The Effect of Users' Working Memory on Preference and Performance in Authentication Mechanisms

Marios Belk
University of Cyprus
1678 Nicosia, Cyprus
belk@cs.ucy.ac.cy

Christos Fidas
University of Cyprus
1678 Nicosia, Cyprus
christos.fidas@cs.ucy.ac.cy

Panagiotis Germanakos
University of Cyprus
1678 Nicosia, Cyprus
pgerman@cs.ucy.ac.cy

George Samaras
University of Cyprus
1678 Nicosia, Cyprus
cssamara@cs.ucy.ac.cy

An effective authentication mechanism should embrace both security and usability aspects as its purpose is to provide maximum protection of application providers' assets but as well usability and transparency to its end users, aiming to minimize cognitive overloads. With the aim to investigate the relation among users' working memory capacity and different types of authentication mechanisms, a study was conducted which entailed a psychometric-based survey for identifying users' working memory capacity, combined with a real usage scenario with two variations of authentication mechanisms. A total of 97 users participated in the reported study during a 5-month period providing interesting insights with respect to users' working memory and preference and performance of authentication mechanisms.

Authentication Mechanism. Working Memory. Usability. Preference. Performance.

1. INTRODUCTION

Research on 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 (Inglesant and Sasse, 2010; Biddle et al., 2011). Researchers promote various designs of authentication mechanisms based on text and pictures, combinations of text and pictures, password managers and policies, etc. (Verma, 2012; Mihajlov and Jerman-Blazic, 2011; Biddle et al., 2011).

In this context, a large-scale study of half a million users, which 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 stronger password instead of focusing on maximizing password strength.

Many shortcomings of authentication mechanisms arise from the limitations of human memory. The number of items the human brain can temporarily store is limited, with a short-term capacity (i.e., working memory) of ~3-7 items, depending on the task (Baddeley, 2007; Cowan, 2010). 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 (Cowan, 2010; Baddeley, 2007) argue that working memory has an effect on mental tasks, such as information processing, comprehension, learning, and problem solving.

Many studies indicate that working memory capacity varies among people and predicts individual differences in intellectual ability (Cowan, 2010; Baddeley, 2007). Such individual differences need to be further investigated aiming to understand whether they affect user interactions with authentication mechanisms.

In light of these challenges, this paper presents results of an empirical study which investigated the effect of working memory capacity of users towards preference and performance issues of two different types of authentication mechanisms; password and graphical authentication mechanisms.

2. METHOD OF STUDY

2.1 Procedure

A Web-based psychometric instrument was developed that assesses the capacity of the visuo-spatial sketchpad of users, which is the temporary storage mechanism responsible for processing visual and spatial information (Baddeley, 2007). This instrument aims to measure the amount of information the visuo-spatial sketchpad of a person can efficiently activate simultaneously by requesting from that person to memorize an abstract image and then compare that image with five other similar images.

Furthermore, a Web-based environment was developed for two introductory Computer Science 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 was used for accessing the courses' material (i.e., course slides, homework exercises) and for viewing their grades. The type of authentication (password or graphical mechanism) was randomly provided during the enrolment process. At the end of the process the sample consisted of half of the students having enrolled with a password and the other half having enrolled with a graphical authentication mechanism. For the purpose of the experiment, in the middle of the semester, the system altered the students' authentication type; students that had enrolled with a password during the first half of the semester were prompted to create a new graphical authentication key and vice versa. The new authentication key would be used during the second half of the semester. The main aim of this process was to capture the interaction data of users for both types of authentication throughout the semester and further elicit their preference towards a particular type.

The password mechanism involved alphanumeric and special keyboard characters. A minimum of 6 characters including numbers, a mixture of lower- and upper-case letters, and special characters were required to be entered by the users. The graphical authentication mechanism involved single-object pictures with one-time authentication codes, where users had to select a minimum of 6 pictures (out of 30 available pictures) in a specific sequence, and was based on the recognition-based, graphical authentication mechanism proposed by Mihajlov and Jerman-Blazic (2011).

The total time required for successful authentication was monitored on the client-side utilizing a browser-based logging facility that started recording time as soon users entered the authentication Web-page, until they successfully completed the authentication process.

