DEPARTMENT OF COMPUTER SCIENCE

ADAPTIVE USABLE SECURITY: PERSONALIZING USER AUTHENTICATION AND CAPTCHA BASED ON INDIVIDUAL DIFFERENCES IN COGNITIVE PROCESSING

MARIOS R. BELK

A Dissertation Submitted to the University of Cyprus in Partial Fulfillment of the Requirements for the Degree of Doctor of Philosophy

December 2015

APPROVAL PAGE

Doctor of Philosophy Dissertation

ADAPTIVE USABLE SECURITY: PERSONALIZING USER AUTHENTICATION AND CAPTCHA BASED ON INDIVIDUAL DIFFERENCES IN COGNITIVE PROCESSING

Presented by

Marios R. Belk

Research Supervisor

Dr. George Samaras

Research Co-supervisor

Dr. Panagiotis Germanakos

Committee Member

Dr. Marios Dikaiakos

Committee Member

Dr. Constantinos Pattichis

Committee Member

Dr. Nikolaos Avouris

Committee Member

Dr. Vania Dimitrova

University of Cyprus

December, 2015

VALIDATION PAGE

Doctoral Candidate: Marios R. Belk

Doctoral Thesis Title: Adaptive Usable Security: Personalizing User Authentication and CAPTCHA based on Individual Differences in Cognitive Processing

The presented Doctoral Dissertation was submitted in partial fulfillment of the requirements for the Degree of Doctor of Philosophy at the ***Department of Computer Science*** *and was approved on the 14th of December, 2015 by the members of the* ***Examination Committee****.*

Examination Committee:

Research Supervisor:

Dr. George Samaras, Professor, University of Cyprus

Research Co-supervisor :

Dr. Panagiotis Germanakos, Research Scientist, University of Cyprus

Committee Member:

Dr. Marios Dikaiakos, Professor, University of Cyprus

Committee Member (Ph.D. Chairman):

Dr. Constantinos Pattichis, Professor, University of Cyprus

Committee Member:

Dr. Nikolaos Avouris, Professor, University of Patras

Committee Member:

Dr. Vania Dimitrova, Associate Professor, University of Leeds

DECLARATION OF DOCTORAL CANDIDATE

The present doctoral dissertation was submitted in partial fulfillment of the requirements for the degree of Doctor of Philosophy of the University of Cyprus. It is a product of original work of my own, unless otherwise mentioned through references, notes, or any other statements.

Marios R. Belk

ABSTRACT (IN GREEK)

Η αλληλεπίδραση ανθρώπου-υπολογιστή μετατοπίζεται από παραδοσιακούς υπολογιστές και αυτόνομες εφαρμογές, προς την αλληλεπίδραση χρηστών με φορητές υπολογιστικές συσκευές και εφαρμογές που υποστηρίζονται από το υπολογιστικό νέφος. Σε αυτό το πλαίσιο, το θέμα της ασφάλειας διαδραστικών συστημάτων κερδίζει ολοένα και περισσότερο την προσοχή ερευνητών και εμπειρογνωμόνων, όχι μόνο από τεχνικής άποψης, αλλά επίσης από την πλευρά της ευχρηστίας. Η κοινότητα ασφάλειας έχει κατανοήσει τη ζωτική σημασία της *«εύχρηστης ασφάλειας»* (*usable security*), η οποία εστιάζεται κυρίως στο σχεδιασμό συστημάτων ασφαλείας που να είναι εύχρηστα και φιλικά προς το χρήστη.

Οι κυρίαρχες αλληλεπιδράσεις ανθρώπων με συστήματα ασφαλείας στον Παγκόσμιο Ιστό σχετίζονται κυρίως με την ταυτοποίηση χρηστών (user authentication) και το διαχωρισμό μεταξύ ανθρώπων-μηχανών μέσω μηχανισμών CAPTCHA. Ο σχεδιασμός και η ανάπτυξη αυτών των μηχανισμών αντιπροσωπεύει ένα υπαρκτό πρόβλημα μεταξύ ασφάλειας και ευχρηστίας, το οποίο προκύπτει κυρίως από αντιφατικούς στόχους και απαιτήσεις που δημιουργούνται μεταξύ των διαφόρων εγγενών εμπλεκομένων παραγόντων. Από τη μία πλευρά, ειδικοί σε θέματα ασφάλειας αυξάνουν συνεχώς τα επίπεδα της ασφάλειας των μηχανισμών ταυτοποίησης χρηστών και CAPTCHA, ενώ από την άλλη, οι τελικοί χρήστες απαιτούν διαφάνεια, προσαρμοσμένες και φιλικές λύσεις που δεν θα αποτελούν εμπόδιο στην εκτέλεση των καθημερινών τους διεργασιών. Παράλληλα, οι πάροχοι υπηρεσιών από κοινού με εμπειρογνώμονες σε θέματα ευχρηστίας, προσπαθούν να αναδείξουν μια βιώσιμη ισορροπία μεταξύ της ασφάλειας και της ευχρηστίας με σκοπό την αύξηση της αποδοχής υπηρεσιών και εφαρμογών από τους χρήστες. Στο πλαίσιο αυτό, η έρευνα σχετικά με τέτοιου είδους μηχανισμούς ασφαλείας αποτελεί προτεραιότητα τα τελευταία χρόνια, με στόχο την ανάπτυξη μηχανισμών που να προσφέρουν υψηλά πρότυπα ασφαλείας και ταυτόχρονα να διατηρούν την απρόσκοπτη αλληλεπίδραση με τους νόμιμους χρήστες.

Επί του παρόντος, η ανάπτυξη μηχανισμών ταυτοποίησης χρηστών και CAPTCHA ακολουθεί κυρίως το μοντέλο *«ένας-σχεδιασμός-για-όλους»*. Κατ' επέκταση, ο ίδιος τύπος μηχανισμού κοινοποιείται σε όλους τους χρήστες χωρίς να λαμβάνεται υπόψη ότι οι χρήστες έχουν διαφορετικά χαρακτηριστικά, πολιτισμικό και γνωστικό υπόβαθρο. Έχοντας κατά νου ότι οι αλληλεπιδράσεις ανθρώπου-υπολογιστή όσον αφορά τους μηχανισμούς ταυτοποίησης χρηστών και CAPTCHA εκτελούνται κυρίως σε γνωστικό επίπεδο, που περιλαμβάνουν την αντίληψη, την αναγνώριση, μνήμη και σκέψη, η παρούσα διδακτορική διατριβή υποστηρίζει ότι ανθρώπινοι γνωστικοί παράγοντες μπορούν να προσφέρουν μια στρατηγική προοπτική για την εξέταση μηχανισμών ταυτοποίησης και CAPTCHA, πλαισιωμένη από θεωρίες ατομικών διαφορών γνωστικής επεξεργασίας.

Στα πλαίσια της διατριβής αυτής επιχειρείται να επανεξεταστεί ο ορισμός της «εύχρηστης ασφάλειας», προτείνοντας μια εναλλακτική προσέγγιση του προβλήματος η οποία ωθείται από την έρευνα σε μοντελοποίηση χρηστών, προσαρμογή και εξατομίκευση συστημάτων αλληλεπίδρασης και ατομικών διαφορών. Κύριος στόχος είναι η εξατομίκευση και βελτίωση της ευχρηστίας μηχα-

νισμών ταυτοποίησης και CAPTCHA λαμβάνοντας υπόψη τα μοναδικά χαρακτηριστικά της γνωστικής επεξεργασίας των χρηστών. Οι στόχοι της διατριβής είναι: (i) Να εξεταστεί η επίδραση γνωστικών παραγόντων στις προτιμήσεις χρηστών και ευχρηστίας διαφόρων μηχανισμών ταυτοποίησης και CAPTCHA, που υποστηρίζεται από μια σειρά έγκυρων μελετών, βασισμένες σε ποσοτικές και ποιοτικές μετρήσεις, (ii) να προταθεί ένα γνωστικό μοντέλο χρηστών, και να μοντελοποιηθεί ένας μηχανισμός προσαρμογής τύπου και πολυπλοκότητας μηχανισμών ταυτοποίησης και CAPTCHA, και (iii) να προταθεί ένα πλαίσιο εξατομίκευσης PAC (Personalized Authentication and CAPTCHA), που προτείνει την καλύτερη δυνατή απόφαση προσαρμογής μηχανισμών ταυτοποίησης χρηστών και CAPTCHA.

ABSTRACT

Computer-human interaction is nowadays shifting from traditional desktop computers and standalone applications towards mobile computing devices and cloud-based oriented applications and services, mainly triggered by developments in network communication technologies. Within this realm, security issues of interactive systems are gaining more than ever the attention not only from a technical and security perspective but also from the user's point of view. 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.

The predominant user security interactions over the World Wide Web are commonly related to user authentication and CAPTCHA mechanisms. Design and development of user authentication and CAPTCHA represents a cross-roads priority problem, between security and usability, which emerge from contradictory requirements posed by different stakeholders, inherent to the function and purpose of each security mechanism. On the one hand, security experts increase continuously the security levels of user authentication and CAPTCHA, while on the other, end-users demand transparent, adaptable and user-friendly solutions. In parallel, service providers together with user experience experts, try to find a viable equilibrium among security and usability in order to increase the acceptability of services and applications. In this context, research on these security mechanisms has received significant attention lately, aiming to offer high security standards and at the same time to maintain a seamless interaction for the legitimate users.

Currently, deployment of user authentication and CAPTCHA mechanisms follow a *"one-size-fits-all"* paradigm. The same type of text-based password and text-recognition CAPTCHA is communicated to all users neglecting the fact that users have different cultural and cognitive backgrounds, and interact in different contexts of use. Bearing in mind that human-computer interactions with regard to user authentication and CAPTCHA mechanisms are in principal cognitive tasks that embrace perception, recognition, remembering and reasoning, this research work builds on the promise that human cognitive factors offer a widely ignored but very strategical perspective for examining user authentication and CAPTCHA tasks framed by theories of individual differences in human cognitive processing.

Henceforth, this work attempts to revisit the definition of usable security by advocating an alternative approach which is driven by research in the intersection of User Modeling, Adaptation and Personalization, and Individual Differences. Main focus is to personalize and improve the usability of user interactions in authentication and CAPTCHA according to the unique cognitive processing characteristics of users. The high-level objectives of the thesis are: (i) Investigate the effects of human cognitive factors on user preference and task performance of different user authentication and CAPTCHA mechanisms, supported by a number of ecological valid user studies, and quantitative and qualitative metrics; (ii) propose a formalization of a cognitive factor-based user model and an adaptation engine for personalizing user authentication and CAPTCHA tasks on design type and

complexity; and (iii) propose PAC (Personalized Authentication and CAPTCHA), a personalization framework that recommends the "best-fit" decision based on the aforementioned formalizations.

ACKNOWLEDGEMENTS

Throughout my Ph.D. research work, I worked closely with several people to whom I am sincerely grateful. Without their constant support and encouragement such an endeavor would be simply not feasible. The fruitful and productive collaborations, the endless discussions and ideas can be realized in the numerous contributions and scientific findings and publications reported in this thesis.

First, my sincere gratitude goes to my respectful Ph.D. supervisor Dr. George Samaras, Professor at the Department of Computer Science, University of Cyprus. Apart from motivating me throughout my research endeavor, so to find myself in a challenging and highly interesting academic environment, I am thankful for his valuable research, intellectual and scientific guidance in the development of my research work as well as in the development of myself as a research scientist. I thank Professor Samaras for introducing me to the area of personalization and identifying the potentials and the need to personalize user authentication and CAPTCHA mechanisms based on human cognitive factors. Heartfelt thanks to him for all these years, for being next to me, believing in me and supporting me in every step.

My sincere appreciations go to my friend and Ph.D. co-supervisor, Dr. Panagiotis Germanakos, Research Scientist at the Department of Computer Science, University of Cyprus, and Senior User Experience Researcher at SAP SE, for his unrelenting help and support throughout the duration of my research. Panagiotis has been next to me since day one of my research journey and a true source of inspiration, always more than willing to take time out in order to assist me during crucial times in my work. I really enjoyed collaborating with Panagiotis and I thank him for helping me identify and understand the need to investigate the influence that individual differences have on the information space, with the aim to guide the design of human-centered interactive systems.

My sincere appreciations go to my friend and collaborator, Dr. Christos Fidas, Lecturer at the Department of Cultural Heritage Management and New Technologies, University of Patras, for his endless support, guidance and supervision, and above all, for the great and fruitful collaboration we had. Christos was always more than willing to help me, and make effective discussions throughout my research work. I thank Christos for introducing me to the area of usable security and the necessity to understand and support users in this context by following user-centered design methodologies. Through the productive discussions we had, his insightful and inspiring ideas, Christos has contributed in investigating and understanding the interdependencies among the human, technology and security design factors reported in this work.

I would like to express my appreciations to my lab fellow, Dr. Panayiotis Andreou, Lecturer in Computing at the University of Central Lancashire, Cyprus, for his support and great collaboration we had. I am thankful to Panayiotis for helping me design the reported framework and respective formalizations of the user model and adaptation procedures.

Many thanks go to Dr. Efi Papatheocharous, Senior Researcher at the Swedish Institute of Computer Science, for the nice collaboration, her professionalism and the interesting discussions we

had. Her expertise in software engineering and AI contributed in realizing the challenging task of implicitly modeling human factors based on navigation behavior of users.

I would like to express my special thanks to Dr. Konstantinos Mourlas, Associate Professor at the Department of Communication and Media Studies, National and Kapodistrian University of Athens, Dr. George Spanoudis, Assistant Professor at the Department of Psychology, University of Cyprus, as well as Dr. Nikos Tsianos and Zacharias Lekkas, researchers at the Department of Communication and Media Studies, National and Kapodistrian University of Athens, for their efforts and productive discussions we had, especially at the early stages of this work that helped me conceiving and developing the human factor-based user model.

I would like to thank Dr. Marios Dikaiakos and Dr. Constantinos Pattichis, both Professors at the Department of Computer Science, University of Cyprus, for their time and efforts in reviewing this thesis and honoring this work by serving as committee members. I would also like to thank the external committee members of this dissertation, Dr. Nikolaos Avouris, Professor at the Department of Electrical and Computer Engineering, University of Patras, and Dr. Vania Dimitrova, Associate Professor at the School of Computing, University of Leeds, who honored this work by visiting Cyprus, and for their valuable time reviewing this thesis.

I also thank my lab fellows at the Department of Computer Science, University of Cyprus, namely Dr. Dimosthenis Georgiadis, Dr. Christophoros Panayiotou, Dr. Andreas Pamboris, and my research collaborators at CITARD Services Ltd., namely Dr. Eleni Christodoulou, Dr. Christophoros Christophorou, Dr. Styliani Kleanthous-Loizou and Dr. David Portugal, for the great collaboration we had throughout the years.

A big thank you goes to various students at the Department of Computer Science, University of Cyprus, for the productive collaboration that helped in implementing many technical aspects reported in this thesis, namely Marios Constantinides, Argyris Constantinides and Andreas Hadjidemetris. Also, I would like to acknowledge the academic, administration and technical support of the Department of Computer Science, University of Cyprus, that provided the support and equipment needed for conducting my research.

I would also like to thank the national research funding programs, the Cyprus Research Promotion Foundation and the University of Cyprus research committee for internal research funds, as well as the structural funds of the European Union, that financially supported this research endeavor through a number of research projects during the years.

Special thanks go also to the students of the University of Cyprus for their time participating in the user studies of this thesis and the valuable feedback provided.

Finally, I would like to thank my family for their unconditional love and support all these years as well as my friends for their patience and understanding for the hours I was not able to be with them.

DEDICATIONS

To my lovely wife Angela, my daughter Anna and my boy Savvas.

To my family, for motivating and encouraging my research and for being always next to me.

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

LIST OF ABBREVIATIONS

ANOVA	Analysis of Variance
ADL	Absolute Distance of Links
AJAX	Asynchronous JavaScript and XML
ANN	Artificial Neural Networks
ASP	Active Server Pages
BPN	Back-Propagation Network
CAPTCHA	Completely Automated Public Turing test to tell Computers and Humans Apart
CNF	Conjunctive Normal Form
CPE	Cognitive Processing Efficiency
CSA	Cognitive Style Analysis
CSS	Cascading Style Sheets
E-CSA-WA	Extended - Cognitive Style Analysis - Wholist Analyst
EEG	Electroencephalography
ELSIN	European Learning Styles Information Network
FD	Field Dependent
FI	Field Independent
FIS	Fuzzy Inference System
FIT	Feature Integration Theory
GEFT	Group Embedded Figures Test
GPS	Global Positioning System
HCI	Human Computer Interaction
HCI-SEC	Human-Computer Interaction and Security
HIP	Human Interaction Proof
HTML	HyperText Markup Language
HTTP	HyperText Transfer Protocol
ICT	Information and Communication Technologies
ID	Identification
IDE	Integrated Development Environment
ILS	Index of Learning Styles
IO	Input/ Output
IP	Internet Protocol
IT	Information Technology
ITS	Intelligent Tutoring Systems
JSON	JavaScript Object Notation
JSP	Java Server Pages

LISP	LISt Processing
LSI	Learning Styles Inventory
LSQ	Learning Styles Questionnaire
MLP	Multi-Layer Perceptron
OCR	Optical Character Recognition
OSIVQ	Object-Spatial Imagery and Verbal Questionnaire
PAC	Personalized Authentication and CAPTCHA
PHP	PHP: Hypertext Preprocessor
PIN	Personal Identification Number
QoS	Quality of Service
QR	Quick Response
RBAC	Role-based Access Control
SQL	Structured Query Language
SVG	Scalable Vector Graphics
TMAC	Team-based Access Control
UCD	User-Centered Design
URL	Uniform Resource Locator
UX	User Experience
VICS	Verbal Imager Cognitive Style
W3C	World Wide Web Consortium
WMC	Working Memory Capacity
WWW	World Wide Web
XHTML	Extensible Hypertext Markup Language
XML	Extensible Markup Language

CHAPTER 1: Introduction

The World Wide Web has become gradually a platform for deployment of complex applications of increased interactivity, as it takes the form of a medium used for complex and important tasks like commercial and governmental transactions, collaborative work, learning and information retrieval. Within this realm, security and privacy issues of interactive systems are considered of paramount importance as it is known that the consequences of a security breach can harm the credibility and legal liability of an organization, decreases users' trust and acceptance while it exponentially increases maintenance and support costs. In this context, one of the most important and challenging issues is to support users, engaged on tasks related to security and privacy, through usable human-computer interface designs (Adams and Sasse 1999; Cranor and Garfinkel 2005; Kobsa et al. 2013; Shay et al. 2012; Inglesant and Sasse 2010; Florencio and Herley 2007; Fidas et al. 2011; Bursztein et al. 2014).

In 2009, the U.S. Government acknowledged *"usable security"* as one of the eleven hard problems to be researched for achieving cyber security, which are scalable trustworthy systems (including system architectures and requisite development methodology), enterprise-level metrics (including measures of overall system trustworthiness), system evaluation life cycle (including approaches for sufficient assurance), combatting insider threats, combatting malware and botnets, global-scale identity management, survivability of time-critical systems, situational understanding and attack attribution, provenance (relating to information, systems, and hardware) and privacy-aware security (Department of Homeland Security 2009). Usable security is therefore pronounced as the cornerstone of future online services and applications which are expected to offer a rich set of computing and communication services to users in a broader context representing unprecedented opportunities to access, manipulate, and share information as well as to accomplish tasks through heterogeneous devices and contexts of use.

User security interactions over the World Wide Web are commonly related with: (a) User authentication; (b) Human Interaction Proof mechanisms (e.g., CAPTCHA – von Ahn et al. 2004); (c) installation and usage of data encryption software tools, especially for secure e-mail communication; (d) installation of certificates for authorization issues, etc. (Fidas et al. 2010). From the aforementioned security interactions the most prominent are related to user authentication and CAPTCHA challenges. Research on these security interactions has received significant attention lately (Fidas et al. 2011; Bursztein et al. 2014; Kobsa et al. 2013; De Luca et al. 2013; 2014; Shay et al. 2015). There is a growing demand to enhance both the security and the usability aspects of such interactions, aiming to offer high security standards to application service providers and interaction transparency to actual users.

User authentication is a critical security mechanism in today's interactive systems (Koved and Stobert 2014). Derived from the Greek work *αὐθεντικός*; meaning real or genuine, user authentication is the act of confirming that a person interacting with a service is who he/she claims to be. In

the same line, CAPTCHA challenges are security defense mechanisms that are utilized by service providers for constructing a high-confidence proof that the entity interacting with a remote service is actually a human being and not malicious software that might attack the system and degrade the quality of a provided service. In the era of cloud-based mobile computing and the globalization of services, user authentication and CAPTCHA mechanisms are becoming increasingly important from a user-centered point of view, since these tasks are performed daily by millions of users across different cultures, with different cognitive backgrounds and diverse contexts of use (De Luca et al. 2014; Hayashi et al. 2013). In this context, this thesis will analyze the aforementioned user security mechanisms, and investigate and offer solutions aiming to improve and support the usability and overall experience of user interactions during authentication and CAPTCHA-related tasks.

1.1 User Authentication

User authentication is currently achieved primarily with the use of text-based passwords. It is estimated that more than 80% of US and UK companies apply some form of text-based password authentication; in many cases it is their sole method for user authentication (Zhang et al. 2009). A variety of studies have been reported that underpin the necessity for increasing usability in authentication mechanisms (Komanduri et al. 2011; Bonneau et al. 2012). The literature reveals many proposals, such as educating and influencing users to create more secure authentication keys (Forget et al. 2008), improving existing recall-based password approaches with recognition of text (Wright et al. 2012), enforcing the creation of secure authentication keys through policies (Komanduri et al. 2011). Despite the popularity of text-based passwords, with the advent of mobile touch-based devices and the disappearance of the standard keyboard in ubiquitous environments, research on proposing alternatives to text-based passwords has received significant attention lately (De Luca et al. 2013; Chiang and Chiasson 2013; Mihajlov and Jerman-Blazic 2011). A recent study of Findlater et al. (2011) demonstrated that typing patterns of users differ in a visual keyboard compared to non-visual affordance. In particular, the speed of entering text on touch-based surfaces is 31% reduced than traditional keyboards (Findlater et al. 2011). In this context, a considerable amount of research has focused on the design and implementation of graphical authentication schemes, that require users to recall and select pictures as their authentication key, with the promise to preserve security and improve usability and memorability, as they leverage the vast capacity and capabilities of the human visual memory system (Angeli et al. 2005; Everitt et al. 2009; Tullis et al. 2011). A number of different approaches to graphical authentication exist that promote alternative authentication interactions utilizing biometric techniques with gestural input (Sae-Bae et al. 2012), pattern recognition techniques in touch-based devices (De Luca et al. 2012), interactions with pictures on mobile devices (Chiang and Chiasson 2013) or interactions with combinations of text and pictures (Wright et al. 2012).

