types of user authentication mechanisms (text-based password and graphical), with the aim to investigate whether individuals with different cognitive processing abilities perform different in terms of efficiency and effectiveness in user authentication tasks.

Initial results demonstrate a main effect of cognitive processing abilities in both efficiency and effectiveness of user authentication mechanisms. In particular, results revealed that users with enhanced cognitive processing abilities performed significantly faster than users with limited cognitive processing abilities in graphical authentication. Regarding text-based password mechanisms, both user types with enhanced and limited cognitive processing abilities performed similarly with no significant differences. A possible interpretation of this result can be based on the familiarity factor of text-password mechanisms, thus, no significant differences were observed between the limited and enhanced user groups. However, since the users were not familiar with the graphical authentication mechanism, results indicated that the enhanced information processing abilities and temporary storage capacity of users have positively affected their performance compared to users with limited cognitive processing abilities. Another important result revealed that users with limited cognitive processing abilities needed significantly less attempts in graphical authentication than text-based password authentication suggesting that graphical authentication keys are easier to be retained in memory for this user group. These findings could be interpreted under the light of the picture superiority effect which suggests that pictures are better recognized and recalled by the human brain than textual information [27, 28]. Accordingly, various studies explain that pictures are more perceptually rich than words which lend them an advantage in memory recall (i.e., recall through recognition), and thus support the fact that users with decreased working memory capacity were more effective in graphical authentication mechanisms than in text-based password mechanisms. On the other hand, given that pictures are more perceptually rich than words, and thus are more demanding from a processing point of view, users with enhanced cognitive processing abilities were significantly faster in graphical authentication mechanisms than users with limited cognitive processing abilities.

From a user-adaptation point of view, such findings suggest that individual differences in human cognition are important to take into account in the personalization process of an adaptive interactive system. For instance, given that users with enhanced working memory capacity needed less tries in graphical authentication, and did not perform significantly different in either authentication type, such a result suggests providing a user with increased working memory capacity with a graphical authentication mechanism. In this respect, adapting the authentication task based on

users' cognitive processing abilities could improve authentication task efficiency and effectiveness, and minimize users' cognitive loads and erroneous interactions. A practical implication of this work could be to explicitly elicit the users' cognitive processing abilities and accordingly suggest the "best-fit" authentication mechanism. A more sophisticated architecture could in addition, implicitly recommend the "best-fit" authentication mechanism based on historical usage data of the user in regard with efficiency and effectiveness of authentication tasks.

The limitations of the reported study are related to the fact that participants were only university students with an age between 17 to 26 years. In addition, carrying out a single assessment of users' cognitive factors might not fully justify the users' classification into specific cognitive-based groups since individuals might be influenced by other circumstances over time such as emotions, urgency, etc. In this respect, further studies need to be conducted in order to reach more concrete conclusions about the effect of individuals' cognitive processing abilities on their performance in authentication tasks. Furthermore, there has been an effort to increase ecological and internal 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.

Given that future studies will contribute to the external validity of the reported research, we suggest that providing personalized user authentication mechanisms, adapted to users' individual characteristics could improve the overall user experience with regard to authentication tasks.

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 Co-LIVING (60-61700-98-009) and SocialRobot (285870).

5 References

1. Herley, C., van Oorschot, P.: A Research Agenda Acknowledging the Persistence of Passwords. J. Security and Privacy, 10, 1, 28-36 (2012)
2. Zhang, J., Luo, X., Akkaladevi, S., Ziegelmayer, J.: Improving Multiple-password Recall: An Empirical Study. J. Information Security 18, 2, 165-176 (2009)
3. Schneier, B.: The Secret Question Is: Why do IT Systems use Insecure Passwords? The Guardian, UK (2009)
4. Cranor, F., Garfinkel, S.: Security and Usability: Designing Secure Systems That People Can Use. O'Reilly & Associates, Sebastopol, CA (2005)
5. Jakobsson, M., Myers, S.: Phishing and Countermeasures: Understanding the Increasing Problem of Electronic Identity Theft. Wiley-Interscience (2006)
6. Biddle, R., Chiasson, S., van Oorschot, P.: Graphical Passwords: Learning from the First Twelve Years. J. ACM Computing Surveys, 44, 4, Article 19 (2012)
7. Jermyn, I., Mayer, A., Monrose, F., Reiter, M., Rubin, A.: The Design and Analysis of Graphical Passwords. In: USENIX International Security Symposium, pp. 1-1. USENIX Association, Berkley, CA (1999)
8. Tao, H., Adams, C.: Pass-Go: A Proposal to Improve the Usability of Graphical Passwords. J. Network Security 7, 2, 273-292 (2008)