2.2 Hypotheses

The following null hypotheses were formulated: i) working memory capacity of users does not have a significant effect on users' preference towards password mechanisms or recognition-based, graphical authentication mechanisms, ii) there is no significant difference with regards to time needed to authenticate through a password mechanism or a recognition-based, graphical authentication mechanism among users having low, medium, and high working memory capacity.

2.3 Demographics of Participants

A total of 97 people participated in the study between January and May 2012. Participants varied from the age of 17 to 24, with a mean age of 20 and were undergraduate students of Electrical Engineering, Psychology and Social Science Departments. A total of 3461 successful authentications have been recorded during the 5 month period.

3. RESULTS

For our analysis, we separated the participants in three categories based on their working memory capacity: Low (N=27, f=27.8%, 33.37 average logins/user), Medium (N=50, f=51.5%, 38.88 average logins/user), and High (N=20, f=20.6%, 30.8 average logins/user).

3.1 Preference of User Authentication

An online questionnaire was provided to the students at the end of the study to express their preference towards a specific type of authentication (i.e., password or graphical). 66 out of the 97 students completed the questionnaire. In Table 1, we summarize the

preferences of authentication types according to the users' working memory capacity.

Table 1: *Users' Working Memory Capacity and Authentication Type Preference*

Working Memory Groups	Preference		Total
	Password	*Graphical*	
Low	*3*	*15*	*18*
Medium	*18*	*19*	*37*
High	*6*	*5*	*11*
Total	*27*	*39*	*66*

A Pearson's chi-square test was conducted to examine whether there is a relationship between users' working memory capacity and their preference towards a specific type of authentication mechanism (i.e., password or graphical). The results revealed that there is significant relationship between these two variables (Chi square value=6.139, df=2, p=0.046). In particular, examining each group (i.e., Low, Medium, High) individually with respect to preference towards a particular authentication mechanism, it has been identified that users with low working memory capacity significantly prefer graphical authentication mechanisms (Chi square value=8.000, df=1, p<0.01). In contrast, users having medium (Chi square value=0.27, df=1, p=0.869) and high working memory capacity (Chi square value=0.091, df=1, p=0.763) have not shown a clear preference towards a specific authentication mechanism.

3.2 Performance in User Authentication

A three by two way factorial analysis of variance (ANOVA) was conducted aiming to examine main effects between the users' working memory capacity (i.e., Low, Medium, High) and authentication type (i.e., password vs. graphical) over the time needed to access the system. Figure 1 illustrates the means of performance per working memory group and authentication type.

The analysis revealed that the main effect of users' working memory capacity on time needed to successfully authenticate is significant (F(2,97)=3.087, p=0.05). Furthermore, a pairwise comparison between the user groups and authentication types was conducted to examine whether they have a significant effect on the time required to authenticate to the Web-site.

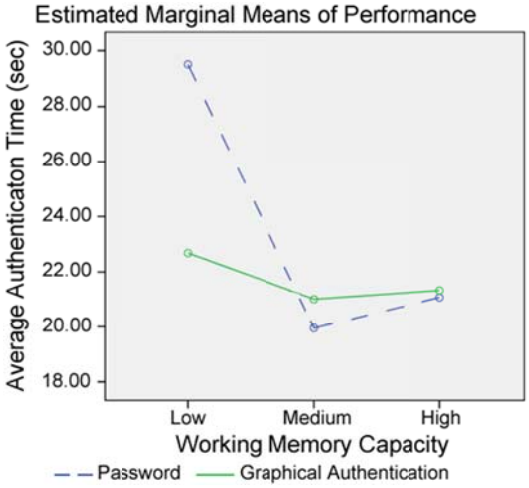

Figure 1: *Estimated Marginal Means of Performance per Working Memory Group and Authentication Type*

The results revealed that users of the Low working memory group performed significantly faster in graphical authentication (22.7 sec) than in password (29.5 sec) mechanisms (F(1,27)=10.630, p=0.003). However, users belonging to the Medium and High working memory group had no significant effect on performance between password and graphical authentication mechanisms (Medium Group: F(1,50)=0.263, p=0.611, and High Group: F(1,20)=0.006, p=0.939), as they performed almost equally the same in both authentication mechanisms compared to the Low working memory group (Figure 1).