1.2 Completely Automated Public Turing test to tell Computers and Humans Apart

CAPTCHA (von Ahn et al. 2004) is a security mechanism widely used today for protecting Web applications and services against malicious software attacks (e.g., comment spam in online blogs, fake account registrations, dictionary attacks of passwords). CAPTCHA is a computer-based challenge-response test as an attempt to ensure that the response is generated by a human being and not a machine. It requires from a legitimate user to type letters or digits based on a distorted image that appears on the screen. Such a challenge is based on the assumption that a distorted text-based image can be easily recognized by the human brain but present significant difficulty for computer OCR (Optical Character Recognition) or other image-recognition systems. CAPTCHA challenges are performed primarily with the use of text-recognition CAPTCHA (Bursztein et al. 2010; von Ahn et al. 2008). The reCAPTCHA project (von Ahn et al. 2008), which is currently the most popular and widely used CAPTCHA online, estimates that over 200 million reCAPTCHAs are completed daily, and it takes an average of 10 seconds to complete one. In addition, major Web service providers such as Google, Facebook, Microsoft and many others utilize text-recognition CAPTCHA to protect their premises against automated attacks (Bursztein et al. 2010). Nevertheless, in the same line with graphical authentication mechanisms, given the increased popularity of mobile touch-based devices, as well as the known usability and security issues of text-recognition CAPTCHAs (Fidas et al. 2011; Yan and El Ahmad 2008), a considerable amount of research has focused on the design and implementation of image-recognition CAPTCHAs that claim to increase the usability of CAPTCHA, especially for mobile touch-based devices since they are language-independent, do not require text-entry (which is difficult on a mobile device (Findlater et al. 2011)), and employ a different domain for CAPTCHA generation beyond character obfuscation (Gossweiler et al. 2009; Vikram et al. 2011; Ross et al. 2010). Image-recognition CAPTCHAs are usually based on image puzzle problems and annotation of static and animated images. Examples include SEMAGE (Vikram et al. 2011) that requires users to select or recognize the content of a set of images, but as well understand and identify the semantic relationship between a subset of them, Sketcha (Ross et al. 2010) and What's Up CAPTCHA (Gossweiler et al. 2009) that require users to adjust randomly rotated images to their upright orientation.

1.3 The Need to Adapt and Personalize Security-related User Tasks

A generic conclusion that can be derived from the aforementioned state-of-the-art research is that: (a) A plethora of user authentication and CAPTCHA designs already exist (therefore the aim of this thesis is not to propose new ones); and (b) existing state-of-the-art designs primarily focus on text-based and graphical-based approaches in both user security mechanisms. However, the focus of analysis, on the presented works, remains mainly on the technology layer and fails to analyze, understand and model the principle human interaction processing workflows, cognitive stages and

transitions in accomplishing such tasks with the utter goal to provide adaptive and personalized solutions. Furthermore, a number of research works investigated the impact of several factors (human, technology and design related) on both user authentication and CAPTCHA mechanisms, aiming to understand human-computer interactions in such realms and further apply that knowledge in designing and developing usable security mechanisms (Biddle et al. 2012; Bursztein et al. 2014; Shirali-Shahreza et al. 2013). In this context, recent research revealed that human factors (e.g., age differences, cognitive differences), technology factors (e.g., device) and design factors (e.g., text vs. images) have a main effect on task performance and user preference of both user authentication and CAPTCHA (Ma et al. 2013; Forget et al. 2014; Belk et al. 2015a; Fidas et al. 2011; von Zezschwitz et al. 2014; Reynaga and Chiasson 2013). Examples include the work of Ma et al. (2013) that 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, 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.

According to the aforementioned research works, findings suggest that it is necessary to understand in depth the interdependencies among the user, the intermediate technology and the user security tasks. Furthermore, by better understanding these interdependencies among the main factors, and applying this knowledge for designing adaptive and personalized security mechanisms could provide a promising direction towards supporting human-computer interactions in such realms.

To this end a number of research questions were formulated in order to investigate the efficacy of such an approach as follows:

- Which human factors are considered important enough and influence the users' interactions with authentication and CAPTCHA mechanisms?
- Does the provision of a particular combination of security design characteristics (e.g., textual vs. graphical), based on specific human factors, have a significant effect on task performance and user experience?
- How to elicit the users' characteristics through explicit and implicit user data collection methods in order to build and maintain comprehensive user models?

- How can we build inclusive user models that will entail human cognitive characteristics of users?
- How to design and develop an extensible personalization framework specializing on adapting security tasks according to a human factor-based user model?

1.4 Problem Statement

Design and development of user authentication and CAPTCHA represents a cross-roads priority problem, between security and usability, which emerge from contradictory requirements posed by different stakeholders (**Figure 1**), inherent to the function and purpose of each user security mechanisms In particular, security experts increase continuously the security levels of user authentication and CAPTCHA, end-users demand transparent, adaptable and user-friendly solutions, and service providers are trying, together with user experience experts, to find a viable equilibrium among security and usability.

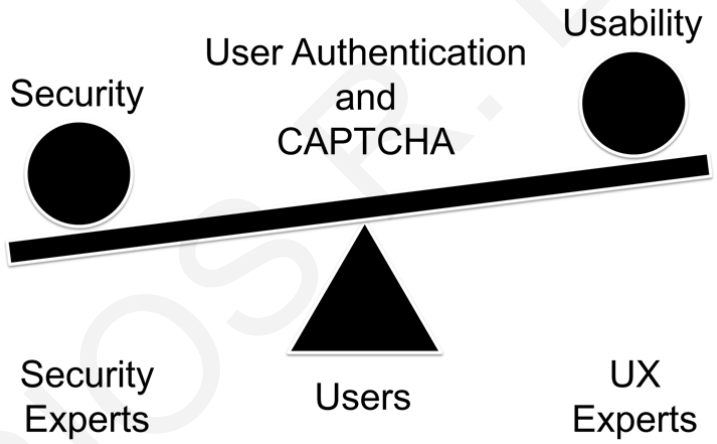


Figure 1. Security vs. usability in user authentication and CAPTCHA design

In this realm, the overarching design goal of these security mechanisms is to simultaneously increase usability, without sacrificing the level of provided security. Such a design goal however is inevitably compromised by service providers due to the increasing computing power of today's systems that are more powerful and more capable in attacking systems, forcing thus service providers to decrease the task usability in an attempt to preserve security. For example, current password mechanisms are becoming increasingly less usable and memorable through strict password policies that require users to memorize an ever-increasing number of alphanumeric and special characters (Proctor et al. 2002; Komanduri et al. 2011; Inglesant and Sasse 2010). In addition, with the increasing capabilities of Optical Character Recognition systems (OCR), current CAPTCHA mechanisms require users to recognize highly distorted text-based challenges (Yan and El Ahmad 2008; Baecher et al. 2011).

In this context, a variety of studies exist that investigated usability issues in user authentication and CAPTCHA mechanisms. An early study of Adams and Sasse (1999), which investigated pass-

word 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 (Florencio and Herley 2007). A more recent study in Inglesant and Sasse (2010) 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 just focusing on maximizing their strength. Furthermore, in the context of CAPTCHA mechanisms, a study of Yan and El Ahmad (2008) raised the usability issues of CAPTCHA and proposed a framework for evaluating various designs, while a more recent study which investigated users' perceptions toward CAPTCHA challenges underpins the necessity for user friendly CAPTCHA challenges as current implementations do not provide an acceptable trade-off solution with regards to usability (Fidas et al. 2011).

1.5 Motivation and Objectives

As discussed in the aforementioned sections, a high number of research works aimed to understand human-computer interactions in user authentication and CAPTCHA by investigating the effect of human, technology and design factors on users' preference and performance in these security tasks. According to existing research works, findings suggest that modeling such factors and applying them in user-adaptive and personalized security mechanisms could improve the user experience and eventually the users' acceptance (Belk et al. 2015a; 2015b). Yet, a common practice with regards to the design of existing user authentication and CAPTCHA mechanisms is that they do not primarily take into consideration intrinsic individual characteristics of users but rather follow a *"one-size-fits-all"* paradigm, i.e., the visual and interaction design of the security task is rarely personalized to the intrinsic characteristics of users which define them as individuals (e.g., individual traits). The majority of today's systems utilize text-based passwords and text-recognition CAPTCHA mechanisms as their sole means for security (Herley and van Oorschot 2012; Bursztein et al. 2014).

In this context, human-computer interactions with regards to user authentication and CAPTCHA mechanisms are in principal cognitive tasks that embrace perception, recognition, recalling and reasoning. Taken into consideration the diversity of humans in cognitive processing styles and abilities (Riding and Cheema 1991; Kozhevnikov 2007; Demetriou et al. 2013), this research work builds on the promise that adapting and personalizing user authentication and CAPTCHA tasks, bootstrapped on the users' cognitive processing characteristics, could provide a promising alternative to current state-of-the-art practices, aiming to support the users' efficiency and effectiveness of processing information as well as decrease cognitive load, and eventually improve the user experience and user acceptance of user authentication and CAPTCHA mechanisms.

Overarching goals of this work are to: (i) Investigate whether a balance could be achieved between usability and security in user authentication and CAPTCHA, to the extent that the one does not over-rule the other, or vice-versa; (ii) investigate whether adaptation and personalization principles could be considered as a viable trigger towards this harmonious co-existence between usability and security in user authentication and CAPTCHA; (iii) increase the understanding about the interdependencies among users' cognitive processing factors and security tasks, and accordingly study the efficacy of balancing usability and security through personalization; and (iv) lay the foundations for the design and development of a personalization framework specializing in adapting and recommending the "best-fit" design factors of security mechanisms, driven by the users' unique cognitive processing characteristics.

In order to investigate the feasibility and efficacy of such a personalization approach in user authentication and CAPTCHA, we set three key objectives as follows:

Objective 1: Investigate and model the effect and interdependencies among cognitive factors of users by taking into consideration theories of individual differences in cognitive processing (Riding et al. 1991; Kozhevnikov 2007; Peterson et al. 2009) and the actual user's tasks. Achieving this objective laid the foundations and drove the framework design.

Objective 2: Design and develop a personalization framework specializing on recommending "best-fit" user authentication and CAPTCHA tasks to users' cognitive processing styles and abilities. Accordingly, the notion of *"adaptive usable security"* has been elaborated as the ability of an interactive system that adapts to these factors aiming to provide personalized solutions to its end-users. The adaptation mechanisms are based on user models, which describe in a holistic way what constitutes the user's cognitive characteristics and preferences.

Objective 3: Evaluate the framework with the aim to improve the framework based on results gathered within ecological valid experimental designs. Continuous evaluation occurred iteratively and throughout the Ph.D. thesis, not just on the resulting mechanisms, with the extensive involvement of end-users during the development lifecycle. The aim was to implement empirical studies driven by grounded psychological and sociological theories and by gradually developing an interdisciplinary framework that would bridge technical possibilities with human factors.

These objectives have been realized through a three-phase methodology. In *Phase A* we designed and conducted several standalone and targeted user studies that investigated various and different human cognitive processing factors, aiming to understand and identify which individual characteristics are considered important enough and might affect users' interactions in user authentication and CAPTCHA mechanisms (the method and results of the studies conducted are extensively reported in chapter 7). Findings of these studies have shown several interaction effects between specific human cognitive factors and user authentication and CAPTCHA design factors in terms of task completion performance and user preference. For example, results have shown that users with Verbal cognitive styles (users that process textual information more efficiently than graphical information) prefer and perform faster in text-based password mechanisms than graphical

authentication mechanisms (Belk et al. 2014a), suggesting that Verbal users should be provided with text-based passwords in order to improve the usability of the authentication task. The aforementioned studies aimed to guide and contribute to the design of personalized user authentication and CAPTCHA mechanisms that take into consideration such intrinsic human factors.

Consequently, in *Phase B*, we have interpreted and translated the observed main effects into adaptation rules in order to map human cognitive factors with design factors of user authentication and CAPTCHA mechanisms. These adaptation rules have been formalized and applied in an extensible personalization framework, namely PAC (Personalized Authentication and CAPTCHA) (described in chapter 6), in which the user authentication and CAPTCHA tasks are personalized based on a two-phase method as follows: (i) Adapt the type of the security mechanism (textual or graphical) based on users' cognitive styles (i.e., Verbal/ Imager and Wholist/ Analyst); and (ii) adapt the complexity level of the security mechanism (number and type of characters/images) based on users' cognitive processing abilities (i.e., limited/ enhanced).

Finally, in *Phase C*, we experimentally validated PAC by investigating whether the suggested adaptation rules improve usability of user interactions and provide a positive user experience in authentication and CAPTCHA tasks.

1.6 Contributions of the Thesis

The main contribution of this thesis is the design and development of a personalization framework for adapting and recommending the "best-fit" design factors of user authentication and CAPTCHA mechanisms based on the users' cognitive processing styles and abilities. It has been proven that user's cognitive factors have an important role in various application areas (e.g., E-Learning, E-Commerce). However, the way cognitive factors used today in order to design and develop usable and secure interactions is considered unwisely and principally based on provider's perception, without following particular rules that could achieve the appropriate mapping with selected content meta-characteristics; thus personalizing the security task to the benefit of the individual user.

To the best of our knowledge, today's most popular on-line services like Facebook, Google, YouTube, Yahoo, Amazon, etc. do not exploit cognitive considerations but they rather employ customization techniques where users have direct control; users explicitly select between certain options. For example, user authentication remains the same regardless that users have different cognitive and cultural backgrounds, different preferences and needs, and develop different functional and mental models.

The added value of this thesis is derived from the combination of the principles applied to human sciences' research, with technologies provided by information science. Most studies incorporate human factors partly in the system design and take into consideration human characteristics that are extracted by the designers in a manner that is not in accordance with the research paradigm that is followed in this thesis. In this thesis the variables that concern individual cognitive charac-

teristics are emerging from grounded psychological theories and are validated through solid statistical analysis. Technology, equally important, is the medium and the area of application, which needs to embrace such "knowledge" in an innovative personalized way. A thorough integration of the two domains is possible preserving the advantages of each science and significantly reducing the possible disadvantages. Hence, the **main innovations** of this thesis are: *(a) The proposed alternative approach to current state-of-the-art practices in usable security, of mapping human factors with design factors for personalizing and supporting users during security-related interactions; (b) the identification of specific cognitive factors (cognitive styles, speed and control of processing and working memory capacity) for the personalization process of user authentication and CAPTCHA mechanisms; and (c) the formalization of an adaptation and personalization process of user authentication and CAPTCHA mechanisms.*

These innovations have been realized through the following main contributions of this thesis:

- **A proposed formalization of a human factor-based user model** (including cognitive styles, speed of processing, control of processing, working memory capacity) for personalizing security-related tasks;
- **A proposed formalization of an adaptation engine** for recommending a particular user authentication and CAPTCHA type and complexity level based on the combination of the user modeling factors;
- **A proposed Personalized Authentication and CAPTCHA (PAC) framework** incorporating the aforementioned formalizations;
- The provision of **quantitative and qualitative results that revealed the effects of human cognitive factors on user preference and task performance of different user authentication and CAPTCHA mechanisms.** These results have been based on a number of ecological valid user studies in which over 800 users have participated by modeling their cognitive processing styles and abilities, and interacting with different types of user authentication and CAPTCHA mechanisms;
- **A proposed set of guidelines and recommendation rules** for designing personalized user authentication and CAPTCHA mechanisms based on the users' cognitive characteristics.

To our knowledge, no other framework embraces the pillars of such security tasks and incorporates a dynamic cognitive-based user model that can be applied for delivery of bootstrapped user authentication and CAPTCHA challenges based on human cognitive factors. The introduction of this user model's concept extends the notion of "traditional" user authentication and CAPTCHA mechanisms, in such a way that incorporates users' cognitive characteristics, which serve as the primal personalization filtering element of user authentication and CAPTCHA tasks.

1.6.1 Publications

A number of scientific papers have been published in journals and conferences based on the outcome and main findings of this thesis. In particular, four (4) journal papers, nine (9) conference papers and two (2) workshop papers have been published prior to the submission of this thesis. Among these, our work on understanding the effect of human cognitive processing abilities on CAPTCHA-related user interactions received the best paper award at the Springer International Conference on Human Factors in Computing and Informatics (Springer SouthCHI 2013), and the work on personalizing user authentication tasks based on human cognitive differences received a best paper award nomination at the Springer International Conference on User Modeling, Adaptation and Personalization (Springer UMAP 2014). All the publications and how they are related to each chapter of this thesis are listed in Appendix A.

1.7 Thesis Overview and Structure

The remaining of the thesis is structured as follows:

Chapters 2-4 focus on the theoretical background and related works of the main areas of this thesis (Security Mechanisms, Personalization research, and Individual Differences in Cognitive Processing). In particular, chapter 2 presents state-of-the-art research works on user authentication and CAPTCHA mechanisms, pin-pointing the main design and security considerations of these mechanisms as well as related research works that investigated the effects of various factors (human and technology related) for personalizing user security tasks.

Chapter 3 analyzes the concept of user models, as a key component of adaptation and personalization systems. It presents the requirements, characteristics, implicit and explicit user data collection methods and user model generation techniques. It further refers to adaptation and personalization as a process liable to alleviate the arising difficulties and complications when users interact with various hypermedia environments. It analyzes existing issues and challenges that influence this research field and presents an extensive review of the two subsequent research domains of Web Personalization and Adaptive Hypermedia, with the related methodologies, techniques and technologies.

Chapter 4 makes a reference to the importance of human factors in Web adaptation and personalization, underpinning their dynamicity and how they can influence the design of multi-purpose interactions and interfaces. It places emphasis on specific cognitive factors that influence information processing, learning, and decision making. Main concern is to identify their impact/ consequences on the information space in various contexts and how these can be utilized in adaptation and personalization systems and services in order to increase their effectiveness and efficiency.

Chapter 5 presents in detail the three-phase methodological approach followed throughout this research endeavor in order to realize the main research objectives of this work.

Chapter 6 details an open and interoperable human-centered personalization framework, namely PAC that bridges the theoretical human perspectives with the deterministic reality of technology and the generation of adaptation rules for personalization of user authentication and CAPTCHA mechanisms. The chapter presents its main modules, components and technologies used for implementing PAC.

Chapter 7 presents a series of ecological valid user studies that aimed to investigate the effects of human cognitive factors on user preference and performance of various user authentication and CAPTCHA mechanisms.

Chapter 8 suggests a set of step-by-step practical guidelines and examples of designing adaptive and personalized user authentication and CAPTCHA mechanisms based on distinct human factors. It further presents the results of an experimental evaluation that aimed to investigate the added value of the proposed guidelines and adaptation effects, in terms of task completion performance and user preference.

Finally, Chapter 9 concludes the thesis with a discussion on the main findings, the limitations of this work, the importance and implications of the reported research and future research prospects.

In each chapter we include an introduction and a summary to directly guide the reader and increase his familiarization with the contents. We also try to consistently correlate (by adding dedicated sections in the main chapters) the various theoretical concepts and models of human factors discussed, to the adaptation and personalization process, emphasizing on implications, interpretations and methods of use.

CHAPTER 2: Usable Security – A Review of User Authentication and CAPTCHA

Nowadays, a high number of security mechanisms exist in which users play an important role in the security process. For example, users setup and make use of passwords for accessing a system, while they have to comply with security certificates and share information that highly affect the security of a system. Furthermore, security mechanisms are deployed on the World Wide Web in which many users are required to interact as secondary tasks in order to proceed with their primary one. For example, they are required to solve a CAPTCHA challenge to prove that they are humans in order to proceed with their main task (e.g., posting a comment in an online blog). Such practices have shown to significantly decrease the experience of users while interacting with the system (Fidas et al. 2011).

In this realm, the research community has come to an understanding regarding the critical importance of *usable security* which is an area that focuses on how to design and develop security mechanisms that respect users' performance and their goals within an interactive system (Cranor and Garfinkel 2005; Kobsa et al. 2013; Shay et al. 2012; Inglesant and Sasse 2010; Florencio and Herley 2007; Fidas et al. 2011; Bursztein et al. 2014). There is a growing demand and interest to enhance both the security and the usability aspects of such mechanisms aiming to meet the security requirements of the system but at the same time to provide interaction transparency to actual users (Inglesant and Sasse 2010; Fidas et al. 2011; Biddle et al. 2012). However, usable security is still an open and challenging research area mainly due to the lack of in-depth understanding of user security tasks and their intuitive integration in the user interface design process by following user-centered design approaches (Fidas et al. 2010). User-centered design approaches focus on interacting iteratively with the end-users, especially for identifying and validating user requirements, designing system prototypes as well as for evaluating them. The aim is to investigate thoroughly what users require from a system design and how the system can support them in accomplishing specific tasks effectively, efficiently, and with a certain degree of user satisfaction. An important aspect of this process is to model a user's interaction with a user interface. A good design practice aims to establish a common ground among designers and users related to aspects of the user-system interaction by formalizing the information architecture of the respective interactive system and specify the interaction flow for accomplishing specific tasks.

As mentioned in chapter 1, user security interactions over the World Wide Web are commonly related with: (a) User authentication; (b) human interaction proof mechanisms (e.g., CAPTCHA challenges – von Ahn et al. 2004); (c) installation and usage of data encryption software tools, especially for secure e-mail communication; and (d) installation of certificates for authorization issues, etc. In this respect, research on usable security entails a high number of challenges and issues due to the multidimensional and complex character of each security mechanism. The two areas that receive significant attention from the research community (and that we also focus in this thesis) are

those of user authentication and CAPTCHA challenges. Both security mechanisms are currently widely deployed in online services and are of critical importance for the security of today's interactive systems. User authentication on the one hand aims to verify that the identity of a user is genuine, whereas CAPTCHA challenges aim to prove that the entity interacting with a service is human and not malicious software. These tasks are currently performed by millions of users as part of their daily activities, thus having a usability flaw in such human-computer interaction cycles could eventually decrease the overall user experience and user acceptance of an interactive system.

In the rest of this chapter we will make an overview of user authentication and CAPTCHA mechanisms, identifying the design and security considerations and constraints of each mechanism. Next we present research works that studied the effect of several human, technology and design factors of user authentication and CAPTCHA mechanisms whose results suggest that personalizing these mechanisms to the unique characteristics of users could improve the user experience and user acceptance.

2.1 User Authentication

User authentication is the process of verifying the physical identity of a person and is a vital component of any security infrastructure of today's interactive systems. During an authentication task, users are required to provide specific secret information in order to prove their identity. Depending on the factor used for authentication, researchers and practitioners promote different mechanisms; *knowledge-based authentication mechanisms* that require from users to either memorize and provide a sequence of characters (e.g., password, personal identification number (PIN)) or a sequence of images; *token-based authentication mechanisms* that require a specific object from users such as a credit card; or *biometric-based authentication mechanisms* that require biometric information from users such as fingerprint information. In this thesis we primarily focus on knowledge-based authentication mechanisms (that principally require users' cognitive processing) with the aim to assist users during such cognitive tasks by providing personalized user authentication tasks bootstrapped on their preferred cognitive processing styles and abilities. Figure 2 illustrates examples of knowledge-based user authentication mechanisms, and Figure 3 illustrates examples of token-based, biometric-based and multi-factor user authentication mechanisms.

In the context of knowledge-based authentication mechanisms, the literature reveals many proposals for improving the usability and user experience of text-based password authentication and graphical authentication mechanisms. Text-based password mechanisms principally require from users to memorize a sequence of alphanumeric characters to gain access to a resource. Accordingly, research works have focused on providing guidance and feedback during password creation (Shay et al. 2015), and assisting users to create memorable passwords, e.g., through image-based mnemonic techniques (Nelson and Vu 2010), text-recognition techniques (Wright et al. 2012) and password policies (Komanduri et al. 2011; Inglesant and Sasse 2010; Vu et al. 2007). Graphical

authentication mechanisms require from users either to solely remember information and reproduce a secret drawing on a static image (recall-based) (Jermyn et al. 1999; Gao et al. 2008; Tao and Adams 2008; Wiedenbeck et al. 2005; Biddle et al. 2012; Chiasson et al. 2008) or create an authentication key by selecting and memorizing specific images, and then recognize the images among decoys to authenticate (recognition-based) (Passfaces 2009; Mihajlov and Jerman-Blazic 2011; Nicholson et al. 2012).