9. Bulling, A., Alt, F., Schmidt, A.: Increasing the Security of Gaze-based Cued-recall Graphical Passwords using Saliency Masks. In: ACM SIGCHI International Conference on Human Factors in Computing Systems, pp. 3011-3020. ACM Press, New York, NY (2012)
10. Passfaces Corporation, The science behind Passfaces, http://passfaces.com/enterprise/resources/whitepapers.htm
11. Mihajlov, M., Jerman-Blazic, B.: On Designing Usable and Secure Recognition-based Graphical Authentication Mechanisms. J. Interacting with Computers 23, 6, 582-593 (2011)
12. Adams, A., Sasse, A.: Users are not the Enemy: Why Users Compromise Security Mechanisms and How to Take Remedial Measures. J. Communications of the ACM 42, 12, 40-46 (1999)
13. Florencio, D., Herley, C.A.: Large-scale Study of Web Password Habits. In: ACM International Conference on World Wide Web, pp. 657-666. ACM Press, New York, NY (2007)
14. 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)
15. Brusilovsky, P., Kobsa, A., Nejdl, W.: The Adaptive Web: Methods and Strategies of Web Personalization. Springer, Heidelberg (2007)
16. Card, S.K., Moran, T.P., Newell, A. The Model Human Processor: An Engineering Model of Human Performance. In: Boff, K.R., Kaufman, L., Thomas, J.P. (eds.) Handbook of Perception and Human Performance. Cognitive Processes and Performance, vol. 2, pp. 1-35 (1986)
17. Demetriou, A., Spanoudis, G., Shayer, S., Mouyi, A., Kazi, S., Platsidou, M.: Cycles in Speed-Working Memory-G Relations: Towards a Developmental-Differential Theory of the Mind. J. Intelligence 41, 34-50 (2013)
18. Hunt, E.B.: Human Intelligence. Cambridge University Press, New York (2011)
19. Demetriou, A., Spanoudis, G., Mouyi, A.: Educating the Developing Mind: Towards an Overarching Paradigm. J. Educational Psychology Review 23, 4, 601-663 (2011)
20. MacLeod, C.M.: Half a Century of Research on the Stroop Effect: An Integrative review. J. Psychological Bulletin 109, 163-203 (1991)
21. Posner, M.I., Raicle, M.E.: Images of Mind. Scientific American Library, New York (1997)
22. Stroop, J.R. Studies of Interference in Serial Verbal Reactions. J. Experimental Psychology 18, 643-662 (1935)
23. Baddeley, A.: Working Memory: Theories, Models, and Controversies. J. Annual Review of Psychology 63, 1-29 (2012)
24. Baddeley, A.: Working Memory. J. Science 255, 5044, 556-559 (1992)
25. Shipstead, Z., Broadway, J.: Individual Differences in Working Memory Capacity and the Stroop Effect: Do High Spans Block the Words? J. Learning and Individual Differences (in press)
26. Demetriou, A., Christou, C., Spanoudis, G., Platsidou, M.: The Development of Mental Processing: Efficiency, Working Memory and Thinking. Monographs of the Society for Research in Child Development 67, 1 (2002)
27. Anderson, J.R.: Cognitive Psychology and its Implications: Seventh Edition. Worth Publishers, New York, NY (2009)
28. Ally, B.A., Budson, A.E.: The Worth of Pictures: Using High Density Event Related Potentials to Understand the Memorial Power of Pictures and the Dynamics of Recognition Memory. J. NeuroImage 35, 378-395 (2007)