4. CONCLUSIONS AND FUTURE WORK

The results presented in this paper constitute an effort to investigate whether individual differences of users have an effect on preference and performance issues related to authentication mechanisms. Such a research endeavour is based on the promise that understanding and modelling human behaviour with regards to security interactions can assist the design and deployment of more usable authentication mechanisms.

As a primary result, the study presented in this paper reveals a significant effect of users' working memory towards their preference and performance on authentication mechanisms. In particular, users belonging to the Low working memory group performed statistically significant faster with graphical authentication than a textual password mechanism. Similar results have been obtained relating with users' preference towards password or graphical

authentication mechanisms, as users belonging to the Low working memory group preferred graphical authentication mechanisms. In contrast, in the case of users that belong to the Medium and High working memory groups, no significant difference in preference and performance was observed between the two variations.

Taking into consideration that a graphical authentication mechanism is from a user's point of view a less demanding cognitive task than a password (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 (Biddle et al., 2011) and thus users with decreased working memory (i.e., Low) find graphical authentication mechanisms more usable and memorable since passwords are more demanding from a memory retrieval point of view. Another interpretation of this result can be based on the fact that users' preference towards graphical authentication might have also been affected by the picture superiority effect (Paivio and Csapo, 1973). On the other hand, users with enhanced working memory capacity could handle both authentication mechanisms more efficiently and effectively, hence no significant preference and performance were reported between the two types.

The limitations of the reported study are related to the fact that the participants were undergraduate students with an age between 17 to 24 years. Furthermore, carrying out a single assessment of users' working memory might not fully justify the users' classification into specific working memory groups. In this respect, further tests need to be conducted in order to reach more concrete conclusions. On the other hand, there has been an effort to increase ecological validity of the research since the participants were involved in real tasks, in their own physical environment, and without the intervention of any experimental equipment or observer.

Future research prospects include further investigating the effect of individual differences of users on preference and performance issues in security-related interactions (Belk et al., 2012). The overarching aim is to drive this research towards the development of a user-centred adaptation framework that will provide personalized security interactions based on cognitive factors of users.

5. ACKNOWLEDGEMENTS

We thank Dr. Artemios G. Voyiatzis for essential discussions related to usable security. The work is co-funded by the EU projects SocialRobot (285870) and CO-LIVING (60-61700-98-009).

6. REFERENCES

Baddeley, A. (2007) Working Memory, Thought, and Action. Oxford University Press, New York, NY, USA.

Belk, M., Fidas, C., Germanakos, P., Samaras, G. (2012) Do Cognitive Styles of Users Affect Preference and Performance related to CAPTCHA Challenges? In Extended Abstracts of CHI 12, Austin, TX, USA, May 5-10, 2012, pp. 1487-1492. ACM Press, New York, NY, USA.

Biddle, R., Chiasson, S., van Oorschot, P. (2011) Graphical Passwords: Learning from the First Twelve Years. ACM Security, Vol. 5, No. 4, pp. 1-43.

Cowan, N. (2010) The Magical Mystery Four: How is Working Memory Capacity Limited, and Why? Current Directions in Psychological Science, Vol. 19, No. 1, pp. 51–57.

Florencio, D., Herley, C. (2007) A Large-scale Study of Web Password Habits. In Proceedings of WWW 07, Banff, Alberta, Canada, May 8-12, 2007, pp. 657-666. ACM Press, New York, NY, USA.

Inglesant, P., Sasse, M.A. (2010) The True Cost of Unusable Password Policies: Password use in the Wild. In Proceedings of CHI 10, Atlanta, GA, USA, 10-15 April, 2010, pp. 383-392. ACM Press, New York, NY, USA.

Mihajlov, M., Jerman-Blazic, B. (2011) On Designing Usable and Secure Recognition-based Graphical Authentication Mechanisms. Elsevier Interacting with Computers, Vol. 23, No. 6, pp. 582-593.

Paivio, A., Csapo, K. (1973) Picture Superiority in Free Recall: Imagery or Dual Coding? Cognitive Psychology, Vol. 5, No. 2, pp. 176-206.

Verma, P. (2012) icAuth: Image-color based Authentication System. International Conference on Intelligent User Interfaces (IUI 2012), Lisbon, Portugal, February 14-17, 2012, pp. 329-330. ACM Press, New York, NY, USA.