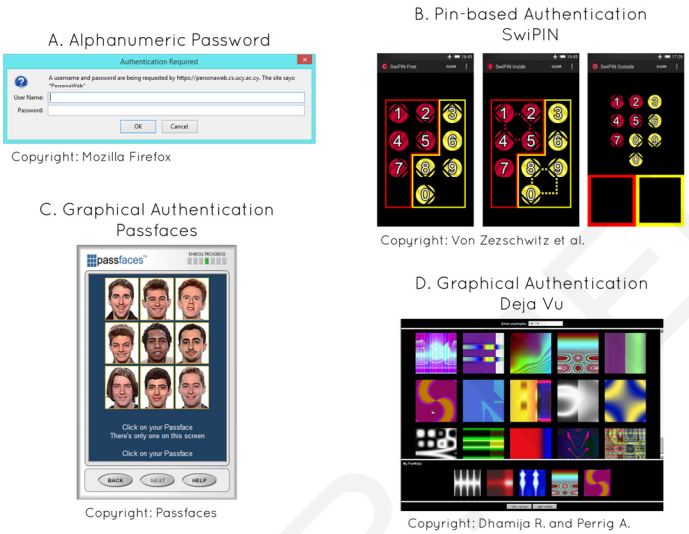


Figure 2. Knowledge-based user authentication mechanisms

A. Alphanumeric Password; B. Pin-based Authentication with SwiPIN (Von Zezschwitz et al. 2015); C. Recognition-based Graphical Authentication with Passfaces (Passfaces 2009); D. Recognition-based Graphical Authentication with Déjà vu (Dhamija and Perrig 2000).

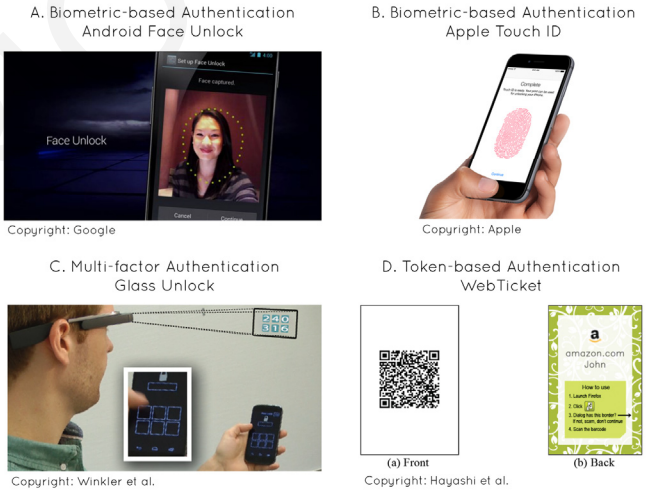


Figure 3. Token-based, biometric-based and multi-factor user authentication mechanisms

A. Biometric-based Authentication with Android Face Unlock (Google); B. Biometric-based Authentication with Apple Touch ID (Apple); C. Multi-factor Authentication with Glass Unlock (Winkler et al. 2015); D. Token-based Authentication with WebTicket (Hayashi et al. 2012)

2.2 Human Interaction Proofs (CAPTCHA)

Human Interaction Proofs (HIP) are security defense mechanisms aiming to prove that the entity interacting with a system is a human being and not a malicious software (Chellapilla et al. 2005). A Completely Automated Public Turing test to tell Computers and Humans Apart (CAPTCHA – von Ahn et al. 2004) is an example HIP mechanism which is widely used today by service providers to protect their systems against automated software attacks (e.g., denial of service attacks, password dictionary attacks, etc.). CAPTCHA challenges typically require from legitimate users to solve visual cognitive-based challenges before performing the primary task of interaction in a system. For example, systems require from users to recognize distorted alphanumeric characters or solve image puzzle problems before commenting on a Web-site. Main aim of this process is to prevent a possible automated software attack that could automatically generate and send thousands of comments in the system that would decrease the quality of services. These challenges are based on the assumption that they can be easily solved by humans but present significant difficulty for computing systems (e.g., Optical Character Recognition (OCR) or other image-recognition systems).

Recent research works underpinned the necessity for designing usable CAPTCHA challenges since studies have shown that current CAPTCHA schemes are difficult to solve and frustrate users (Fidas et al. 2011; Bursztein et al. 2010). In this context, researchers and practitioners promote different types of challenges aiming to address usability issues of CAPTCHA, without compromising security. Depending on the type of challenge, current CAPTCHA implementations are classified in the following three categories: (i) *Text-recognition challenges* require from a legitimate user to type alphanumeric characters based on a distorted image that appears on the screen (von Ahn et al. 2008; Bursztein et al. 2014; Chew and Baird 2003); (ii) *image-recognition challenges* require from users to solve image puzzle problems and annotate static or animated images (e.g., select images of a particular theme – Elson et al. 2007; Vikram et al. 2011; Gossweiler et al. 2009); and (iii) *speech-recognition challenges* that require users to listen and recognize a recording of simple words and numbers which entails disturbance and noise (Bigham and Cavender 2009; Holman et al. 2007; Gao et al. 2010). Figure 4 illustrates selected CAPTCHA mechanisms of each category.

The literature also reveals a high number of alternative CAPTCHA mechanisms that follow hybrid approaches that combine text- and image-recognition challenges, drag-and-drop interactions, semantic approaches, etc. Examples include NuCAPTCHA that illustrates animated instead of static text in the challenge (NuCAPTCHA 2015), Emerging (Xu et al. 2014) which is an alternative approach that addresses security flaws found in NuCAPTCHA, SolveMedia CAPTCHA that incorporates brand advertisements in the challenge and users are required to type the text of an advertiser's brand text (SolveMedia 2015), video approaches such as the work of Kluever and Zanibbi (2009) that proposed a technique for using content-based video labeling as a CAPTCHA challenge and users are then required to label these videos to pass the challenge, and sweetCAPTCHA that is

an action-based CAPTCHA in which users are required to drag-and-drop specific objects onto other objects (e.g., *"drag the shoes into the box"* or *"drag the carrot to the bunny"* (Figure 4F)).

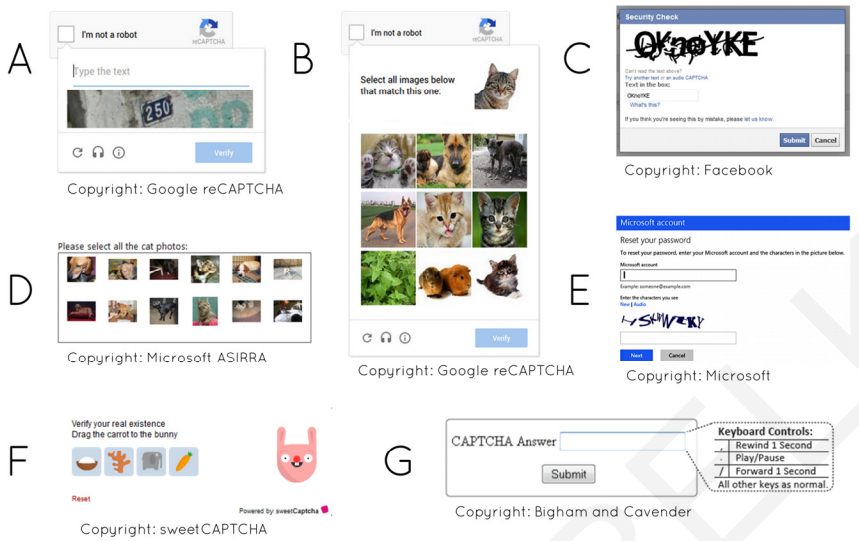


Figure 4. Selected CAPTCHA schemes

A. NoCAPTCHA reCAPTCHA (text-recognition); B. NoCAPTCHA reCAPTCHA (mobile friendly image-recognition); C. Facebook CAPTCHA (text-recognition); D. Microsoft ASIRRA (image-recognition) (Elson et al. 2007); (E) Microsoft CAPTCHA (text-recognition); F. sweetCAPTCHA (drag-and-drop interaction); G. Non-visual Access CAPTCHA (speech-recognition) (Bigham and Cavender 2009)

2.3 Design Considerations and Constraints

An important challenge of any adaptation and personalization system is to identify which aspects of the system can be adapted and why, with the aim to improve the usability and experience of user interactions. Accordingly, we identified and present the design and security considerations of knowledge-based user authentication and CAPTCHA mechanisms.

2.3.1 Design Considerations in Knowledge-based User Authentication

Knowledge-based authentication mechanisms (*"what the user knows"*) require from the user to memorize specific information (e.g., password, passphrase, PIN code, sequence of images, etc.). Text-based passwords are the dominant means for authentication and are currently utilized in the majority of computing systems worldwide since they are familiar to most of the users, and easy and inexpensive to implement (Herley and van Oorschot 2012; Herley et al. 2009). Nevertheless, passwords have always been criticized about their security flaws (Bonneau et al. 2012). Various studies have been reported that underpin the necessity for secure and usable authentication mechanisms

(Shay et al. 2012; Komanduri et al. 2011; LeBlanc et al. 2010; Shay et al. 2010; Inglesant and Sasse 2010; Florencio and Herley 2007; Adams and Sasse 1999). The literature reveals many proposals for improving password security, such as educating and influencing users to create more secure passwords (Forget et al. 2008; Forget and Biddle, 2008; Yan et al. 2004), improving existing recall-based password approaches with recognition of text (Wright et al. 2012), enforcing the creation of secure passwords through password policies (Komanduri et al. 2011; Inglesant and Sasse, 2010; Vu et al. 2007; Florencio et al. 2007), automatically generating secure passwords and mnemonic passphrases (Kuo et al. 2006; Leonhard and Venkatakrishnan, 2007). Furthermore, password managers (Halderman et al. 2005; Chiasson et al. 2006) have been proposed to minimize users' cognitive load.

A great amount of research of knowledge-based authentication mechanisms has focused on the design and implementation of graphical authentication schemes (see Biddle et al. (2012) for a recent review). This is further strengthened by the technological shift of current computing systems toward touch-based devices in which entering textual information (in this case, text-based passwords) on touch-based keyboards is a demanding task (Findlater et al. 2011). In addition, graphical authentication mechanisms claim to preserve security and improve usability and memorability of user authentication as they leverage the vast capacity and capabilities of the human visual memory system (Angeli et al. 2005; Everitt et al. 2009; Biddle et al. 2012) and are memorable over extended periods of time (Tullis et al. 2011). Principally, graphical authentication mechanisms require from a user to enter an authentication key represented by images in a specific sequence. Graphical authentication schemes can be classified into three categories according to the memory task in remembering and entering the authentication key; *recall-based*, *cued-recall-based* and *recognition-based authentication*.

Recall-based authentication mechanisms require that users remember information and reproduce a secret drawing on a static image as their authentication key. The first recall-based authentication mechanism proposed was Draw-a-Secret (DAS – Jermyn et al. 1999) where users draw their authentication key on a two dimensional grid. Variations of the first DAS system that aimed to improve some of its usability issues include BDAS (Dunphy and Yan 2007) which added background images to the existing DAS to encourage the creation of stronger authentication keys, YAGP (Yet Another Graphical Password – Gao et al. 2008) that modified DAS to accept approximately correct drawings, Passdoodle (Varenhorst 2004) that added additional factors, such as, pen color, number of pen strokes, drawing speed for the matching process to add variability of drawings, Pass-Go (Tao and Adams 2008) where users draw their authentication key using grid intersection points, as well as commercial applications of Pass-Go, like Google Android mobile phones for unlocking screens by drawing an authentication key on a 3x3 grid.

Cued-recall authentication mechanisms require users to identify specific locations on a static image and are intended to reduce the memory load on users since specific cues are utilized in order to assist the recall of information. The dominant cued-recall authentication system is PassPoints

(Wiedenbeck et al. 2005) and its variations (Biddle et al. 2012). In PassPoints, users click anywhere on a picture, with a tolerance metric defined around each click-point to avoid the need for pixel-perfect entries in the future. Variations include Persuasive Cued Click Points (Chiasson et al. 2008) that assists users to select random authentication keys by highlighting a random part of the picture where the click has to occur. Recently, Bulling et al. (2012) have proposed a gaze-based authentication scheme that supports users in selecting secure gaze-based graphical passwords. In particular, the proposed authentication scheme uses saliency maps to mask out those areas of the image most likely to attract visual attention with the aim to increase the security of gaze-based cued-recall graphical authentication mechanisms.

Recognition-based authentication mechanisms require that the user creates an authentication key by selecting and memorizing specific images, and then recognize the images among decoys to authenticate. The most popular and extensively researched recognition-based graphical authentication system to date is Passfaces (2009) that uses human faces as part of the authentication key. Variations have been proposed that use different content in images, like the Story system (Davis et al. 2004) that uses everyday objects, places and people as the authentication key, and ImagePass (Mihajlov and Jerman-Blazic 2011) that utilizes single-object images as the authentication key. Another recent work proposed the Tiles system (Nicholson et al. 2012) in which users are assigned a target image and subsequently asked to select segments of that image with the aim to help mitigate the threat from verbal sharing and observation attacks.

To this end, knowledge-based user authentication mechanisms, and more specifically text-based passwords and graphical authentication mechanisms entail various design features. Based on the aforementioned analysis, we categorize important and widely used features as follows: (i) Design type (e.g., text-based, picture-based); (ii) interaction design type (e.g., selecting images/ text vs. typing text vs. touching visual images/ text objects vs. drawing patterns); (iii) image type (faces, abstract or single-object); (iv) number of user-selected images/ characters for the authentication key; (v) number of decoy images illustrated during graphical authentication; (vi) the policy of the authentication key (e.g., allow or not using the same image multiple times in a single key); (vii) the procedure for graphical authentication (e.g., showing more decoy images in one screen vs. showing less decoy images in multiple screens) (Ma et al. 2013).

2.3.2 Security Considerations in Knowledge-based User Authentication

The literature reveals that various user authentication schemes entail different security strengths and weaknesses (Renaud et al. 2013; Biddle et al. 2012), since in each case different factors exist that affect the security of the authentication mechanisms. According to Biddle et al. (2012), attacks can be classified in two broad categories; *guessing attacks* or *capture attacks*. Guessing attacks are considered an important threat in user authentication. These are either performed online in which the attacker guesses and enters the authentication key through the live login interface or performed

offline in which the attacker first gains full access to the system's database that contains verifiable authentication keys (e.g., hashes). In both text-based and graphical authentication, online guessing attacks can be prevented by using additional security measures that are enabled after consecutive unsuccessful logins (e.g., CAPTCHA). Offline guessing attacks are prevented by processing the authentication key through a hash function in case the attacker gains full access to the authentication keys. Thus, the attacker is required to check if an authentication key attempt is correct by first hashing the guessed key and then compare it to the value stored in the database. Accordingly, the theoretical space of an authentication key is vital for preventing offline guessing attacks. Thus, in both text-based and graphical authentication mechanisms, the number and type of images has a significant effect on guessing attacks (Komanduri et al. 2011; Biddle et al. 2012).

Capture attacks aim to acquire the authentication key by capturing data while the user enters the authentication key during login. Most common capture attacks include: (i) *Shoulder surfing attacks* in which the attacker visually observes the user entering the authentication key; (ii) *phishing attacks* (password fishing); (iii) *social engineering* in which users might share their authentication key (either willingly or through phishing); and (iv) *malware attacks* (malicious software). A high number of research works have focused on minimizing threats of shoulder surfing attacks, such as De Luca et al. (2013) that proposed an approach using fake cursors in on-screen password mechanisms and Winkler et al. (2015) that proposed a hybrid approach for preventing shoulder surfing attacks on smartphones by leveraging a private near-eye display (i.e., Google Glass). Researchers have also focused to prevent social engineering by assisting users to create secure and memorable passwords (Nelson and Vu 2010; Wright et al. 2012) as well as investigating the type of image used in graphical authentication mechanisms (Mihajlov and Jerman-Blazic 2011).

2.3.3 Design Considerations in CAPTCHA

An acceptable CAPTCHA solution should embrace both security and usability aspects as its purpose is to provide safety of operation to Web application providers but as well usability and transparency to its end users, aiming to minimize the added cognitive effort of a casual user interacting with it. Various studies have been reported that underpin the necessity for increasing usability of current CAPTCHA implementations. A study of Yan and El Ahmad (2008) raised the usability issues of CAPTCHA and proposed a framework for evaluating various designs. A recent study which investigated users' perceptions towards CAPTCHA challenges underpinned the necessity for user friendly CAPTCHA challenges as current implementations do not provide an acceptable trade-off solution with regards to usability (Fidas et al. 2011). Results have shown that even experienced users expressed their difficulties in solving a CAPTCHA challenge during their first attempt (Fidas et al. 2011).

In this context, research on CAPTCHA mechanisms has received significant attention lately aiming to increase security but at the same time usability. Researchers promote among others inter-

action with pictures, audio and video as a possible alternative to text-based CAPTCHA (Elson et al. 2007; Vikram et al. 2011; Ross et al. 2010; Gossweiler et al. 2009; Kluever et al. 2009). Accordingly, current CAPTCHA implementations can be classified into three broad categories: *text-recognition*, *image-recognition*, and *speech-recognition*.

Text-recognition CAPTCHA, which are also the most widely used today, require from a legitimate user to type letters or digits based on a distorted image that appears on the screen. Popular text-recognition CAPTCHA include among others reCAPTCHA (von Ahn et al. 2008), BaffleText (Chew and Baird 2003) and Gimpy (von Ahn et al. 2004). Furthermore, major Web service providers such as Google, Facebook, Microsoft and many others utilize text-recognition CAPTCHA to protect their services against automated software attacks (Bursztein et al. 2010).

Image-recognition CAPTCHA are usually based on image puzzle problems and annotation of static and animated images. For example, in ASIRRA (Elson et al. 2007), users are required to select pictures that illustrate cats among dogs. SEMAGE (Vikram et al. 2011) similarly requires users to recognize the content of a set of images, but as well understand and identify the semantic relationship between a subset of them. Other popular examples include IMAGINATION (IMAge Generation for INternet AuthenticaTION) (Datta et al. 2005), that uses a two-round click-and-annotate process in which a user needs to first click on the geometric center of an image among a composite image tiled with multiple distorted images, and then annotate a distorted image of a simple object with one word of an available list of words, ARTiFACIAL (Rui and Liu 2004), where users are required to identify a single human face in a challenge, and click the six facial corners (four eye corners and two mouth corners) on the face to pass the challenge, Sketcha (Ross et al. 2010) and What's Up CAPTCHA (Gossweiler et al. 2009), that require users to adjust randomly rotated images to their upright orientation.

Finally, *speech-recognition CAPTCHA* are usually based on audio comprehension which principally require users to enter the words and numbers listened from a recording of a combination of simple words and numbers where disturbance and noise has also been added. Speech-recognition CAPTCHA are more difficult to solve and internationalize, and more demanding in terms of time and efforts in comparison with text-recognition and image-recognition CAPTCHA. However, audio-based CAPTCHA challenges have become an alternative for visually-impaired people. Examples include Text-to-Speech (Chan 2003) and human in contrast to synthetic voice recognition (Gao et al. 2010). In this thesis we primarily focus on text- and image-recognition CAPTCHA rather than speech-recognition CAPTCHA since these are considered a significantly more demanding task in terms of solving time and are mostly used for users with physical impairments which is out of the scope of this thesis (Bigham and Cavender 2009).

2.3.4 Security Considerations in CAPTCHA

The success rate of an attack is the primary metric to evaluate CAPTCHA attack effectiveness (Zhu et al. 2010) and several research works have investigated the impact of specific design factors on CAPTCHA security (Bursztein et al. 2014; 2011; Golle 2008; Zhu et al. 2010). The work of Bursztein et al. (2014; 2011) has shown that specific text features in text-recognition CAPTCHA challenges affect the security of the mechanism. In particular, the following features affect the security (and the usability) of the challenge: (i) The length and font size used in the challenge; (ii) the rotation and collapse of the characters; and (iii) the number, width and color of lines illustrated in the challenge. The work of Bursztein et al. (2011) also showed that incorporating background images with noise is ineffective to attacks.

The works of Golle (2008) and Zhu et al. (2010) revealed that the security of image-recognition CAPTCHA challenges are affected by the following factors: (i) Number, type and color of objects used in the challenge; (ii) the semantic meaning of the objects used in the challenge; and (iii) the source and generation of the objects (i.e., new challenges should be independent to past challenges). Furthermore, the work of Golle (2008) revealed that degrading the quality of the object or using distortion (as in text-recognition challenges) is ineffective to attacks, but rather decreases the usability of the challenge.

Finally, based on the work of Bigham and Cavender (2009), the security of speech-recognition CAPTCHA is affected by the number of characters used in the challenge, the alphabet and the added background noise in the narration.

2.4 Personalization in User Authentication and CAPTCHA

A recent streamline of research has focused on the influence of specific human, technology and design factors affecting user authentication and CAPTCHA task performance. Main aim of these works is to understand human-computer interactions in such realms, and further apply that knowledge in designing usable authentication and CAPTCHA mechanisms.

2.4.1 Understanding Human Interactions in User Authentication

Recent research works investigated the effects of several factors (human, technology, design) on user authentication (Table 1). For example, Nicholson et al. (2013) suggested personalizing the user authentication type based on age differences. In particular, this research work investigated age differences (young users and older adults) in various user authentication types (i.e., personal identification numbers (PIN) and graphical authentication), regarding the number of attempts needed to authenticate. Results revealed that young users need less attempts to authenticate than older adults

on both graphical and PIN. Furthermore, young users do not have significant differences in number of attempts between graphical and PIN, whereas older adults need less attempts on graphical compared to PIN. Belk et al. (2014a; 2014b) recently investigated how users' cognitive styles (Verbal and Imager) and cognitive processing abilities' (limited and enhanced) affect task completion performance between text-based and graphical authentication mechanisms. In particular, results revealed that overall, users authenticate faster with text-based passwords compared to graphical authentication, with Verbal users being faster than Imager users, whereas Imager users perform more efficiently in graphical authentication mechanisms, compared to Verbal users. Furthermore, users with enhanced cognitive processing abilities authenticate faster and need less attempts in graphical authentication than users with limited abilities, whereas in text-based passwords, no significant differences exist between limited and enhanced cognitive abilities' groups. Such results suggest personalizing user authentication tasks by adapting the type of user authentication (textual or graphical) based on the users' cognitive processing styles and abilities. Ma et al. (2013) investigated how cognitive disabilities of users (users with Down syndrome vs. neuro-typical users) affect task performance and user preference of text-based passwords and graphical authentication mechanisms. Results revealed that overall, text-based passwords are completed faster and with less attempts than graphical authentication. Users with Down syndrome need more time to create and enter a username and password than neuro-typical users. Furthermore, persons with Down syndrome are able to quickly learn and memorize the graphical authentication key suggesting that graphical authentication mechanisms could be a valid alternative for users with Down syndrome. In addition, the research suggests that Web service providers should offer personalized authentication functions that allow the users to select their preferred authentication types. In a similar approach, Forget et al. (2014) recently proposed a work-in-progress authentication scheme for enabling users to choose the preferred user authentication mechanism (e.g., text or graphical) instead of providing a one-size-fits-all user authentication type.

Table 1. Factors affecting the user experience of user authentication

Authors	Human	Technology	User Authentication Design
Nicholson et al. (2013)	Age differences (younger vs. older adults)	-	PIN and graphical
Belk et al. (2014a)	Cognitive styles (Verbal vs. Imager)	-	Password and graphical
Belk et al. (2014b)	Cognitive processing abilities (limited vs. enhanced)	-	Password and graphical
Ma et al. (2013)	Cognitive disabilities (Down syndrome vs. neuro-typical)	-	Password and graphical

Forget et al. (2014)	User preference	-	Any user authentication type
von Zezschwitz et al. (2014)	-	Device type (desktop, tablet, smartphone)	Password
Schlöglhofer et al. (2012)	-	Smartphone	PIN, text-based passwords and graphical authentication
Schaub et al. (2012)	-	Smartphone	Virtual keyboard layout (iOS, Android, Windows Phone, Symbian, MeeGo)

From the technology perspective, recent research investigated how several technology factors affect user authentication task performance and user behavior, such as device type, interaction design and virtual keyboard layout (von Zezschwitz et al. 2014; Schlöglhofer et al. 2012). The main findings of the studies suggest that user authentication mechanisms should be personalized based on the interaction device type. In particular, von Zezschwitz et al. (2014) recently investigated the effect of device type (desktop computers, tablets, smartphones) on password entry performance, users' password choice and users' security behavior. Results revealed that password input in mobile devices is slower than desktop computers and that users choose easy and fast to enter passwords for mobile devices compared to desktop computers. Schlöglhofer et al. (2012) compared also different authentication types (PIN, text-based passwords and graphical authentication) regarding device unlock function duration on smartphones. Results suggest that PINs are the fastest to enter, graphical authentication is considered as usable as PINs and passwords are the least usable in terms of time to authenticate on smartphones. Schaub et al. (2012) compared different virtual keyboard layouts (iOS, Android, Windows Phone, Symbian, MeeGo) regarding password entry performance and composition. Significant differences were observed between different virtual keyboards in password entry time and error rates, with Windows Phone and iOS virtual keyboards being the most usable (fast password entry times and high typing accuracy).

2.4.2 Understanding Human Interactions in CAPTCHA

A number of research works have also focused on the individuality of users and accordingly utilize the users' individual and contextual characteristics to provide more usable and personalized CAPTCHA. Table 2 summarizes several research attempts that investigated the effects of human, technology and design factors on CAPTCHA. In this context, a recent work of Fidas et al. (2015) has overviewed existing user studies that revealed a main effect of several human, technology and design factors on CAPTCHA challenges, and accordingly proposed a conceptual framework for

personalizing CAPTCHA challenges by incorporating these factors in an individual context model. Furthermore, results of a study reported in Fidas et al. (2011) suggested that lingual characteristics of users should be considered for personalizing text-recognition CAPTCHA challenges since a considerable number of participants prefer to solve text-recognition CAPTCHA that are using characters from their native-speaking language alphabet instead of the traditional Latin-based. Another research work of Belk et al. (2012a; 2015a) suggested that cognitive styles and cognitive processing abilities of users affect preference and performance with respect to different types of CAPTCHA challenges (text-recognition and image-recognition) as well as different complexity levels of CAPTCHA. Results of the studies revealed a positive tendency of Imager users preferring and performing efficiently in image-recognition CAPTCHA, in contrast to Verbal users that significantly performed faster and preferred text-recognition than image-recognition CAPTCHA. Furthermore, users with enhanced cognitive processing abilities were significantly faster in solving the text-recognition CAPTCHA than users with limited cognitive processing abilities. From an accessibility perspective, Bigham and Cavender (2009) proposed personalized CAPTCHA for supporting users with vision problems and other disabilities. Other personalization examples include Geo-CAPTCHA that provides personalized content in the CAPTCHA challenge such as geographic information of the user which is only known to the user, aiming to prevent third party human attacks but as well to improve usability (Wei et al. 2012), and the work of Albert et al. (2010) that proposed a two-level image-based CAPTCHA utilizing additional personal information of the user as part of the challenge (e.g., mother's maid name of the user).

Table 2. Factors affecting the user experience of CAPTCHA

Authors	Human	Technology	CAPTCHA Design
Fidas et al. (2011)	Lingual differences	-	Text-recognition
Belk et al. (2012a)	Cognitive styles	-	Text-recognition, image-recognition
Bigham and Cavender (2009)	Users with vision problems	-	Speech-recognition
Wei et al. (2012)	Users' geographic location	-	Text-recognition
Albert et al. (2010)	Users' personal information	-	Text-recognition
Wismer et al. (2012)	-	Smartphones	Text-recognition, image-recognition, speech-recognition
Reynaga and Chiasson	Users' context while interacting	Smartphones	Network and bandwidth usage

(2013)	(standing, sitting, walking)		
Shirali-Shahreza et al. (2013)	-	Smartphones	Text-recognition
Chow et al. (2008)	-	Smartphones	Text-recognition

From the technology perspective, a recent study of Wismer et al. (2012) compared the usability of text-, image- and speech-recognition CAPTCHA on mobile devices, suggesting the users' positive attitude and preference towards solving image-recognition CAPTCHA when these are deployed on mobile devices. Reynaga and Chiasson (2013) suggested to personalize mobile-based CAPTCHA interactions based on the users' context while interacting (e.g., standing, sitting, walking) as well as taking into account network and bandwidth usage. Furthermore, research works have proposed CAPTCHA mechanisms that leverage interaction design capabilities of mobile devices, such as SeeSay CAPTCHA (Shirali-Shahreza et al. 2013) that is specifically designed for mobile users, that requires users to say the answer to the system (instead of typing it) based on a visual stimulus. In the same context, Clickable CAPTCHA (Chow et al. 2008) was proposed for personalizing text-recognition CAPTCHA for mobile-based interactions by converting the text-based challenge into a clickable challenge aiming to simplify and speed-up the entry of the text-based solution.

2.5 Summary

User security interactions over the World Wide Web are commonly related to user authentication and CAPTCHA mechanisms (Florencio and Herley 2007; Bursztein et al. 2014). Studies have already shown a number of usability and user experience issues in such human-computer interaction cycles and the research community has acknowledged the necessity for designing more usable security mechanisms (Fidas et al. 2011; Florencio and Herley 2007). Furthermore, a high number of research works have shown that human factors affect user interactions in both user authentication and CAPTCHA mechanisms in various contexts of use, suggesting that personalization strategies may assist the design and development of more usable security mechanisms.

In this respect, this thesis aims to propose an alternative approach to current state-of-the-art practices with the aim to achieve a balance between usability and security of two widely deployed and critical security mechanisms. The purpose of this chapter was to review existing research works in user authentication and CAPTCHA in order to better understand and identify the main design and security factors that could play an important role in the adaptation and personalization process of user authentication and CAPTCHA mechanisms.

CHAPTER 3: User Modeling, Adaptation and Personalization

Engineering interactive systems under the notion of user-centered design approaches does not always intuitively embed features that correspond to the users' characteristics and needs. A challenge met especially in current interactive systems is to dynamically adapt the content presentation and functionality of the system based on explicitly or implicitly retrieved information about the user, aiming to improve usability and provide a positive user experience. In this context, adaptive user interfaces (Schneider-Hufschmidt et al. 1993; Brusilovsky 2001) in interactive systems provide an alternative to the "one-size-fits-all" approach of static user interfaces by adapting the system's structure, terminology, functionalities and presentation of content to users' perceptions, needs and preferences, aiming to increase the usability of the interface and provide a positive user experience.

Starting with a few pioneering works on adaptive hypertext in the early 1990s, personalization research now attracts many researchers from different communities such as hypermedia, user modeling, machine learning, natural language generation, information retrieval, intelligent tutoring systems, affective computing, cognitive science, and Web-based education (Brusilovsky and Maybury 2002). The most important and most elaborate works on adaptive user interfaces were originally developed in the fields of information retrieval (Korfhage 1997) and intelligent tutoring systems (Sleeman and Brown 1982). Information retrieval and filtering systems attempt to find documents that are most relevant to user interests and then to order them by the perceived relevance. Intelligent tutoring systems (ITS), strive to select educational activities and deliver individual feedback that is most relevant to the user's level of knowledge.

Various recent research works exist in the literature that propose different approaches for adaptation and personalization, like the work of Reinecke and Bernstein (2011) suggesting an approach for adapting user interfaces based on the cultural preferences of users; Li et al. (2013) proposing an adaptive spellchecker and predictor for people with dyslexia that can adapt its model and interface according to the users' individual behavior; Cheng et al. (2013) recommending an implicit user modeling approach that automatically adapts the layout and position of virtual keyboards based on how and where users are grasping the tablet device; and Matuszyk and Spiliopoulou (2014) emphasizing on a collaborative filtering method for constructing a user's neighborhood by selecting only those users that are reliably similar to the user.

Furthermore, today's major Web information retrieval systems have showed a certain degree of recognition towards this approach, such as Google (2015a), Bing (2015), and Amazon (2015) that offer personalized results and recommendations, by employing adaptation technologies and techniques. These service providers have been offering personalized results and recommendations by employing various intelligent user modeling and adaptation algorithms. Popular approaches for recommendation include collaborative filtering and content-based filtering (Pazzani and Billsus 2007; Konstan and Riedl 2012). Collaborative filtering first collects and analyzes data about the users' interactions with the system or the users' preferences, and then predicts for the rest of the

users their future preferences based on the similarity of their interests. Content-based filtering creates a user profile based on a weighted vector of the item features appearing in the content which is more frequently visited by the user. The weights indicate the importance of each feature to the user. Furthermore, various algorithms are employed to recommend new items that are similar to the weighted vector of the user. Various machine learning techniques are used to predict user preference or estimate the probability that users will like particular items, such as cluster analysis, classification, decision trees, and artificial neural networks.

Although the notion of personalization has found its way in users' everyday interactions in Web interactive systems, various research issues are still open with regard to the most influential factors of personalization, such as the behavioral drivers and navigation interaction of users in executing task-oriented reasoning processes. In addition, there is lack of understanding of the relation between individual styles, cognition levels (abilities), emotional processing characteristics and navigation behavior within interactive systems. An interesting example is the case of users' interactions with online content, such as content included in encyclopedia articles. In that case, based on observations of human behavior and preference, the personalization process could influence both the way content is represented as well as the way the content is structured, and thus may have a significant impact on improving the users' experience. Assuming that the content of Web interactive systems can be presented in two ways, either as a visual or a verbal representation of information, illustrating the same content, and users may go through the content in a specific navigation pattern (or navigation behavior), we suggest that individual differences in cognitive styles, which describe the way individuals perceive, process and organize information (Riding and Cheema 1991), might be applied effectively for facilitating the user modeling process of adaptive Web interactive systems (Germanakos et al. 2008). In this context, the most widely accredited cognitive style dimensions are the Verbal/ Imager dimension that indicates the habitual approach and preference of users representing information verbally or graphically, and the Wholist/ Analyst dimension, which describes the way individuals organize and process information in a holistic or an analytic approach (Peterson et al. 2009; Riding and Cheema 1991).

From a technical point of view, an important challenge for designing an effective adaptation and personalization system is to study and incorporate structures of meta-data (i.e., semantics) at the Web content provider's side, as well as propose the construction of a Web-based adaptation mechanism that will serve as an automatic filter, adapting the distributed Web content based on the user's characteristics. Semantic mark-up can contribute to the whole adaptation process with machine-understandable representation of Web content. In this context, machine-understandable data can be incorporated in the design of Web-based systems to inform the adaptation mechanism of the intention of specific sections and accordingly adapt them based on the user's characteristics and adaptation rules (Belk et al. 2012b; Hori et al. 2004).

This chapter presents the underlying principles of user modeling, adaptation and personalization. It initially presents the underlying principles of user modeling by presenting the most common

user modeling factors for adaptation and personalization, existing explicit and implicit data collection methods for eliciting such factors and state-of-the-art user model generation mechanisms. We further present the main personalization categories and adaptation technologies from a technical and design perspective. From a technical perspective we focus on the main personalization categories and adaptation technologies for adapting content and functionality based on the characteristics of each user. From the design perspective we present the main adaptation effects that are communicated to the user interface of adaptation and personalization systems. We also make a reference of selected state-of-the-art adaptation and personalization systems and frameworks starting with recent ones towards early pioneering ones. We conclude the chapter with a discussion on modeling human factors in interactive systems and personalization categories and adaptation technologies.

3.1 User Modeling for Personalization

An essential feature of an interactive system is its user model. The user model is a representation of static and dynamic information about an individual that is utilized throughout the whole interaction process aiming to trigger a number of adaptation and personalization effects (i.e., the same system can look different to users with different user models – Brusilovsky and Millán 2007; Frias-Martinez et al. 2005). For example, an information retrieval system may select and prioritize the most relevant items to the user's goals and/or interests. An educational hypermedia system may provide adaptive navigation support by manipulating the links based on the user's knowledge and learning goals. A privacy-preserving mechanism in a commercial Web-based system may adapt the content to the user's level of knowledge towards privacy terms (e.g., provide novice users with personalized privacy information awareness by using simplified terms and additional explanations).

Key technical issues in designing and developing adaptation and personalization systems include how to construct accurate and comprehensive models of each individual user and how these can be used to identify a user and describe the user's behavior in the system. With the advent of new and heterogeneous interaction device types and globalization of services, user modeling has become a challenging endeavor since today's interactive systems are accessed by different users, with different cognitive and cultural backgrounds, interaction device types and contexts of use. In this respect, researchers and practitioners alike have modelled various factors about the users and accordingly provide adaptive and personalized services. Example factors include among others: (i) The user's interest in a particular domain, e.g., E-Commerce systems infer the user's interest towards specific products based on their buying history (Goy et al. 2007); (ii) the user's level of knowledge on a particular learning domain, e.g., E-Learning hypermedia systems model the user's level of knowledge (novice or expert), and accordingly present personalized learning material and content (Brusilovsky and Millán 2007); (iii) the user's individual traits such as personality traits, cognitive processing styles and abilities and accordingly present personalized recommendations of music items (Ferwerda et al. 2015), personalized user authentication tasks (Belk et al. 2014a) or personal-

ized checkout processes in E-Commerce systems (Belk et al. 2015c); and (iv) the user's technology factors such as device type and screen size used and accordingly adapt the interaction and visual design of the system (Herder and van Dijk 2002).

A user model can include static information that rarely or never changes (e.g., demographic information), or dynamic information when it changes frequently over time. Such information is obtained either explicitly, using online Web forms, questionnaires and/or psychometric tests, or implicitly, by dynamically inferring characteristics about the users based on their navigation behavior in the system. For example, such implicit information can be extracted from the total time spent on a particular Web-page by a user, which can be in turn used to understand the interest of the user towards the main subject of that Web-page. Various research works have attempted to investigate the most effective source of information for user modeling (Gauch et al. 2007; Jawaheer et al. 2010; Wærn 2004). Based on Gauch et al. (2007) it is yet not clear-cut whether implicitly created models are more or less accurate than explicitly created models. Nevertheless, since implicit information gathering does not affect the human-computer interaction or the users' cognitive load (Gauch et al. 2007), it seems to be the preferable approach for collecting information about users. On the other hand, this approach is much more complex than explicit user feedback since in most cases the data obtained may be imprecise, incomplete and/or heterogeneous.

According to the nature of information that is being modeled, we distinguish models that represent information about the user and about the user's context of use. We next discuss in detail these categories.

3.1.1 User Information

Adaptation decision in adaptation and personalization systems was traditionally based on modeling information that reflects on various aspects about the user. We elaborate our analysis on the five most widely applied characteristics being modeled in such interactive systems: *knowledge*, *interests*, *goals*, *background*, and *individual traits* (Brusilovsky and Millán 2007).

Knowledge

Modeling user's knowledge is commonly found in educational hypermedia systems, indicating the level of expertise a user has on a specific subject being taught or the domain represented in a hypermedia system. Adaptation and personalization systems principally adapt content presentation and provide adaptive navigation support based on the user's knowledge model. For example in MetaDoc (Boyle and Encarnacion 1994), expert users are presented with low-level details of a concept and less additional explanations, while novice users are provided with additional support through explanations and less low-level details.

User's knowledge is a dynamic feature since it might change throughout the user's interactions with the system. In this context, an important challenge of adaptation and personalization systems that model the user's knowledge, have to update the user model depending on the changes of the user's knowledge. According to Brusilovsky and Millán (2007), the most common forms of user knowledge modeling are simple scalar models and more complex structural models. *Scalar models* are similar to stereotype models that represent the level of user's overall knowledge on a particular domain based on a quantitative value (e.g., value from 1 to 10) or a qualitative value (e.g., beginner-intermediate-expert). Scalar models are usually generated based on explicit user data collection methods such as self-assessment questionnaires. Although scalar models are easy to implement, they entail an important limitation since they average the user's level of knowledge on the domain, without comprehensively representing the user's level of knowledge on different parts of the domain.

Structural models aim to alleviate this issue by modeling the user's knowledge of different parts of the domain. A widely used structural model is the *overlay model* (Brusilovsky 2001; Hohl et al. 1996) in which each concept of the domain model stores a particular value representing the user's knowledge level on the particular concept (e.g., expert/ intermediate/ novice). Nevertheless, overlay models are hard to initialize since this requires an extensive interview with the user or a long questionnaire at the very beginning, in order to model all knowledge values of the domain model. Accordingly, several systems combine different solutions to alleviate such problems. For example, Hypadapter (Hohl et al. 1996) uses scalar models in the beginning to classify new users and set initial values, and then utilizes overlay models. Extensions of the overlay model include the *bug model* of Tsiriga and Virvou (2003) that represents misconceptions about a concept. For example, a bug model will include misconceptions of a user's problem solving knowledge which is based on incorrect user behavior (e.g., user typos, calculation errors).

Interests

Modeling user's interests has been commonly applied and researched in information retrieval and filtering systems, such as Web recommender systems. Main aim is to model a person's attention or curiosity towards particular domain concepts (e.g., product categories of an E-Commerce system), and accordingly filter and recommend items of that domain concept. Based on the literature, a user model of interests is also known as a user profile which can be a data instance of a user model but also the whole user model itself that is representing the user's interests or preferences in terms of keywords or concepts (Gauch et al. 2007). In addition, a user profile representing interests may include demographic information of the user, like name, age, gender, profession, etc., which is used by the system to refine the personalization process, for example, by presenting personalized male- or female-related products based on gender.

Information for building the user profile can be based on explicit user data collection methods (e.g., user's feedback through registration forms) or based on implicit user data collection methods utilizing the user's navigation behavior. User profiles can be static in which the information remains the same over time (e.g., gender) or dynamic in which the information is modified. Dynamic profiles are further categorized into short-term dynamic profiles that represent the user's current interests and long-term dynamic profiles that represent the user's interests that do not change frequently over time.

The most common approach for representation of user interests is the weighed vector of keywords (Gauch et al. 2007). In this approach, each keyword is associated with a numerical representation (weight), indicating the strength of the user's interest or preference towards that keyword. Each keyword may represent a particular domain concept. The keywords are either explicitly provided by the user (e.g., during registration), or extracted implicitly from Web-pages visited by the user during browsing, bookmarked or saved by the user. The most common technique for assigning weights of interests is based on the widely known *tf*idf* weighting scheme from information retrieval (Salton and McGill 1983). In this technique, each user profile is represented as a weighted vector of keywords, and the Web-pages that are retrieved by the system in response to a search are also converted to a weighted vector of keywords. Then, both vectors are compared using the *cosine* formula, and documents whose vectors are closer to the user's profile are then shown to the user.

A more powerful variation of the keyword-level approach is the concept-level approach for modeling the user's interests through a weighed overlay of a concept-level domain model (e.g., ontologies) (Kleanthous-Loizou et al. 2013). The concept-level approach for interest modeling is similar to the overlay modeling approach of user's knowledge. Concept-level models are more powerful and more accurate than keyword-level models since they can separately model different aspects of user interests given a standard definition of entities and their relationships.

The usage of keyword-level models or concept-level models highly depend on the nature of hypermedia content and has led to *closed corpus hypermedia systems* and *open corpus hypermedia systems*. In closed corpus hypermedia systems, such as adaptive museum guides, the content is indexed during system creation, whereas in open corpus hypermedia systems, such as adaptive news systems, new content must be indexed at the time of its insertion in the system (Ardissono et al. 2001). Due to this constraint, adaptive hypermedia systems usually use concept-level models since these have a closed corpus of documents and could be manually indexed during system creation, whereas information retrieval and filtering systems use keyword-level models due to their open corpus nature of content (i.e., new dynamic information is constantly added) requiring them to process documents automatically. Furthermore, research works exist that proposed hybrid solutions combining concept-level models with automatic document processing (Conlan et al. 2006) or combinations of concept-level and keyword-level models (Díaz and Gervás 2005).

Goals

Modeling a user's goal or task aims to elicit the user's objective and intention in the system. For example, a search goal in an information retrieval system (e.g., electronic encyclopedia, E-Commerce system), a learning goal/ objective in an educational system (e.g., E-Learning system) or a specific task in an application system (e.g., electronic performance support system). Modeling the user's goals is challenging since goals can be dynamic and change within a session of a specific task of the user. Furthermore, another challenging issue is the goal recognition phase. Principally, goal-based modeling systems recognize and mark the current running goal from a predefined list of goals. Different approaches exist for identifying the user's goal. The simplest approach is to let the user explicitly indicate the goal from a predefined list (Garlatti and Iksal 2000).

More sophisticated approaches implicitly infer the goal through user's interaction, for example, by tracking the time a user spends on a topic; the current goal is inferred through a weighted vector of goals (Kaplan et al. 1993). Furthermore, the ADAPTS support system (Brusilovsky and Cooper 2002) utilizes an alternative goal recognition process by determining the current task of the user within a task hierarchy, by following the user's aircraft maintenance operations. Furthermore, given that the goal recognition process may be not be that precise, research works have utilized probabilistic methods (Encarnação 1997; Micarelli and Sciarrone 1996) and data mining technologies (Hollink et al. 2005; Jin et al. 2005) to classify the user's current goal.

Recently, Barua et al. (2014) proposed a goal model that enables users to set, monitor and refine their models over the long term. Barua et al. have evaluated their work with a lab study and field trial providing evidence that the goal interface is usable and aids people in setting their long term goals. In another recent work, Baikadi et al. (2014) proposed an approach for goal recognition that leverages Markov Logic Networks. In particular, the approach utilized a machine learning framework that combined probabilistic inference with first-order logical reasoning aiming to encode relations between problem-solving goals and discovery events, domain-specific representations of user progress in narrative-centered learning environments.

Background

Modeling the user's background aims to represent the user's level of experience on a domain that might be related but is eventually outside the core domain of the system. For example, in a medical information system, the core domain is the hospital, the medical procedures, and terminology. Related but essentially outside the core domain could be the user's profession and experience of work. In this context, the medical information system can distinguish users by their profession (e.g., student, nurse, doctor) which implies the level of knowledge of that person (Brusilovsky and Millán 2007) and accordingly present personalized content to them (complex medical terminology to doctors whereas easier medical terminology to students).

Modeling user background is a subset of knowledge modeling since it is commonly utilized to infer knowledge. Nevertheless, the representation and handling of user's background is much simpler as it is a rather stable feature, provided explicitly to the system and represented as a simple stereotype model, rather than a complex overlay model.

Individual Traits

Modeling individual traits aims to elicit characteristics of users that define them as individuals. Popular examples are personality traits (e.g., introvert/ extravert), cognitive styles (e.g., imager/ verbal), cognitive processing abilities (e.g., working memory) and learning styles. Individual traits are stable user characteristics and are traditionally extracted using psychometric tests or questionnaires.

A considerable amount of research efforts have been undertaken focusing on modeling and utilizing cognitive factors for adaptation and personalization in interactive systems. Several approaches (Germanakos et al. 2008; Triantafillou et al. 2004; Graf et al. 2009; Papanikolaou et al. 2003) have distinguished users based on their cognitive styles and learning styles and provided different adaptation effects accordingly. In a study, Germanakos et al. (2008) have distinguished imager and verbal users, and wholist and analyst users based on Riding's Cognitive Style Analysis (Riding 1991). Each user was provided with adaptive presentation of content and different navigation organization. In a similar approach, Triantafillou et al. (2004) distinguished field dependent and field independent users based on Witkin et al. (1977) and provided different navigation organization, level of user control, and navigation support tools for these groups. Results in both studies indicate that cognitive styles have significant impact in the adaptation and personalization process of Web environments by increasing usability and user satisfaction during navigation and learning performance. On the contrary, various studies concluded that cognitive styles do not have a main effect on users' task performance and preference within hypermedia environments (Brown et al. 2006).

3.1.2 Context Information

Adapting to the user's context of use is commonly related to the user's location, interaction device, physical environment, social context, interaction history, etc. Two major context models that have been proposed in the literature are related to the user's platform and location characteristics which are further discussed in this section, as well as social characteristics that are popular in today's social networks.

Platform-oriented Context Modeling

Platform-oriented context modeling indicates information related to the user's computing environment, such as the device used, its hardware and software, and the available network bandwidth. These platform oriented settings might affect the effectiveness and efficiency of specific tasks as they can influence performance oriented attributes. As an example, low connection bandwidth can cause the replacement of a video based CAPTCHA challenge (Von Ahn et al. 2004) with a static CAPTCHA challenge. Also, if the user's platform cannot show colored pictures or bandwidth is low, the system can convert the pictures to black and white or low resolution (Rist 2001). In another approach a movie could be replaced with a picture in case the user's platform could not show movies due to the absence of a movie player or low bandwidth.

Platform-oriented context modeling is typically described by a set of name-value pairs (e.g., *<screen size, 1024x800>*), which is used in order to provide the most effective available solution according to the user platform oriented context.

Location-oriented Context Modeling

Location-oriented context modeling indicates information related to the user's current physical location. This kind of adaptation is popular in several social activities' contexts such as tourist and gastronomy guides (Cheverst et al. 2000; Panayiotou and Samaras 2004) that present or recommend to the users a subset of nearby objects of interest based on the user's location. In particular, Panayiotou and Samaras (2004) proposed a mobile-based adaptive interactive system that suggests restaurants or fast food stores based on the user's current location and time. For example, the system suggests restaurants that are close to the user's current location in the evening for dinner, or fast food stores in the afternoon. With regard to usable security, a recent study revealed that location information is an important issue which affects user's perception and effectiveness in security oriented tasks (Fidas et al. 2011). In particular, the results of this study suggest providing localized CAPTCHA challenges to the users' location and lingual characteristics aiming to increase usability in CAPTCHA interactions.

Social-oriented Context Modeling

Social-oriented context modeling represents the social activity (e.g., rating of products, participation at social events, etc.) of users. The majority of social context modeling systems recommend items (e.g., products, friends, events, etc.) to users according to the social context model of other users with similar characteristics (e.g., similar interests, same friends, same hobbies, etc.). With the current trend of organizing and sharing digital content through social networks, adaptation and personalization systems could utilize the social activity of users to construct their models based on

other users that have similar preferences and settings. A recent study in Kao-Li et al. (2011) proposed a social tag-based method (i.e., sharing of content through user-created metadata) to recognize how users like specific items and further utilize this information for the recommendation of multimedia items to users with similar preferences.

3.2 User Data Collection Methods

The aforementioned user characteristics are principally elicited through a user modeling mechanism utilizing explicit information from the user, i.e., user guided modeling, and/or implicit information, i.e., dynamic user modeling. These two categories are discussed next.

3.2.1 Explicit User Data Collection Methods

Explicit user information collection methodologies rely on personal information provided by the users, typically via registration forms. The data collected usually contain demographic information (i.e., age, gender, and profession), interests and/or preferences. Common techniques for obtaining explicit information that allows specification of the user model include the use of checkboxes, drop-down lists, or text fields where users express freely their opinion. All these techniques have the advantage that the format of the replies are standardized but the main drawback is that the user is aware that the system is storing this information and usually the process may be disrupted due to unwillingness of the user to provide the information, lack of trust or time to participate in the process. Also, the results from these techniques are human-error prone since if the questions are not carefully designed then they might be inaccurate, inconclusive, or at worst, deceptive.

Explicit user data collection approaches are commonly utilized for customizing user interfaces. In this case, a collection of user preferences are used to create a user model and the services provided adapt in order to increase information accessibility. For instance, Google explicitly asks users to provide their personal information which is stored to create user models. The Web-site content is then dynamically organized based on the users' preferences.

An important drawback of customization approaches is that users may not accurately or fully report their preferences and characteristics. Furthermore, most interactive systems utilizing such approaches barely invoke the user to update the information and rarely have intelligent mechanisms behind to identify that something has changed in the users' preferences. Thus, this results to static user models even though the user's interests may change over time. As a consequence, the user model may become highly inaccurate over time.

3.2.2 Implicit User Data Collection Methods

User models could be also dynamically generated based on implicit information, such as the navigation behavior of users. These mechanisms are transparent to the user and do not add disruption or require any additional effort by the user during the process of interacting with the system for constructing the models. Kelly and Teevan (2003) provide an overview of the most popular mechanisms for dynamically collecting implicit user information. Gauch et al. (2007) also summarizes different approaches to implicit user information collection.

The most common source of information about users is their browsing history from which the users' interests are extracted. Browsing history of users contains URLs visited by the user and the date/ time of the visits. Accordingly, meaningful information could be extracted based on this information, e.g., number of visits to a particular URL and the time spent in that Web-page. Browsing histories could be collected in two ways: Users sharing their browsing caches on a periodic basis (Gauch et al. 2007), or users installing a proxy server that acts as their gateway to the Internet, thereby capturing all Web traffic generated by the user (Trajkova and Gauch 2004). The first technique utilizes the Web browser's cache system that stores the user's Web browsing history. This technique does not require any installation of specific software. However, in order to extract meaningful information from the collected data, the user is required to upload the cache periodically. In the second technique, proxy servers allow easily capturing information without placing any major burden on the user because they only require an initial setup and do not require any software to be maintained or updated afterwards on the user's desktop computer. An important drawback however is that no user model can be created without having a specific proxy enabled by the user.

Another approach to collect implicitly information while the user navigates in an interactive system is through the usage of agents (e.g., Web browser plugins). Browser agents can be installed on the user's desktop computer and are able to capture all of the activities the user performs while browsing. Apart from collecting the user's browsing history (i.e., URLs visited), browser agents accurately collect information about the actions performed on a Web-page, such as bookmarking and downloading to disk. Accordingly, based on this additional information about the user's browsing activity, agents may suggest links on the current page that might be of interest. An important drawback of this approach is that it requires specialized software to be installed.

Enhancements of Web browser agents are desktop agents which are commercial toolbars that include personalized features with the aim to help users organize their browsing activity stored in their desktop caches. Furthermore, navigation activity for desktop agents is not limited to the Web, but also includes access of users on their local computer, e.g., personal folders and documents. Such search tools are implemented in applications like Stuff I've Seen (Dumais et al. 2003).

3.3 User Model Generation

The simplest approach of user model generation is in the case where the information collected by the user is used as-is and remains unprocessed. For example, users might explicitly express their interest on specific topics of a news publishing system which will be further used by simple rule-based mechanisms to adapt the interface by displaying the selected topics on the top of the users' interface. More intelligent approaches for generating user models include cases where the browsing activities of users may be utilized by *data mining* techniques to recognize regularities in user paths and integrate them in a user model.

Data mining is the process of discovering patterns in large data sets. Main aim is to extract information from raw data and transform it into understandable data for further use (Chakrabarti et al. 2006). A thorough literature review on how data mining techniques can be applied to user modeling in the context of adaptation and personalization systems may be found in the works of Eirinaki and Vazirgiannis (2003), Pierrakos et al. (2003) and Mobasher (2007). In this context, the most widely applied and researched approaches for data mining are *clustering*, *classification*, *association discovery* and *sequential pattern mining*. We next provide an overview of each approach.

3.3.1 Clustering

Clustering is an unsupervised process that groups users together sharing common characteristics or similar navigation behavior (Nasraoui et al. 2008; Castellano and Torsello 2008; Castellano et al. 2008). Nasraoui et al. (2008) perform clustering on user sessions to place users in homogeneous groups based on the similar activities performed and then extract specific user models from each cluster. Clustering techniques are also used in order to divide users into segments containing users with similar navigation behavior. Using a similarity metric, a clustering algorithm groups the most similar users together to form clusters. Because optimal clustering over large data sets is impractical, most applications use various forms of greedy cluster generation. These algorithms typically start with an initial set of segments, which often contain one randomly selected user. Then, they repeatedly match users to the existing segments. Once the algorithm generates the segments, it computes the users' similarity to vectors that summarize each segment, chooses the segment with the strongest similarity and classifies the user accordingly. Some algorithms classify users into multiple segments and describe the strength of each relationship (Perkowitz and Etzioni 2000). The same concept is found within fuzzy clustering techniques, examples of which include the work of Castellano and Torsello (2008) that categorized users based on the evaluation of similarity between fuzzy sets using a relational fuzzy clustering algorithm and Castellano et al. (2007) that derived user models by analyzing user interests. Variations of fuzzy clustering methods include Fuzzy c-medoids, Fuzzy c-trimmed-medoids, relational Fuzzy Clustering-Maximal Density estimator

(RFC-MDE) algorithm, hierarchical clustering approaches, which are applied to group user sessions (Fu et al. 1999).

3.3.2 Classification

Classification is a supervised learning process that maps user information (e.g., interaction data) into one of several predetermined classes which usually represent different user models (Wu et al. 2007). Main aim is to understand existing data and predict how new instances might behave. In the context of adaptation and personalization, classification can model the behavior of users based on predefined classes of users. The most common classification methods are *decision tree induction*, *Bayesian classifiers* and *artificial neural networks* (Pierrakos et al. 2003).

Decision tree induction is one of the most popular classification methods (Choa et al. 2002). This method builds a decision tree and then utilizes it to perform classification. A decision tree is a structure that entails a root node which is the topmost node, branches and leaf nodes. Internal non-leaf nodes denote a test on an attribute, each branch denotes the outcome of a test, and each leaf node denotes a class prediction. In the context of adaptation and personalization, decision tree induction has been widely applied in recommender systems (Nikovski and Kulev 2006; Choa et al. 2002).

Bayesian classification is a probabilistic classifier based on applying the Bayes' theorem which enables prediction of future events and provides an embedded scheme for learning (Rett et al. 2008). The Bayesian interpretation of probability can be seen as an extension of logic that enables reasoning with propositions whose truth or falsity is uncertain. To evaluate the probability of a hypothesis, the Bayesian probability specifies some prior probability, which is then updated in the light of new, relevant data. Bayes' formula provides a means to make inferences about an environment of interest described by a state, given an observation. Several research works have utilized Bayesian theory in the context of recommender systems such as early works of Miyahara and Pazzani (2000) that aimed to improve collaborative filtering in recommender systems with simple Bayesian classification and more recent works of Wang and Tan (2011) that similarly aimed to improve collaborative filtering based on a naïve Bayesian method.

Artificial Neural Networks (ANNs) are also used as a powerful technique to dynamically and transparently model human behavior in adaptation and personalization systems. Numerous researchers have attempted to use ANNs in the context of adaptation and personalization systems, primarily for classification of users with the same characteristics and creation of user models with the aim to recommend and adapt content and functionality (Frias-Martinez et al. 2005). For example, Kim et al. (2004) have proposed an ANN-based collaborative filtering method that investigates the possibility of identifying and predicting the correlation between users or items in a Web environment using a Multi-Layer Perceptron (MLP). Chou et al. (2010) aim to identify the users' prior knowledge for specific products in E-Commerce applications by analyzing their navigation patterns

through Web mining and constructing a Back-Propagation Network (BPN – Wu et al. 2006) that uses a supervised learning method and a feed-forward architecture, in order to predict the users' potential future needs. Magoulas et al. (2001) use ANNs to learn and fine tune rules and/or membership functions from input-output data to be used in a Fuzzy Inference System (FIS). In particular, they have proposed a classification/ recommendation system with the aim to plan the learning content of a course according to the student's level of knowledge.

3.3.3 Association Discovery

Association discovery techniques aim at generating associations and correlations among sets of items (Linden et al. 2003; Su and Khoshgoftaar 2009). Association rules are commonly used in E-Commerce systems to relate different products based on the users' viewing history, e.g., when users view product A and afterwards view product B, then an association rule is created between product A and B indicating a high relationship between the two products (Pierrakos et al. 2003). Accordingly, this information is further utilized by the system to offer recommendations based on the navigation behavior of users.

Early works on adaptation and personalization (Mobasher et al. 1999) proposed association discovery techniques utilizing item sets with the aim to dynamically recommend Web-pages to users. Alternative approaches for discovering associations between items utilize Bayesian networks for defining structured relations between the topics of a Web-site (Schwarzkopf 2001; Ardissono and Torasso 2000).

Association discovery mining techniques have been primarily applied for the prediction and recommendation of the next interesting Web-page and have not been extensively applied in other contexts. According to Pierrakos et al. (2003) the main reason that association discovery mining has not been widely studied in this context is because the prediction of the next best Web-page is best modeled as a sequential prediction task in which association discovery techniques are not appropriate.

3.3.4 Sequential Pattern Mining

Sequential pattern mining aims at finding relevant patterns between data items that are delivered in a sequence (Mabroukeh and Ezeife 2010). Thus, sequential pattern discovery considers time in the discovery process with the aim to identify patterns that frequently occur. In the context of Web usage mining, this approach can be used to identify the navigational patterns of users. Sequential pattern mining can be categorized in two widely researched methods: *deterministic methods* that focus on tracking the navigational behavior of users (Spiliopoulou et al. 1999; Paliouras et al. 2000), and *stochastic methods* that represent the users' transitions of Web-pages within a Web-site

aiming to predict next visits. A widely used stochastic method is the Markov model to represent the transitions of users in Web-sites (Parka et al. 2008; Cadez et al. 2000; Yang et al. 2003) and they are utilized to indicate the next page users might request to visit based on their current location and previous navigation paths. Thus, in the context of a Web-based application, representation schemes, like the ones in Markov chains can be utilized to represent the transition of users between Web-pages, using for example sequence vectors, and thus identify groups of users following same or similar paths.

3.4 Personalization Categories

Personalization can be split in six categories: *Link personalization*, *content personalization*, *personalized search*, *context personalization*, *authorized personalization* and *humanized personalization* and are discussed in detail in the following sub-sections.

3.4.1 Link Personalization

Link personalization involves the adaptation and personalization of the structure and presentation of hyperlinks in an interactive system. This is achieved by selecting the links that are more relevant to the user (e.g., based on interests, preferences), changing the original navigation space by reducing or improving the relationships between nodes, and adapting the presentation of links. Link personalization is used in E-Commerce applications for recommending relevant products to the users based on their buying history and their ratings on specific products or category of products (Rossi et al. 2001). A popular example of applying link personalization in real-life E-Commerce systems is in Amazon (2015) that recommend products to users with relevant to purchased items, new releases, shopping groups, etc. (Rossi et al. 2001; Linden et al. 2003). Link personalization is also widely applied in educational hypermedia systems for adapting the link structure and navigation of particular learning material and concepts (Germanakos et al. 2007). For example, based on the knowledge model of a user (that represents the knowledge level of the user on particular concepts of a domain), the system may prioritize links pointing to information with easier difficulty level first, in case the student has novice levels of knowledge on the particular concepts, or present links pointing to information with higher difficulty level first in case the student has expert levels of knowledge. Another example may be based on cognitive styles (Wholist/ Analyst) for presenting different navigation patterns depending on the student's preferred way of organizing and processing visual information (Germanakos et al. 2007).

3.4.2 Content Personalization

Content personalization involves adapting and personalizing the content of the user interface. Content personalization can be classified in two categories:

(1) Node structure personalization entails filtering the content that is relevant to the users, illustrating sections and information in which the users may be interested. They may explicitly indicate their preferences, or these may be inferred through their static user model or navigation activity. For example, in Apple (2015), users may reorganize and choose a set of "widgets" to be displayed in the initial screen of their mobile device, and further personalize the content to be displayed based on a specific set of attributes. Automatic personalization may also occur, e.g., a sports news application may present localized information to the users based on their GPS location information.

(2) Node content personalization is finer grained than structure personalization and involves adapting the information of the same node to various users. An example can be based on E-Commerce systems that provide users with different discounts by personalizing the price of the same product according to the users' buying history (Rossi et al. 2001).

3.4.3 Personalized Web Search

Personalized Web search (Wen et al. 2009) is the process of tailoring and personalizing the search results to an individual's interests by taking into consideration information about the individual beyond the query provided. Personalized Web search is implemented on the server side as part of a search engine's methods or on the client side on the user's computer (e.g., as a plugin on the Web browser). According to Pitkow et al. (2002), there are two general approaches to personalize the Web search results: (i) By modifying the user's query; and (ii) by re-ranking search results.

In order to provide personalized search results to users, the system models the users' characteristics, interests and preferences on specific concept categories. Specifically, information maintained in the user model may include: (i) Demographic information such as age, gender, language, education; (ii) geolocation information such as country, address; (iii) interests and preferences; (iv) search history such as prior queries submitted by the user, visited links, downloaded files; (v) browsing behavior such as mouse clicks, mouse movements, scrolling and bookmarking; and (vi) user actions such as bookmarking a Web-page, setting Web-sites as favorites.

According to Wen et al. (2009), modeling users' information for personalized Web search can be achieved through the following techniques: (i) Personalized search based on content analysis in which the system compares and checks the content similarity between Web-pages and user models; (ii) personalized search based on hyperlink analysis in which the system computes the personalized importance of Web documents for each user; and (iii) personalized search based on collaborative approaches in which the system presents similar search results to users with similar user models.

3.4.4 Context Personalization

Context personalization refers to the adaptation of information that is accessed in different contexts of use (Rossi et al. 2001). Context personalization can be based on the user's location, interaction device, physical environment or social context. For example, a text-recognition CAPTCHA mechanism may localize the text-based challenge by presenting characters personalized to the users' localized information (Fidas et al. 2011).

A high number of research works have focused on personalizing content and functionality of interactive systems based on the user's location. Location-based personalization systems recommend new locations of interest to the users by taking into account their interests and preferences, utilizing content-based or collaborative recommendation techniques (Herder et al. 2014). Herder et al. (2014) has identified four streamlines of research focusing on location-based services: *Human mobility patterns* focusing on people's movements, number of visits, etc.; *predicting next locations* that utilize data mining techniques such as Markov Models and Bayesian Models for predicting the user's next location; *location and social media* aiming to analyze human mobility based on social media data analysis, although research in this area is sparse due to the fact that users rarely share their exact location in the data they share; and *location-based services* that primarily provide location-based recommendations and contextualized search results (Bellotti et al. 2008). Another example is adapting information according to the characteristics of the interaction device and the context of use (Lankhorst et al. 2002). Context personalization can also occur on a combination of contextual parameters such as recommending near-by restaurants to users based on their location and time (e.g., lunch, dinner – Panayiotou and Samaras 2004; Teevan et al. 2011).

3.4.5 Authorized Personalization

Authorized personalization is applied when an interactive system provides different access of information and action permission to users with different roles in the system. The most widely known approach of authorized personalization is role-based access control in which access rights in particular sections of a system are categorized under a role name. In this approach, a many-to-many relationship exists between users-roles-permission in which each user belongs to particular roles, and each role relates to particular permissions. Depending on the status and responsibilities of a user within an interactive system, different roles and thus permissions are given to that user. For example, in a conference paper management system, such as Precision Conference (2015), users have different access rights and action permission depending on their role (authors, reviewers, organizers). In this context, depending on their role in the system, authors may only be able to submit and upload their own paper, whereas the primary reviewer may be able to view and manage multiple papers submitted by the authors.

Role-based access control is highly scalable and hierarchies of roles enable the easy assignment of permissions including the permissions that are associated with one role to another role. An early role-based approach is Role-based Access Control (RBAC – Sandhu 1998) which enhances traditional mandatory and discretionary models for restricting system access to authorized users. Team-based Access Control (TMAC – Thomas 1997) is an access control model that focuses on collaborative team work and incorporates context information (i.e., the members of a team and the object instances) that is associated with collaborative tasks and accordingly applies this context information for access control. Various research works exist that extended the TMAC model with additional factors aiming to model more access policies (Georgiadis et al. 2001; Alotaiby and Chen 2004). For example, in the work of Georgiadis et al. (2001) the TMAC model is enhanced with additional information such as time of access, the location from which access is requested, the location where the object to be accessed resides, transaction-specific values that dictate special access policies, etc.

3.4.6 Humanized Personalization

Humanized personalization aims at creating personalized user interfaces based on intrinsic human factors such emotional factors (anxiety, stress), personality traits, cognitive styles, learning styles, visual attention, elementary cognitive processing abilities, etc. Given the highly complex and multi-dimensional character of these factors, personalizing content and functionality of interactive systems based on such human factors is still at its infancy and not yet widely applied in commercial interactive systems. Furthermore, a practical limitation applying to these factors is related to the fact that the elicitation and user modeling process requires explicit user data collection methods in which users perform a series of psychometric tests, respond to specially designed questionnaires or participate in controlled laboratory studies utilizing external hardware devices such as eye tracking devices for measuring the visual attention and visual search of users, and physiological sensors for measuring blood pressure, heart rate, skin conductance aiming to model the user's anxiety, stress, etc.

Nevertheless, driven by existing research works in psychology suggesting that individuals differ in such human factors, as well as empirical findings that indicate the impact of personalizing content and functionality of interactive systems based on such intrinsic human factors, it is important to further investigate the effects and impact of applying these in adaptation and personalization systems to the benefit of the user. In particular, a high number of research works revealed significant effects of applying several human factors in adaptation and personalization systems in various application domains. For example, Tsianos et al. (2010) conducted a user study aiming to examine learners' emotional arousal variability, and possible correlations of the physiological data with other psychological constructs such as trait and self-reported anxiety. According to the findings, heart rate was significantly correlated with trait and self-reported state anxiety, but not with academic

performance in an on-line exam. Skin conductance and blood volume pulse had only marginal variations, perhaps due to the absence of intense stimuli. In a recent work of Steichen et al. (2014), a user study that investigated the effect of elementary human cognitive processes and eye gaze patterns on visual search tasks in information visualization, identified a number of pattern differences that could be leveraged by adaptation and personalization systems aiming to implicitly elicit and consequently adapt to different user characteristics. In the same line, the work of Belk et al. (2014a) revealed that human cognitive differences (i.e., cognitive styles and abilities) could be leveraged for adapting and personalizing security-related tasks such as user authentication mechanisms for improving the task completion performance and effectiveness of such tasks.

3.5 Adaptation Technologies

Adaptation and personalization systems apply specific algorithms that decide what kind of adaptation will be applied to with respect to their content and functionality. Various adaptation technologies have been proposed in the literature during the years. Among those, the most widely applied and researched include *user customization*, *rule-based filtering*, *content-based filtering*, *collaborative filtering*, *Web mining*, *demographic-based filtering* and *agent technologies*.

3.5.1 User Customization

User customization provides a mechanism that allows users to construct a custom interface representation based on their own preferences. Once the user has entered this information, a matching process is used to find items that meet the specified criteria and display them to the user. The system in this case is not considered adaptive, but rather adaptable because it is explicitly configured by the user how to adapt its content and functionality. Most of today's major service providers provide several user customization mechanisms as part of their services such as Google's (2015b) Gmail that enables users to set the desired display density of the users' emails (i.e., "comfortable" and "cosy" view for larger displays, and "compact" view for smaller displays). Gmail also provides a mechanism for configuring and rearranging email categories (through drag-and-drop functionality of visual tabs) as well as choose a predefined visual theme from which the user can select from and apply different backgrounds on the user interface of his emails. In the same line, other email providers such as Microsoft's (2015) Outlook provide various user customization mechanisms for adapting the display of the online email management system.

3.5.2 Rule-based Filtering

Rule-based mechanisms refer to the process of producing high-level information from a set of low-level metrics, related to both static and dynamic user context information. Bearing in mind that the dynamic part of the context data model can be updated in real time it becomes obvious that the reasoning capabilities supported provide an added value assisting users in different tasks. Such rules can initiate automated system actions or compare predictive user interaction models with actual user interaction data gathered in real time, providing thus valuable insights related to the current user goals and efficiency of interactions. For example, an online banking system may contain a rule "([USER].*logged=false* and [USER].*loginattempts.count>2*) then [UIOBJECT.*livesupport.show=true*]", which indicates that the system should automatically offer a live customer support option to users who could not succeed to login in the system for several times. Based on another usage scenario such a rule-based mechanism could extremely increase usable security by offering a live customer support option to users whose E-Banking Web accounts are locked due to numerous unsuccessfully login attempts. A detailed analysis and comparison of rule-based mechanisms can be found in (Smyth 2007).

3.5.3 Content-based Filtering

Content-based filtering suggests labeling of links by analyzing the content of pages. A typical content-based filtering mechanism includes the following steps: (i) Pre-fetch the content behind the links of the current page; (ii) parse the pre-fetched pages to create a weighted keyword vector of each page; (iii) compare the weighted keyword vector of each page with the user's preferences, that are also usually represented using a weighted keyword vector; and (iv) suggest pages whose keyword vectors are the same with the user's preferences.

This technique is primarily characterized by two weaknesses, content limitations and over-specialization. There are content limitations like information retrieval methods that can only be applied to a few kinds of content, such as text and images, and the extent aspects can only capture certain aspects of the content. On the other hand content-based recommendation systems provide recommendations merely based on user models, therefore, users have no chance of exploring new items that are not similar to those items included in their models and thus leading to over-specialization. A detailed analysis and comparison of content-based filtering mechanisms can be found in (Pazzani and Billsus 2007).

3.5.4 Collaborative Filtering

Collaborative filtering (Schafer et al. 2007) exploits the social process of people to recommend something they have experienced (e.g., read a book, watched a movie, etc.) to other people. Collaborative filtering mechanisms are based on the assumption that if users *X* and *Y* rate *n* items similarly, or have similar behaviors (e.g., buying, watching), hence will have similar interests. Adaptation and personalization systems utilize collaborative filtering mechanisms to provide navigation support by recommending links of interest to the user based on earlier expressed ratings or navigation behavior of similar users.

There are two general classes of collaborative filtering algorithms, *memory-based methods* and *model-based methods* (Eirinaki and Vazirgiannis 2003). Moreover, the goals in a collaborative filtering system are basically focused upon the reduction of computation time, the increase of the extent in which predictions can be computed in parallel, and the increase of prediction accuracy. Collaborative filtering can further refine the process of giving each individual personal recommendations compared to rule-based filtering. It overcomes the drawbacks of the content-based filtering because it typically does not use the actual content of the items for recommendation. It usually works based on assumptions. With this algorithm, the similarity between the users is evaluated based on their ratings of products, and the recommendation is generated considering the items visited by the nearest neighbors of the user. In its original form, the nearest-neighbor algorithm uses a two-dimensional user-item matrix to represent the user models. Some highlighted drawbacks of collaborative filtering include the following: (i) Collaborative filtering mechanisms are often based on matching in real-time the current user's model against similar records obtained by the system over time from other users. However, it becomes hard to scale collaborative filtering techniques to a large number of items, while maintaining reasonable prediction performance and accuracy. Part of this is due to the increasing scarcity in the data as the number of items increase. One potential solution to this problem is to first cluster user records with similar characteristics, and focus the search for nearest neighbors only in the matching clusters. In the context of adaptation and personalization this task involves clustering user transactions identified in the pre-processing stage; (ii) traditional collaborative filtering does little or no offline computation, and its online computation scales with the number of customers and catalogue items. The algorithm is impractical on large data sets, unless it uses dimensionality reduction, sampling, or partitioning, all of which reduce recommendation quality; (iii) user input may be subjective and prone to bias; (iv) explicit user ratings may not be available; (v) models may be static and can become outdated quickly; (vi) collaborative filtering mechanisms are not able to recommend new items that have not already been rated by other users. An object will become available for recommendation only when many users have seen it and rated it, making it part of their user models first; and (vii) collaborative filtering mechanisms are not satisfactory when dealing with a user that is not similar enough with any of the existing users.

3.5.5 Web Mining

Web mining includes data mining techniques with the aim to identify patterns from Web systems. It is divided in three main categories: (i) *Web content mining* which aims at the extraction and integration of data and knowledge from Web-page content; (ii) *Web-structure mining* which aims at the analysis of node and connection structure of a Web-site; and (iii) *Web usage mining* which aims at extracting useful information from server logs about the interaction activity of users, e.g., discover what users are looking for in a Web-page. Web usage mining is primarily related to adaptation and personalization. This process applies statistical and data mining techniques on server log data, resulting in a set of useful patterns that indicate users' navigational behavior. The data mining methods that are employed are: Association rule mining, sequential pattern discovery, clustering, and classification. Given the site map structure and usage logs of a Web-site, a Web usage miner provides results regarding usage patterns, user behavior, session and user clusters, click stream information, etc. Alternative works have also focused on analyzing usage data beyond the scope of a single Web-site, through the analysis of usage data collected by the proxy servers of an Internet Service Provider (Pierrakos et al. 2004). Furthermore, additional information about the individual users can be obtained by the user profiles (Deshpande and Karypis 2004; Eirinaki and Vazirgiannis 2003; Cingil et al. 2000). The overall process can be divided in two steps: (i) The pre-processing and data preparation step, including data cleaning, filtering, and transaction identification, resulting in a user transaction file; and (ii) the data mining step in which usage patterns are discovered via specific usage mining techniques such as association rule mining, association-rule discovery and usage clustering (Mobasher et al. 2000).

One of the main advantages of Web usage mining are summarized as follows: (i) The models are dynamically obtained from user patterns, and thus the system performance does not degrade over time as the models age; (ii) using content similarly alone as a way to obtain aggregated models may result in missing important relationships among Web objects based on their usage. Thus, Web usage mining will reduce the need for obtaining subjective user ratings or registration-based personal preferences; (iii) models are based on objective information (how users actually use the Web-site); (iv) there is no explicit user rating or interaction with users (saves time and other complications); (v) it supports preservation of user privacy, by making effective use of anonymous data; (vi) the usage data captures relationships missed by content-based approaches; and (vii) it can enhance the effectiveness of collaborative or content-based filtering techniques. Nevertheless, usage-based personalization can be problematic when little usage data is available pertaining to some objects or when the content attributes of a Web-site must be integrated into a Web mining framework and used by the recommendation engine in a uniform manner (Mobasher et al. 2002).

3.5.6 Demographic-based Filtering

Demographic-based filtering complements other adaptation technologies such as rule-based and collaborative filtering, aiming to refine the personalization result. In particular, demographic information of users (e.g., age, gender, profession, etc.) can be utilized to infer users' interests and accordingly recommend particular objects. This method uses demographic information to identify the types of users that prefer a certain object and to identify one of the several pre-existing clusters to which a user belongs aiming to tailor recommendations based on information about others in this cluster (Pazzani 1999; Basilico and Hofmann 2004).

Early examples of demographic-based filtering approaches include LifeStyle Finder (Krulwich 1997) that aimed to generate user models based on a large-scale database of demographic data. Nevertheless, one of the challenges of demographic-based filtering approaches is that obtaining demographic information can be difficult, and when obtained, the information is usually of poor quality (Mobasher 2007). In LifeStyle Finder, the system provides a dialog to the user to help categorize the user. In an early work of Pazzani (1999), an alternative approach was proposed for obtaining demographic information by leveraging the work users already expended in creating a homepage on their Web browser. Main aim of the approach was to minimize the effort required to obtain demographic-based information.

3.5.7 Agent Technology

Agents are processes that aim at performing tasks for their users, usually with autonomy, playing the role of personal assistants (Delicato et al. 2001; Panayiotou and Samaras 2004). Agents usually solve common problems that users are experiencing on the World Wide Web such as personal history, shortcuts and Web-page watching. Some of the agents' main characteristics could be distinguished according to their abilities used and according to the tasks they execute. The former include characteristics such as intelligence, autonomy, social capacity (inter-agent communication), and mobility, while the latter classify the agents into information filtering agents, information retrieval agents, recommendation agents, agents for electronic market, and agents for network management (Delicato et al. 2001). Pioneer personalization systems implemented with agents are: ARCHIMIDES, Proteus, WBI, BASAR, 1:1 Pro, Haystack, eRACE, mPersona, Fenix system, and SmartClient (Pu and Faltings 2002; Panayiotou and Samaras 2004; Delicato et al. 2001).

3.6 Adaptation Effects in User Interfaces

User-centered design approaches are essential in designing complex interactive systems which iteratively involve the user in the whole design and development process. In this respect, aiming to

achieve a common understanding between users and interaction designers, a necessary step involves the formalization of the information architecture and the specification of the interaction flow of specific tasks. This requires modeling and analysis of the user actions at an abstract level and identifying the most appropriate content, visual presentation and interaction flow, as depicted in Figure 5.

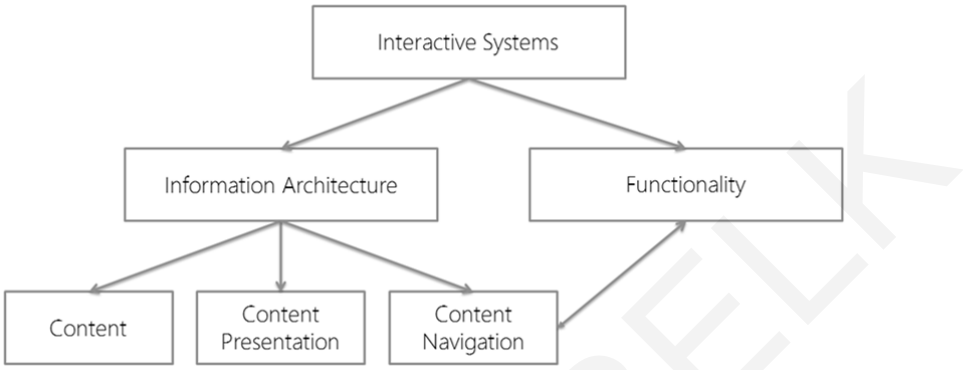


Figure 5. High-level architecture of interactive systems

A key challenge in adaptation and personalization systems is which visible features of the system can be adapted by a particular technique. Based on (Brusilovsky 2001; Brusilovsky 1996), there is a number of ways to adapt hypermedia. These are classified under two main classes of adaptation technologies; content-level adaptation, called *adaptive content presentation* and link-level adaptation, called *adaptive navigation support*. Adaptive presentation relates to the adaptation of hypermedia elements inside nodes, and adaptive navigation support relates to the adaptation of links inside nodes, indexes and maps. These are discussed below.

3.6.1 Adaptive Content Presentation

Adaptive content presentation relates to the adaptation of hypermedia elements inside nodes. The idea behind adaptive content presentation is to adapt the information elements (or content) inside a node accessed by a particular user to the needs and preferences of that user. Adapting the presentation of content within a node is most often performed as a manipulation of fragments. Such manipulations aim to provide prerequisite, additional or comparative explanations. For example, additional information can be shown for users with a specific state of knowledge to provide missing prerequisite knowledge, additional details, or a comparison with a previously known concept. Techniques that are used to provide adaptive presentation include: (i) Inserting/ removing relevant to the user fragments; (ii) expanding/ collapsing content fragments (e.g., expand additional explanations to novice users); (iii) altering content fragments (e.g., present a diagrammatical representation of a concept to an Imager cognitive style user (Germanakos et al. 2009)); and (iv) sorting content fragments (e.g., some users may prefer to see an example before a definition, while others prefer it the other way around).

In the work of Germanakos et al. (2009), users with different cognitive typologies (i.e., Verbal, Imager, Intermediate) were provided with different content fragment variations, i.e., users belonging to the Verbal class (that process textual content more efficiently) were presented with more textual content, whereas users belonging to the Imager class (that process graphical content more efficiently) were presented with more graphical content. Furthermore, this study provided adaptive navigation support (described next) based on other cognitive factors (i.e., Wholist-Analyst) that affect navigation behavior of users in interactive systems.

3.6.2 Adaptive Navigation Support

Adaptive navigation support relates to the adaptation of links inside nodes. This kind of adaptation supports user navigation in an interactive system, by adapting to the goals, preferences and knowledge of the individual user. The core idea behind this kind of adaptation is to adapt the presentation of hyperlinks/ functionality within a node. Adaptive navigation support can be achieved by: (i) Guiding the user in the system by suggesting a node to visit according to the user's goals, preferences and knowledge. Direct guidance is popular in adaptive educational hypermedia systems where students get suggested nodes based on their level of knowledge on the specific subject (e.g., ELM-ART – Weber and Brusilovsky 2001); (ii) prioritizing links that are relevant to the user. Link ordering is primarily applied in interactive systems that contain non-contextual hyperlinks such as, adaptive news systems and commercial Web shops. For example, adaptive news systems typically recommend a prioritized list of news articles based on the modeled user's interests and preferences. Similarly, E-Commerce systems recommend a prioritized list of products based on the modeled user's interests and product ratings. Link ordering is typically performed by content-based filtering mechanisms; (iii) hiding, removing or disabling links to restrict navigation space to irrelevant nodes. Link hiding has been very popular in the area of adaptive educational hypermedia systems that aim to protect the users from the complexity of the whole hyperspace and reduce their cognitive overload by hiding irrelevant to them nodes. For example, if the user has novice level of knowledge on a particular concept, the system restricts the user from navigating to it; (iv) augmenting links with additional information about the node behind the link, with some form of annotation. Link annotations are provided with different visual signs, for example different icons, different color and intensity of anchors, or different font sizes. Furthermore, Web technologies such as HTML5 and CSS3 enable adaptive Web systems to annotate hyperlinks with verbal annotations on hyperlink mouse-overs, for example display information on the Web browser's status bar or as a "tooltip" over the hyperlink when the user moves the mouse pointer over the hyperlink; and (v) dynamically generating new, non-authored links based on the user's interests and/or current context (i.e., location) in the system. Link generation is popular in the field of adaptive navigation support systems and Web recommender systems for the dynamic generation of links that are useful within the current context of the user. Web recommender systems attempt to recommend a prioritized list

of relevant to the user items, typically based on the user's interests. In this respect, Web recommender systems focus in the underlying technology. On the other hand, adaptive navigation support systems focus on helping users to find their way through hyperspace by adapting links on a page. Link adaptation in adaptive navigation support systems take into account various features of the user, including user's interests, goals, knowledge, and current context (i.e., location in hyperspace). In all cases, navigation support techniques provide guidance that takes into account the user's current location in hyperspace (Brusilovsky 2007). Thus, adaptive navigation support systems focus on the interface.

Accordingly, although the difference between adaptive navigation support systems and Web recommender systems is not clear, an important difference between these two groups is that adaptive navigation support systems primarily focus on the user's current location in hyperspace and aim to guide the user by introducing additional hyperlinks that may be useful in the current context, while Web recommender systems primarily focus to recommend hyperlinks that are related with the user's short- and long-term interests.

3.7 Web Adaptation and Personalization Systems and Frameworks

Given the multidimensional character of user modeling, adaptation and personalization, building a complete adaptive interactive system that will follow an end-to-end process is a challenging endeavor. Thus, the literature reveals a high number of research works that focus and investigate targeted challenges and issues rather than complete personalization systems. For example, incorporating human factors in the design of personalized user authentication mechanisms requires first to investigate whether and which ones affect user interactions in authentication-related tasks. Then, once identified, the observable main effects can be further used to develop adaptation rules and alternatives for personalizing user authentication tasks. Apparently, such an approach requires extensive research efforts by first understanding the users and their behavior in a specific context of use, and accordingly further developing and iteratively evaluating and refining a solution. In this context, we list below a representative number of Web adaptation and personalization systems and frameworks that have been designed and developed during the last twenty years.

1. PersonaWeb (Germanakos et al. 2015) is an extended and technically enhanced version of Smartag (described next – Belk et al. 2012b) that focuses on adapting and personalizing content and functionality of E-Commerce environments based on human cognitive factors.
2. Hybreed (Hussein et al. 2014) is a software framework for developing complex and hybrid, context-aware recommender systems.
3. Adaptive Notifications in Virtual Communities (Kleanthous-Loizou and Dimitrova 2013) is a framework for supporting knowledge sharing in virtual communities through adaptive notifications.

4. Smartag (Belk et al. 2012b) is an adaptation and personalization system that personalizes the visual and interaction design aspects of E-Commerce product views based on individual differences in cognitive processing.
5. PRESYDIUM (Personalized Emergency System for Disabled Humans – Chittaro et al. 2011) is a Web-based adaptive medical information system that provides personalized instructions to nurses and volunteers to better assist persons with disabilities.
6. PERSONAF (Personalised Pervasive Scrutable Ontological Framework – Niu and Kay 2010) is an abstract framework for pervasive ontological reasoning aiming to address several personalization challenges in the context of pervasive computing such as supporting the ontological reasoning about location, personalization of information about location, and personalization to each user's conceptions of a building.
7. CTRL (Collaborative Tutoring Research Lab – Walker et al. 2009) is a framework for providing adaptive collaborative learning support, enabling researchers to combine different types of adaptive support utilizing domain-specific models as input to domain-general components.
8. EKPAIDEION (Tsianos et al. 2008) is an adaptive educational hypermedia system that adapts and personalizes the content presentation and navigation support within computer-based educational environments.
9. The AdaptiveWeb system (Germanakos et al. 2007) aimed to personalize content and functionality of interactive systems based on intrinsic human factors.
10. Knowledge Sea II (Brusilovsky et al. 2006) is a personalized information access system aiming to assist users to effectively organize and maintain Web-based educational resources.
11. CUMAPH (Cognitive User Modeling for Adaptive Presentation of Hyper-Documents – Tarpin-Bernard and Habieb-Mammar 2005) is an environment in which the hyper-document presentation is adapted and personalized by selecting the elements that best match the users' cognitive processing characteristics.
12. mPERSONA (Panayiotou and Samaras 2004) is a flexible personalization system for the wireless user that personalizes content and functionality based on user mobility, the local environment and the user and device model.
13. INSPIRE (Papanikolaou et al. 2003) is an adaptive educational hypermedia system which emphasizes the fact that learners perceive and process information in different ways, and integrates ideas from theories of instructional design and learning styles.
14. SQL-Tutor (Mitrovic and Martin 2002) is a knowledge-based teaching system which supports students learning SQL.
15. Proteus (Anderson et al. 2001) is a system that constructs user models using artificial intelligence techniques and adapts the content of a Web-site taking into consideration also characteristics of the wireless connection.

16. Web Browser Intelligence (WBI, pronounced "WEB-ee" – Maglio and Barret 2000) is a developed system that provides a loosely confederated group of agents on a user's workstation capable of observing user actions, proactively offering assistance, modifying resulting Web documents, and performing new functions.
17. ARCHIMIDES (Bogonicolos et al. 1999) personalizes the search results of users according to their interests.
18. TANGOW (Carro et al. 1999) is a tool for developing Internet-based courses, accessible through any standard Web browser. Courses are structured by means of teaching tasks and rules which are stored in a database and are the basis of TANGOW guidance ability.
19. AHA (De Bra and Calvi 1998) is an open Adaptive Hypermedia Architecture that is suitable for various different applications.
20. SKILL (Neumann and Zirvas 1998) is a scalable Internet-based teaching and learning system. The primary objective of SKILL is to cope with the different knowledge levels and learning preferences of the students, providing them with a collaborative and adaptive learning environment utilizing Web technologies.
21. ELM-ART II (Weber and Specht 1997) is an intelligent interactive textbook to support learning programming in LISP.
22. BASAR (Building Agents Supporting Adaptive Retrieval – Thomas and Fischer 1997) provides users with assistance when managing their personal information spaces.
23. InterBook (Brusilovsky et al. 1996; 1998) is a tool for authoring and delivering adaptive electronic textbooks on the World Wide Web.

The aforementioned systems can be categorized under the main domains of educational hypermedia systems and information retrieval systems, each one utilizing different features in their user models and applying different adaptation mechanisms and effects. Thus, these systems primarily focus on tackling usability and user experience issues in the context of online education and information retrieval. In the context of this thesis, we are motivated by existing state-of-the-art research in user modeling, adaptation and personalization, and accordingly utilize methods and techniques with the aim to improve usability and user experience issues of critical and prominent security mechanisms (user authentication and CAPTCHA). To our knowledge, no other adaptation and personalization systems applies cognitive processing characteristics of users as part of their user models, and accordingly apply these characteristics for recommending "best-fit" design factors of user authentication and CAPTCHA mechanisms (see also chapter 2 for a review on existing personalization approaches in user authentication and CAPTCHA).

3.8 Modeling Human Factors in Interactive Systems

Since the early 1990s, applications and services running on the World Wide Web have significantly grown in size and usage. As user interactions in such realms have become an integral part of peo-

ple's lives, in line with the globalization and sophistication of products and services, the need for personalization strategies for addressing "one-size-fits-all" issues and meeting the users' individual needs and preferences is nowadays even more evident.

As described in this chapter, researchers and practitioners have already identified various characteristics of users and factors that have important roles within specific domains and contexts of use for adapting and personalizing content and functionality of interactive systems. In particular, the factors being modeled for personalization in interactive systems include among others information about the users (e.g., interests, knowledge, preferences, needs and goals), information about the interaction device (e.g., screen size, input type), and information about the context of use (e.g., physical, social – Brusilovsky and Millán 2007). A number of techniques have been proposed to explicitly extract this information (e.g., through Web forms, questionnaires, etc.) or implicitly based on the users' navigation behavior within the system (Frias-Martinez et al. 2005), as well as through collaborative filtering based on users' common product ratings or buying history (Linden et al. 2003; Karat et al. 2004).

A high number of research studies have shown that modeling the aforementioned factors in specific domains of interaction enable users to demonstrate significant improvement in tasks' completion efficiency, effectiveness, comprehension and user experience. For example, personalizing educational hypermedia systems to the students' level of knowledge on particular domains and concepts has shown that raises students' comprehension capabilities. Furthermore, recommending specific products according to the users' interests on particular product categories has shown to improve task completion efficiency and provide a positive user experience. In this context, due to the heterogeneous users' needs and requirements within each domain, modeling these factors could be considered as a successful step towards personalizing human-computer interactions and improving the user experience. Nevertheless, the question remains whether such user models in each domain could be considered complete enough, and whether all the available vital factors of users are taken into account in order to provide a more complete, effective and human-centered result.

In this realm, as specific factors have shown to influence certain domains (e.g., modeling interests in recommender systems, and modeling knowledge in educational hypermedia systems), we believe that individual traits (attributes that define each person as an individual, e.g., cognition, emotions, personality) and their respective values may have an important (even though different in various cases) role in all domains and contexts of use that entail a human interacting with a computing system. For example, emotions might affect students while taking an exam in an educational hypermedia system, or might affect the users' decision for buying a particular product in an E-Commerce system. Furthermore, bearing in mind that human-computer interactions in interactive systems are primarily processed on a cognitive level, e.g., users are required to process and comprehend information, solve problems and take decisions, we suggest that such individual traits should be investigated and integrated in the user interface design process of interactive systems, with the aim to personalize their visual and interaction design accordingly.

Apparently, modeling individual traits and personalizing content and functionality of interactive systems is a challenging endeavor given the multi-dimensional and complex nature of such human factors. In this respect, individual differences have been widely applied in personalization systems but with mixed outcomes so far. On the one hand, modeling human cognitive factors for personalization systems has shown to improve task completion performance and user experience (Steichen et al. 2014; Belk et al. 2014a; 2014b; Su et al. 2011; Graf et al. 2009; Frias-Martinez et al. 2007; Germanakos et al. 2008; Papanikolaou et al. 2003; Bull and McCalla 2000). On the contrary, various studies concluded that cognitive processing factors do not have a main influence on users' task performance and preference within adaptive hypermedia environments (Brown et al. 2006; Mitchell et al. 2004). Thus, modeling individual traits and incorporating these in personalization systems still remains an important and challenging issue, and further studies and approaches are yet to be found (Brusilovsky and Millán 2007). In addition, we should not omit to clarify that such a diversity of research findings could be the result of the endogenous multidisciplinary approach of such study designs as follows: (i) The elicitation process of intrinsic human factors of users is heavily dependent on the validity and accuracy of the elicitation tools used in the various studies; (ii) the methodology of each study differs based on the scope and objectives of each research work in which also various external factors and different circumstances might influence the results such as environment, emotions of users, urgency, etc.; and (iii) given the multidimensional nature of intrinsic human factors and overall complexity of conducting such studies, the evaluation should be replicated over time since a single assessment of the influence of such characteristics on user interactions might not fully justify the results.

3.9 Summary

In this chapter we first made an effort to sum up existing knowledge and state-of-the-art works on user modeling in the context of adaptation and personalization systems. In summary, the information being modeled can either be static, when it contains parts that rarely or never change (e.g., demographic information), or dynamic, when the data change frequently. Such information is obtained either explicitly, using online registration forms and questionnaires resulting in static user models, or implicitly, by recording the users' navigation behavior and/or preferences during human-computer interaction. In the latter case, each user can either be regarded as a member of group and take up an aggregated user model or be addressed individually and take up an individual user model. The analysis on user modeling also showed that a high number of research works revealed successful personalization approaches that maintain user models which consist of various user characteristics and contextual features depending on their domain of application (most popular ones found in recommender systems and educational hypermedia systems). Yet, the question still remains, when a user model is considered complete? Do designers and developers of interactive

systems take into consideration those factors determined by individual differences for providing a more accurate and comprehensive result?

Furthermore, we overviewed the main personalization categories and respective adaptation technologies used for adapting and personalizing content and functionality of interactive systems to the individual user. We also described the main adaptation effects that are communicated to the user interface as a result of the respective mapping rules and adaptation technologies. We also presented an overview of selected state-of-the-art of adaptation and personalization systems and frameworks.

Traditionally, the aforementioned methods and techniques have been extensively considered from the two overarching research areas of adaptive hypermedia and Web personalization. It is quite clear that these two areas share a number of differences but at the same time many similarities, with the most evident one the fact that they share the same objective. Over time, both research directions have been using interchangeably adaptation technologies and effects for personalizing what is presented to the users, based on their specific needs and preferences. However, one could argue that the application fields are predominantly different, as adaptive hypermedia has found popular use in educational hypermedia and on-line information systems, whereas Web personalization in information retrieval systems (e.g., search engines) in the E-Business/ E-Commerce sector (with respect to products and services delivery). In this context, it could be inferred that Web personalization has a more extended scope than adaptive hypermedia and is a relatively new area of research. It explores adaptive content selection and adaptive recommendation based on modeling user interests and interaction behaviors. In fact, the most evident similarity is that they both make use of a user model to achieve their goal. However, the way they maintain the user model is different; adaptive hypermedia requires a regular interaction with the user, while Web personalization employs algorithms that continuously follow the user's navigational behavior without necessarily requesting explicitly an interaction with him. Generally, adaptive hypermedia refers to the manipulation of the link or content structure of an application to achieve adaptation and makes use at a larger extent explicit user modeling, whereas Web personalization refers to the whole process of collecting, classifying and analyzing Web data, and determining based on those the actions that should be performed so that the user is presented with personalized information. Technically, two of the adaptation/ personalization techniques they are using are the same: The adaptive navigation support (of adaptive hypermedia and else referred to as link-level adaptation) and link personalization (of Web personalization); and adaptive presentation (of adaptive hypermedia and else referred to as content-level adaptation) and content personalization (of Web personalization). Last but not least, it is noteworthy to mention that both research fields make use of artificial intelligence techniques.

Nevertheless, although adaptive hypermedia and Web personalization might have been usually applied in different application domains, adapting content and functionality of interactive systems based on different contextual requirements and constraints (and in cases utilizing different technol-

ogies), systems in both areas share a common high-level goal; to accurately model the pertinent users' characteristics and accordingly adapt their behavior to meet the unique expectations of users and offer a seamless positive and personalized user experience.

CHAPTER 4: Human Factors in Web Adaptation and Personalization

The effort to introduce human individual differences in the design of adaptation and personalization systems by creating user models and adaptation mechanisms that will be able to regulate information processing factors to the benefit of the unique user, is a challenging direction towards human-centered interfaces. Such an endeavor is mainly hampered by the fact that there is very limited experience regarding which characteristics are the most important in Web interactions (Tsianos et al. 2013). The term individual differences is indeed very broad, since it could include from genetics to personality; thus, it should be mentioned that the way that it is used in the context of this thesis derives from the field of differential psychology. The term (initially in German, Psychologie der individuellen Differenzen) was proposed by Stern (1900), in order to summarize the research on mental differences, in coordination to a notion of "general psychology". The emergence and proliferation of the individual differences research is not however directly linked to cognitive research; in fact, researchers from the fields of differential and cognitive psychology have often opposed each other, especially on whether psychometrical approaches are truly related to human cognitive structures (Glaser and Pellegrino 1978). Also, it is rather indisputable that, for the most part, individual differences research was based on (or provided a basis for) the study of intelligence (Dillon and Watson 1996). A common focal point of the theories of intelligence originate from the work of Thurstone (1948), who claims that there are certain distinct basic mental abilities (factors), in which people differ at some extent. All this work was at a large extent summarized by Carroll's (1993) very influential meta-analysis, which led to the development of his three stratum theory. A review by Deary (2001), on a relatively recent state of research on intelligence, revealed that individuals predominantly differ in the following abilities (the definitions are cited from McGrew 2009, p. 5-6):

- Visual (and spatial) ability: "The ability to generate, store, retrieve, and transform visual images and sensations".
- Verbal ability: "The breadth and depth of a person's acquired store of declarative and procedural reading and writing skills and knowledge".
- Memory (short-term): "The ability to apprehend and maintain awareness of a limited number of elements of information in the immediate situation (events that occurred in the last minute or so)".
- Processing speed: "The ability to automatically and fluently perform relatively easy or over-learned elementary cognitive tasks, especially when high mental efficiency (i.e., attention and focused concentration) is required".

Even though these intelligence factors are highly stable throughout a person's life-time, fluid reasoning, memory, and speed tend to deteriorate with high age. Such psychometric theories of individual differences are indeed much elaborated and complicated. However, we consider that a broad and thorough understanding of how people differ when required to perform mental tasks is

necessary in order to subsequently narrow down the number of possible user attributes that could be used in an adaptation and personalization scheme.

In our view, the aforementioned areas of cognition are a good starting point for the study of their respective effects in adaptive interactive systems. They are composed of constructs that refer to habitual or preferred modes of thinking, perceiving, and remembering (Tennant 1988), or to consistent individual differences in preferred modes of organizing and processing information and experience (Messick 1984). Interactive systems require both visual and verbal (reading) processing of information, affecting the high-level cognitive factors of the human brain, such as cognitive styles, in the way individuals process and remember information and primarily affect preference and performance in hypermedia systems, while at the same time maintain awareness of different elements (i.e., hyperlinks). On the other hand, persons with limited abilities in elementary cognitive processes, such as working memory capacity, may face increased difficulties in such systems, generating for example excessive cognitive loads during interactions resulting to imbalance situations, of what is expected from them and their perceived ability to meet those expectations (or demands). These assumptions do not necessarily imply that more intelligent persons excel during interactions with a system; each individual may have different strengths and/or weaknesses, and perhaps the employment of personalization techniques could result in providing tailor-suited environments.

A thorough presentation and analysis of all the cognitive theories and models that connect to the various levels of information processing is not in the scope of this thesis. Rather, our main effort in this chapter is to discuss a number of factors that we believe primarily influence information processing with respect to the decision making, problem solving and learning. Our main concern is to create a basic theoretical understanding pertinent to the utilization of those factors and their effects in the design and development of specific use cases of human-centered adaptation and personalization models and rules. Similarly, the reader could exploit and integrate alternative theories and/or routes of application depending always on his research directions and the distinctiveness of his studies.

4.1 Human Cognition and Information Processing

Historically, the research attempts of cognitive psychology concentrated upon the study, with the use of scientific research methods, of the human perception and cognitive processes that take place in the human mind during information processing (Davou 2000). At the beginning of the 20th century, the investigation of the mechanisms that affect the learning process was one of the main research directions for cognitive psychologists, who tried to design research procedures that would emulate the methods of pure and applied sciences, in an effort to establish psychology as “real” science. This view point led to the primacy of the phenomena that could be observed and more specifically to the correlation of the stimulus with the measurable results of a behavior. However, the intermediate processes of the mind and the mechanisms during the learning process could not

be directly observed deflecting from the aims and objectives of this research. The limited association of stimulus with the response, as well as the difficulty of making predictions and evaluations based on rigorous experimental methods, formed the core of behaviorism which became the dominant theoretical approach to the processes of learning (Hock 1999). It is worth to mention, that a cornerstone theory regarding the processes of learning and cognition, opposing the dominant theories of behaviorism at the time, is the one proposed by Tolman (1948) who introduced the concept of cognitive maps. A cognitive map is a mental representation which serves individuals to acquire, code, store, recall, and decode information about the relative locations and attributes of phenomena in their everyday or metaphorical spatial environment.

Nevertheless, the so called "cognitive revolution" was realized with the development of the computer in the 1950s which had a significant influence in psychology. The computer provided the grounds for researchers to use it as a metaphor through of which they could compare the human mental processing, by representing non-observable processes in an observable manner (computer-mind analogy). This comparison was used as a means for better understanding the way information is processed and stored in the human mind. The information processing perspective, which was an alternative theoretical approach taking over the so far theories of behaviorism, was based on the idea that individuals apply a more thorough processing of the information they receive, rather than simply responding to a stimuli they are presented with. Since then, the information processing theory (referring, for many, to the "software level" when associated with the human brain) has become one of the most prominent psychological theories that describes the process of learning, which can be defined as a change in a person's mental structures that creates the capacity to demonstrate different behaviors (Eggen and Kauchack 2007). More specifically, it emphasizes on how a stimuli from the environment goes through the processes of attention, perception, and storage throughout a series of distinct memory stores (Lutz and Huitt 2007). The organization of information in computing systems is proportionate with the inclusion of knowledge in the human brain, which supports the argument for efficient learning with the use of electronic environments.

Inevitably, cognitive psychology, as one of the main disciplines of cognitive science, is associated with the research fields of computer science, and more specifically with artificial intelligence, following a parallel path in developments; exchanging research data and theoretical approaches. In particular, artificial intelligence used theoretical models of cognitive psychology to understand and simulate human perception and processing while contributing decisively to demonstrate to what extent these models are effective. Furthermore, throughout the history of cognitive psychology, the field of artificial intelligence attracted psychologists and contributed to the development of theories driven occasionally from a different reasoning (Flanagan 1991), such as:

- The growth of computational power enables practitioners and researchers to simulate human behavior and address complex and hard to solve problems.
- This field is dominated by the concept of information processing and application rules.
- Computers use and interact with symbols on various levels.

- In the case of artificial intelligence, psychological events can be realized in various ways without being characterized by the physical manifestation of cognitive processes, but by their role in the operating procedure.

In addition, many argue that the metaphorical relationship between computing and cognitive psychology has contributed for the educational effectiveness of hypermedia due to the structural similarities in the organization of information (Swindler 2001).

Nonetheless, despite the promising convergence and results of artificial intelligence and the information processing model, over the past decades, researchers recognized that computers can only serve as a loose and pretty general model of human memory, which is related to the specifics of how the brain actually codes or manipulates information as it is stored in memory (human memory is one of the primary areas of cognition and is discussed in the next section).

At a secondary level (also called as the "hardware level" of the human mind), that dictates the relationship of cognitive psychology with neuroscience; research works concluded that learning and information processing depend upon inherent structural parameters (Graber 2000). This predicts individual differences in learning and processing abilities among individuals, constituting a subject of interest for adaptation and personalization systems too. Specifically, the network of the human brain is estimated to consist of 10 to 100 billion neurons, out of which each one of them has the specialized ability to process specific information, and is triggered when a stimuli is associated with the encoding ("programming") of each neuron. Incoming information is fragmented into very small pieces and processed by specialized neurons, and then, if necessary, regenerated. The possibility to develop logical associations depends in turn on the electrical connections between neurons, synapses. Accordingly, the cognitive response to a stimulus depends on the presence or not, and the number of available synapses between the existing information associated with the stimulus and the ability to formulate new synapses (Graber 2000). Furthermore, the failure of processing new information may be related mostly with the physiological parameters of an individual rather than the behavioral ones. That is because even though the structure of the brain between people is broadly similar, the number of connections vary, and although they link to external stimuli, there is a tendency of repetition, and the trigger of existing synapses, rather than the creation of new ones. In addition, during childhood, the human brain is highly receptive to new input of information due to the large number of nerve recipients, transmitters and connections. In adulthood, the synapses that are not used become inactive. Thus, practicing and training of mental abilities broadens the possibility of processing information.

To the extent that neuroscience can portray the way information is recorded at the level of "hardware", cognitive functions are not independent of the physiology of the human brain, but rather they affect how each person perceives and processes information. These differences can also relate to the learning process, even though it is not clearly discernible because of the high complexity of the human brain and the relationship between the "hardware" and the "software" of the human mind.

4.1.1 The Role of Human Memory

Over the last fifty years, a high number of works have focused on understanding human cognitive processes, proposing various models, definitions and interpretations on the structure of an internal information processing system. Researchers have attempted to describe the basic architecture of this system, defining as 'information', any stimulus that is newly processed or is already exploited by the human mind to comprehend objects, events and situations (Anderson 2009). The study of memory and its relationship or integration to human cognition was at the time in the center of most research directions in cognitive psychology. The various suggestions and perspectives tried to formulate a consensus on several aspects of information processing, mainly emphasizing on how the brain encodes, stores and retrieves information from the memory. These approaches, triggered many times by conflicting realizations, refer to memory as a multi-faceted, limited capacity, mechanism that maintains a number of connections, representations, or structures which are related to the accumulated life-time perceptions and/or mental experiences of a person. The stored information is liable to change or manipulated when new stimuli or knowledge is acquired, while the interaction of the new information with the stored information could be demonstrated as a top-down, bottom-up or a combination of the two, system (Gibson 1979; Driscoll 2001; Eliasmith 2001; Winn and Snyder 2001; Huitt 2000).

Despite the disagreement and the different view angles on many levels of understanding, it seems that there is an agreement among most cognitive psychologists on some basic principles, which are derived from an inherent consistency of cognitive processes during execution (when individuals process information – Huitt 2000). This agreement or homogeneity was proposed through the Multi Store Model of Memory of Atkinson and Shiffrin (1968), which has been widely used for explaining how information is processed by humans. The Multi Store Model of Memory suggests that memory is made up of a series of stores and it consists of three separate components (see Figure 6): *The sensory register*, in which sensory information enters memory (e.g., acoustical, visual information); *the short-term memory* (also called working memory), which receives and holds input from both the sensory register and the long-term memory; and *the long-term memory*, where information which has been rehearsed in the short-term memory is stored indefinitely. In case rehearsal does not occur, information is forgotten, lost from short-term memory through the processes of displacement or decay. This model is forced to simplify and break a dynamic process in its essential components, while in many places appears to represent human functions in a highly mechanistic way.

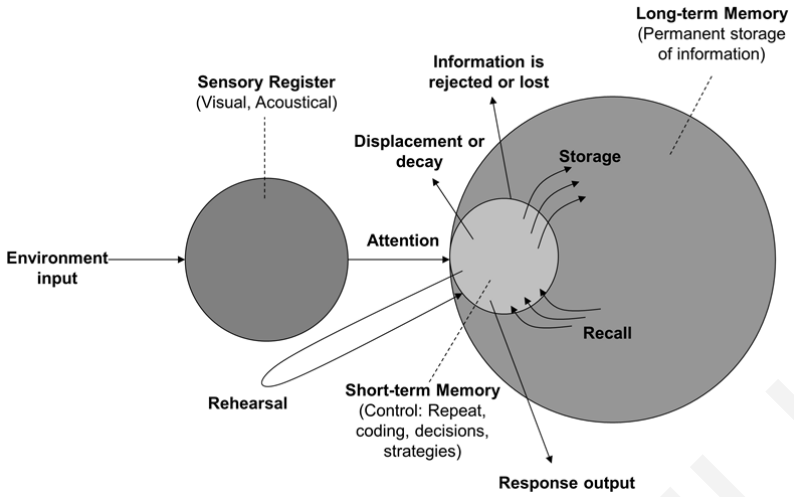


Figure 6. Representation of the Multi Store Model of Memory (Atkinson and Shiffrin 1968)

Still, in this context, a number of research works have criticized its simplicity since it ignored the functional dynamic aspect of information processing for the sake of a structural, linear description (Baddeley 1990). Recent research models and methods suggested replacement of the above weaknesses, enriching the original memory model with statements about the quality and depth of processing in which the information is submitted in each area of the cognitive system (Craik and Lockhart 1972), or highlighting explicitly the importance of a particular area, the working memory for the current information process (Baddeley and Hitch 1974; Baddeley 1986). Nevertheless, the three main components of the model, in the form of treatment and nature of the information they process are in general widely accepted. The main components of the memory model are described next (Davou 2000; Eysenck and Keane 2005).

Sensory Memory

Any stimulus that is coming from the individual's surrounding environment and detected by the human senses is briefly available in sensory memory. This temporary retention of information as they enter the brain is also called sensory buffer, because it concerns information detected by the senses and not yet processed further in the human brain for processing and interpretation. An unlimited amount of information can be put into sensory memory but being only active for a limited amount of time, since as the person is continuously in communication with the environment, new information is constantly shifting and entering while removing the old. The detection of the information in sensory memory is also related to the concept of attention, and the information is further processed to a subsequent stage in short-term memory. This refining capacity of sensory memory has the advantage to "withstand" the unrestricted flow of information but also a key disadvantage is that, when the rate and intensity of inflow of such information increases, and exceeds the decay rate or shifting "useless" information, its effectiveness and efficiency is dropped, causing confusion.

Short-term Memory and Working Memory

Due to the high number of sensory input from the environment, much of the information in sensory memory decays and is forgotten. Once information is attended, it is transferred to the short-term memory. In contrast to sensory memory where a high number of information can be active, in short-term memory the time and capacity is limited. According to Miller (1956), short-term memory might contain from 5 to 9 objects active at the same time (7±2). More recent studies have refined and extended these findings and further confirmed the limited capacity of short-term memory. At this stage, the information stays for a longer time active than in the sensory memory. The information may be contained in the short-term memory for up to 30 seconds. Apart from the limited capacity and the limited life time of information, a third characteristic of short-term memory is its high fragility (Eysenck 1988). In particular, the information in short-term memory is not yet permanently "registered" in the cognitive system. Information is maintained in this part of the system and undergoes the required processing, which will either lead to permanent storage (in long-term memory) or will be rejected from the human mind. This temporary hold of information is fragile and easily disrupted by other incoming information (or existing, retractable information), so that a possible distraction can lead to confusion or total loss of information. Short-term memory is the area where new and current information is entered and processed in the human mind, but also associated with existing information an individual has in long-term memory that is drawn to use as a reference framework for the classification and interpretation of new information. Given its limited capacity, short-term memory is unable to retain a lot of information concurrently active for processing, which eventually might cause the problem of "overload" of the cognitive system in case a high number of information is being presented and processed.

The conception of working memory grew out of the literature on short-term memory (Baddeley 1992; 2012) as an empirical model of cognitive functions used for temporarily storing and manipulating information. Although short-term memory and working memory are used interchangeably in many occasions, short-term memory could be referred as the simple temporary storage of information, whilst working memory as the combination of storage and information manipulation (Baddeley 2012). Baddeley and Hitch (1974) proposed the multi-component model of working memory (see Figure 7) which consists of a *central executive* that is the central system for pointing attention to relevant information, removing irrelevant information as well as coordinating cognitive processes when multiple tasks must be performed at the same time.

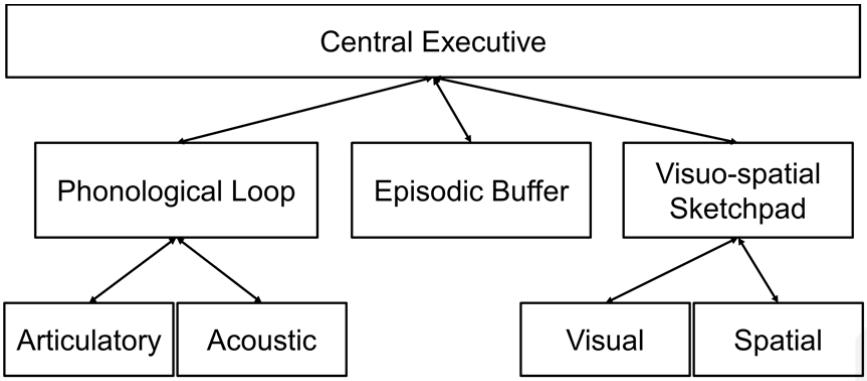


Figure 7. Baddeley and Hitch's working memory model (1974)

In the initial model, the central executive consists of two subsystems (slave systems), the *phonological loop* that stores phonological information and continuously articulates its contents for refreshing the information and prevent decay, and the *visuo-spatial sketchpad* that stores visual and spatial information (e.g., constructing and manipulating visual images (e.g., shape, color, etc.), and representing mental maps (e.g., location). An extension of the model was proposed in Baddeley (2000), in which a fourth component was included in the model, the *episodic buffer*. The episodic buffer holds representations that integrate phonological, visual, and spatial information as well as information not covered by the slave systems (e.g., semantic and musical information).

Long-term Memory

Long-term memory is the final stage of Atkinson and Shiffrin's human memory model (Atkinson and Shiffrin 1968). In this stage, information remains for a long period of time or indefinitely. In short-term memory, newly entered information is associated with older, related information retrieved from the long-term memory which is further organized and interpreted for giving meaning to the information. In the long-term memory, this new and processed information is stored in a wider network of knowledge for each person. Opinions of researchers differ on the duration of stay of information in long-term memory. Some consider that once the information is entered into this form, this information is never removed or lost by an individual's cognitive system. Others argue that there is a possibility that information might be "lost" from long-term memory, in case the information is not placed in the correct position within the network of information already available to the person, or in case this information has not created strong bonds with other existing information (Baddeley 1990; Eysenck 1988). Nevertheless, it is agreed that the information entered in long-term memory is maintained throughout the life-time of the individual and serves as a knowledge base on which the new information is decoded, i.e., compared, interpreted and organized (Loftus and Loftus 1980).

Long-term memory is comprised of *explicit memory* and *implicit memory* (Atkinson and Shiffrin 1968). Explicit memory (declarative memory) refers to information that is consciously

available. Explicit memory has three subdivisions: *Episodic memory* that refers to memory for specific events in time (e.g., remembering a person's name and incidence of interaction with that person); *semantic memory* that refers to factual information (e.g., the meaning of words); and *autobiographical memory* that refers to information regarding events and experiences of an individual. Implicit memory refers to procedural information about the body of the person, e.g., how to brush the teeth, how to swim, etc.

4.1.2 Visual Perception

Visual perception is of vital importance in our everyday lives, since it enables individuals to move around freely, to recognize other people or objects, to read books, to identify depth and proximity or to watch videos and movies. Similarly, visual perception, as well as the concept of visual attention (as described in the following sections), are some of the most important factors that influence the area of HCI. As it is known, the most common human-computer communication medium is the screen of a device, where through the optical channel a user perceives the information that is presented. The use of graphics on the computer screen enables the representation of images which resemble real objects causing the same cognitive recognition procedures as those followed in the real world. *Visual perception* as defined by Sekuler and Blake (2002, p. 621) is *"the acquisition and processing of sensory information in order to see, hear, taste, or feel objects in the world; also guides an organism's actions with respect to those objects"*. Even though it might be considered as an inherent "automatic" ability that many times is ignored, visual perception is a complex process that is supported on the one hand by the functioning of the optical sensor (eye, neural pathways, and the brain), and on the other hand by the cognitive functioning of understanding the receptive stimuli. The eye receives the stimuli in the form of light, which stimulates the light-sensitive retina at the back of the eye, in which thousands endings of the optic nerve are concentrated, that in turn help to transfer the visual stimulus to the corresponding brain center. Understanding the visual stimuli is the process that allows us to recognize three-dimensional objects, their relative distances, the color, the brightness, etc. A big number of theoretical approaches that investigate this process support that individuals perceive the surrounding world by combining the receptive stimuli based on their prior knowledge and experiences generating meaning and images (Marr 1982). Our expectations and context may affect our visual perception, while the post-processing of the visual stimulus and our past experience allows us to see the images stable while we move in space, the color and brightness of objects unchanged as light is constantly changing. It also allows us to understand that the size of objects does not change, although those get eventually visually smaller when we are moving away from them. Nevertheless, there is still a major controversial theoretical issue based on which psychologists usually are divided. This is expressed through the understanding whether the perception starts by the stimulus itself (and the information related to it), known also as 'bottom-up' or 'direct theory' of perception (Gibson 1966), or it is more 'indirect' a.k.a. 'constructiv-

ist' or 'top-down' theory (Gregory 1970), that refers to the use of contextual information (increasing meaning) in the pattern recognition or in our perception of reality.

The Gestalt psychology has also influenced significantly the study of how individuals perceive visual components and how they are organizing them. Gestalt theory, which contributes mostly to the concept of the perceptual grouping, tries to understand the ability of individuals to acquire and maintain meaningful perceptions in a rather chaotic world by forming a global whole with self-organizing abilities. Its principles (or laws of organization) support that the human mind maintains a perception of the visual stimuli that gives value to the whole (standing as a reality on its own) irrespective of the parts that it consists of (Wertheimer 1923; Koffka 1935; Kohler 1947). The Gestalt principles are briefly summarized as follows: (a) Principle of *proximity*, objects that are close to each other are formulating groups; (b) principle of *similarity*, objects which are similar with respect to their shape or color belong to the same group; (c) principle of *closure*, objects (or regular figures) that are not complete tend to be perceived as a whole by individuals (our mind fills in the visual gap); (d) principle of *continuity*, the elements of objects that are aligned within an object tend to be grouped together perceived as an integrated whole; (e) principle of *common fate*, the elements that move towards one (the same) direction or in the same speed are perceived as elements of a common group that moves towards that directional line or path; and (f) principle of *symmetry*, the elements (or areas) of objects contained between symmetrical limits appear (or perceived) to create solid coherent shapes.

The Gestalt principles have a direct application in HCI and the design of interactive hypermedia systems since their usability and acceptability by the users depend at a large extent upon whether: They facilitate grouping of similar objects or shapes, they connect the details of figures or content on reasonable ways when information is missing (e.g., surfaces presented as homogeneous regions rather than as scattered spot phenomena), they provide meaningful descriptions on activities, they use metaphors and identical terminology on prompts, menus, help, etc., they maintain consistent sequence of actions in similar situations, and so on.

4.1.3 Visual Attention, Speed and Control of Processing

Attention is defined as a process of concentrating on a discrete aspect of information (visual or auditory). During this process attention is deviating from any other (not pertinent) objects in order to achieve effective engagement with the particular object (James 1890). A high number of researches have focused on *visual attention* since it is considered as one of the most important human sense and because visual objects can be precisely controlled and manipulated (e.g., display time, shape of the object, etc.) for investigating and understanding the concept of visual attention (Eysenck and Keane 2005). Several research works (Vecera et al. 2014; Corbetta and Shulman 2002; Posner 1980; Posner and Petersen 1990; Yantis and Jonides 1990) suggest that attention is split in two main types: the *goal-driven*, which is voluntary, endogenous and directed from the target, and the

stimulus-based, which is involuntary, exogenous and directed by the stimulus. Depending on whether the objects of attention are one or more, attention can be focused or divided. In the latter case, peripheral vision is used in which visual information is viewed from outside the center of the gaze, e.g., when viewing the movements in a room while talking to a person.

The process of visual attention may be divided into two successive stages: the pre-attentive stage and the limited-capacity stage. In the *pre-attentive stage*, the information goes through a parallel processing from the entire field of view, and determines areas of interest through it (determines important visual elements). The pre-attentive stage of vision subconsciously defines objects from visual primitives, such as lines, curvature, orientation, color and motion and allows definition of objects in the visual field. The *limited-capacity stage*, which is based on the aforementioned pre-attentive mapping, performs a high-level processing which is driven by some more generic criteria. When items pass from the pre-attentive stage to the limited-capacity stage, these items are considered as selected. Interpretation of eye movement data is supported by the empirically validated assumption that when a person is performing a cognitive task, while watching a display, the location of his gaze corresponds to the symbol currently being processed in working memory and, moreover, that the eye naturally focuses on areas that are most likely to be informative (Gulliver and Ghinea 2004).

From the perspective of individual differences in human cognition, various theories exist that aim to describe and explain how and why individuals differ in attention (Demetriou et al. 2013). Researchers attempted to understand attention and the functioning of the human mind in terms of more basic processes, such as control of processing and speed of processing (Demetriou et al. 2013). *Control of processing* refers to cognitive processes that can identify and concentrate on goal-relevant information and inhibit attention to irrelevant stimuli. Control of processing is also closely related to the individual's *speed of cognitive processing* which refers to the maximum speed at which a given mental act may be efficiently executed. Speed of cognitive processing and control of processing are directly related to a person's age, as well as to the continuous exercise and experience, with the former to be the primary indicator.

Various research works argue that the aforementioned cognitive processes have an effect on comprehension, learning and problem solving (Conway et al. 2002; Shipstead et al. 2013; Demetriou et al. 2002; Unsworth and Spillers 2010; Klingberg 2009). They are mainly used in mental tasks, such as arithmetic tasks, e.g. 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, or recognizing the distorted text of a CAPTCHA mechanism.

Studies revealed the relationship between cognitive processing abilities and working memory capacity (Conway et al. 2002; Polderman et al. 2006). Enhanced speed of information processing facilitates access to information that is sustained in the working memory system (Baddeley 1992). In addition, enhanced speed of processing enables individuals to handle more efficiently information flow during problem solving, because information can be represented, interpreted, and inte-

grated before it is lost through decay or interference (Hale and Fry 2000). On the other hand, enhanced working memory capacity enables individuals to represent and process more information units at the same time enabling them to construct more complex concepts or relations.

The relationship between control of processing and working memory capacity is also well documented (Shipstead et al. 2013; Engle 2002; Kane et al. 2007). Working memory capacity predicts the ability to rapidly focus attention (Heitz and Engle 2007). For example, individuals with enhanced working memory capacity are less susceptible to Stroop interference (Hutchison 2007; Unsworth and Spillers 2010). Working memory capacity also predicts the ability to avoid being distracted by powerful stimuli. For example, a study conducted by Conway et al. (2001) investigating working memory capacity effects within the cocktail party phenomenon, revealed that individuals who detect their name in an irrelevant message have relatively limited working memory capacities, suggesting that they have difficulty blocking out, or inhibiting, distracting information.

4.1.4 Learning Styles

Learning styles represent a particular set of strengths, techniques and preferences that individuals employ during the learning process (on how they learn). For many years, research on learning styles has generated great interest but also divergent viewpoints (Coffield et al. 2004), since they are widely varied, and some of them fail to exhibit satisfactory reliability and validity (Markham 2004). In this respect, many researchers have criticized the scientific basis and theories of learning styles and their influence on educational learning (Coffield et al. 2004; Henry 2007; Curry 1990). However, as empirical research often demonstrates, learning style and the definition of specific learning strategies is an important factor in the computer mediated learning process, facilitating individuals to achieve more effective learning (Tsianos et al. 2006; Boyle et al. 2003), though not always in an expected way (John and Boucouvalas 2002). It has been argued that the distribution of learning material in ways that match learners' ways of processing information is of high importance, since it *"can lead to new insights into the learning process"* (Banner and Rayner 2000). Regarding these individual differences, there have been many attempts to clarify cognitive and learning parameters that correlate to the effectiveness of learning procedures, often leading to comprehensive theories of learning or cognitive styles (Cassidy 2004). Within the context of educational psychology, theories of learning styles have been developed, addressing the issue of individual differences in learning, or more specifically the perception, processing and retaining of information, while they also serve as a link between cognition and personality (Sternberg and Grigorenko 1997). Learning styles, as a term, are frequently used interchangeably with cognitive styles (described in more detail in the next section), which are *"consistent individual differences in preferred ways of organizing and processing information and experience"* (Messick 1984). Nevertheless, learning styles and cognitive styles are broader concepts that incorporate a greater number of not

mutually exclusive characteristics, in which learning styles rather focus on learning than on cognitive tasks (Cassady 2004).

Curry's 3-layer onion model (Curry 1983) classifies learning styles in a way that they are not mutually exclusive, but co-exist in different levels of learning processes. Specifically, moving from the inside to outside, the innermost layer is called *cognitive personality style*, and is the most stable trait. The middle layer is the *information processing style*, whilst the outermost consists of *instructional preferences*. Theories that fall in the inner layer are mostly related to cognition or traditional personality research, while more learner-centered approaches fit in the middle layer. The outer layer is more unstable, and it should be mentioned that according to Sadler and Riding (Sadler-Smith and Riding 1999) it is affected by the inner layer. However, the Dunn and Dunn model (1985) that belongs to the layer of instructional preferences exhibits high reliability and validity, but its implications are not easily related to Web-based environments. On the basis of this onion model a number of learning styles' models has been proposed in the literature (the reader can find a more thorough classification in Atkins et al. 2001).

Kolb's Learning Styles Inventory (LSI – Kolb and Kolb 2005) has been widely used for personalizing E-Learning hypermedia systems (Milosevic et al. 2007; Botsios et al. 2008). The Kolb's LSI proposed four distinct learning styles associated with four stages that students go through during a learning cycle: (i) Students initially gather solid experience on an issue; (ii) based on this experience students make (internal) reflections on the issue; (iii) they create abstract concepts and make generalizations; and finally (iv) they test in practice (experimentally) new knowledge and provide explanations for new situations. In his model, Kolb proposed that each individual shows preference for one of the four stages of the cycle, which uses at a greater extent and gives the appropriate learning style. Accordingly, the Kolb LSI distinguishes an individual's learning style as: (i) *Convergers*, individuals that prefer to discover possibilities and relationships, concentrate better when studying alone and better understand through abstract thinking; (ii) *divergers*, individuals that prefer real life experience and discussion, are imaginative, like brainstorming and group work, prefer observing; (iii) *assimilators*, individuals that solve problems with deductive reasoning and have the ability to create theoretical models; and (iv) *accommodators*, individuals that solve problems by carrying out plans and experiments, challenges theories, are adaptable and work based on gut feeling rather than logic.

Another learning style theory is the Felder/ Silverman Index of Learning Styles (ILS – Felder and Silverman 1988) which has also been widely used for personalizing E-Learning hypermedia systems (Graf and Kinshuk 2009; Papanikolaou et al. 2003). The Felder/Silverman ILS distinguishes students into one of the following learning style dimensions: (i) *Sensing learners* that are concrete, practical, oriented towards facts and procedures, or *intuitive learners* that are conceptual, innovative, oriented towards theories and meanings; (ii) *visual learners* that prefer visual representations of presented material (e.g., pictures, diagrams, flow charts), or *verbal learners* that prefer written and verbal explanations; (iii) *active learners* that learn by experimenting and working with

others, or *reflective learners* that learn by thinking things through and working alone; and (iv) *sequential learners* that work linearly, orderly and learn in small incremental steps, or *global learners* that have a holistic approach in learning and learn in large leaps.

Other popular learning style models include among others Neil Fleming's VARK model (Leite et al. 2009) which distinguishes learners as visual learners, auditory learners, reading-writing preference learners and kinesthetic learners or tactile learners, and Honey and Mumford's Learning Styles Questionnaire (LSQ – Honey and Mumford 2006) that made two adaptations to Kolbs' experiential model to reflect managerial experiences of decision making/problem solving, and proposed four dimensions (Activist, Reflector, Theorist and Pragmatist). An extended review of other learning style models (including cognitive style models) can be found in the report of Coffield et al. (2004) that reviewed the literature on learning styles and examined the 13 most influential models.

4.1.5 Cognitive Styles

Research on cognitive styles is an area of human sciences to explain empirically observed differences in information mental representation and processing. Different theories have been proposed over time suggesting that individuals have differences in the way they process and remember information. Due to the multi-dimensional nature of cognitive styles, a global definition has not been given to date. Nevertheless, in a recent global E-Survey of 94 individual style researchers and experts (Peterson et al. 2009) of the ELSIN network (European Learning Styles Information Network), who were asked to comment on the state of the field and their own understanding of the phenomenon being studied, the majority agrees that *"cognitive styles are individual differences in processing that are integrally linked to a person's cognitive system. More specifically, they are a person's preferred way of processing (perceiving, organizing and analyzing) information using cognitive brain-based mechanisms and structures. They are partly fixed, relatively stable and possibly innate preferences"*.

The work of Riding and Cheema (1991) is considered an important turning point for cognitive style research (Peterson et al. 2005), that made a survey of approximately thirty different cognitive styles and concluded that most of the proposed theories measured two broad style dimensions: (i) A *Verbal/ Imager* dimension that refers to how individuals process information and indicates their preference for representing information verbally (Verbals) or in mental pictures (Imagers); and (ii) a *Wholist/ Analyst* dimension that refers to how individuals organize information and indicates a preference of structuring information as a whole to get the big picture (Wholists) or structuring the information in detail (Analysts). We next describe these two dimensions.

Verbal/ Imager Dimension

One of the most widely accepted theories of human cognition is the Dual Coding Theory (Paivio 2006; Paivio and Csapo 1973). It suggests that visual and verbal information (respectively, image-based and text-based) is processed and represented differently and along two distinct cognitive subsystems in the human mind; the visual and verbal cognitive subsystems. Each subsystem creates separate representations for information processed which are used to organize incoming information that can be acted upon, stored, and retrieved for subsequent use.

Many psychology studies have reported that pictures are better recognized and recalled by the human brain than textual information, referred as the picture superiority effect (Anderson 2009; Ally and Budson 2007; Brady et al. 2008; Paivio and Csapo 1973). Paivio's Dual Coding Theory explains the picture superiority effect that pictures are more perceptually rich than words which lends them an advantage in information processing. Pictures are processed and represented as they are perceived (e.g., color, shape, etc.) but are also represented automatically as words (e.g., *"picture of a car"*), and thus have two representations for the same picture being observed. In contrast, textual information is not automatically represented as a picture without explicit instruction or additional mental effort. The redundant representation for pictures (two representations instead of one) increases their processing efficiency and memory strength. In addition, the picture superiority effect might be explained by the fact that pictures are mentally represented along with the features being observed, whereas text is visually sparse and represented symbolically, where symbols might have a different meaning depending on the form of the text, which requires an additional processing for the verbal subsystem. For example, 'X' may represent the Roman numeral 10 or the multiplication symbol (Biddle et al. 2012).

Nevertheless, other research findings claim that the picture superiority effect does not always hold and is affected by various factors (Oates and Reder 2010; Reder et al. 2009; Brady et al. 2008; Robertson and Köhler 2007; Whitehouse and Maybery 2006). For example, 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. This way the picture can be represented efficiently and effectively in its dual form (visual and verbal). Results of their study reveal that abstract pictures are not memorable as single words since the visual stimuli is difficult to identify, and hence, a generation of a consistent textual label is not easy or possible. Robertson and Köhler (2007) have further provided evidence that the ability to label a picture affects its processing and memory. In their study, they assessed 4-6 year old children and reached the conclusion that whenever children could successfully name aloud the picture during encoding were more likely to remember it later.

In this context, as an effort to explain the aforementioned empirically observed differences in users' mental representation and processing of information, many researchers have developed theories of individual differences in cognitive style from the perspective of dual coding theory (Riding

and Cheema 1991), and consequently, argue that individuals have differences in the way they process and remember information. In particular, individuals may process verbal information more efficiently than visual information (Verbals), whilst others the opposite (Imagers). Although it is likely that individuals switch strategies depending on the nature of the task, studies have revealed that individuals consistently prefer one or the other strategy (Riding and Cheema 1991). Furthermore, ability might affect preference towards a particular strategy in that if a particular mode of processing is more efficient for a person then it is more likely to be preferred.

Wholist/ Analyst Dimension

The Wholist/ Analyst dimension is strongly related to the theory of field dependency/ independency proposed by Witkin (Witkin 1962; Witkin et al. 1977) which is considered one of the most important and highly researched cognitive styles (Rezaei and Katz 2004; Riding and Cheema 1991). In particular, Witkin distinguished individuals being field dependent and field independent in which he describes field independence as *"an analytical, in contrast to global, way of perceiving which entails a tendency to experience items as discrete from their backgrounds and reflects ability to overcome the influence of an embedding context"*. For example, when confronted with problems, some individuals are good at extracting things from the context and prefer to handle them in a more analytical way. In contrast, individuals termed as field-dependent cannot abstract an element from its context and are intended to handle problems in a holistic way.

Accordingly, Riding and Cheema (1991) proposed the Wholist/ Analyst dimension and classified users to the cognitive typologies of Wholist or Analyst which are respectively mapped to the field dependent and field independent typologies of Witkin. Their different characteristics and implications on hypermedia systems are the following: (i) Users that belong to the *Wholist* class view a situation and organize information as a whole, proceed from the whole to the parts and organize information in loosely clustered wholes. Wholists have high assertiveness, and especially in extreme types, they are decisive; while (ii) users that belong to the *Analyst* class view a situation as a collection of parts, stress one or two aspects at a time, proceed form the parts to the whole and organize information in clear-cut groupings (chunking down). Analysts have low assertiveness and especially in extreme types, they are indecisive.

4.1.6 Elicitation Methods of High-level and Elementary Cognitive Processes

Elicitation methods for high-level information processes include mainly questionnaires where participants express their experiences and preferences, and psychometric tests that measure response times of participants on specific aptitude tasks. In the case of learning styles, popular elicitation tools include Kolb's Learning Style Inventory (Kolb and Kolb 2005), the Felder/Silverman Index of

Learning Styles (Felder and Silverman 1988) and Honey and Mumford's Learning Styles Questionnaire (Honey and Mumford 2006). In the case of cognitive styles, 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"* (OSIVQ – Blazhenkova and Kozhevnikov 2009). However, for the reason that questionnaires showed relatively low internal reliability and poor predictive validity (Blazhenkova and Kozhevnikov 2009; McAvinue and Robertson 2007), objective measures through the development of psychometric tools have emerged, such as response time in solving cognitive tasks that require verbal or visual processing. In particular, psychometric tools have been proposed that typically require from the participant to provide an answer to text-based or image-based statements. Depending on the response time of each answer, the ratio of means or medians between the verbal and visual statements is computed and further used to classify the participant to a particular group; Verbal or Imager group. Popular psychometric tests that highlight differences in the Verbal/ Imager dimension include the VICS test (Peterson et al. 2005) and the CSA test (Riding 1991). Figure 8 and Figure 9 illustrate an example of the VICS test in which individuals are presented with a set of cognitive verbal and imagery tasks. Figure 8 illustrates an example of an imagery item, in the form of a word, while Figure 9 illustrates the same core imagery item as in Figure 8, but this time in the form of a picture. Main aim is to illustrate the pictures and words in a different format and not in content, aiming to investigate if users respond differently to the picture and word based stimuli.

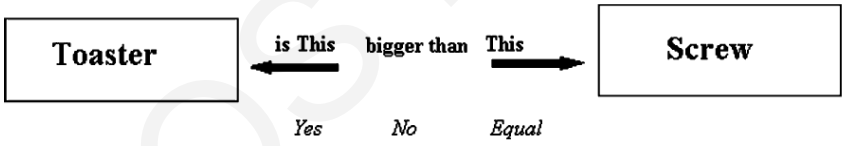


Figure 8. Example of an imagery item in the word form (Peterson et al. 2005)

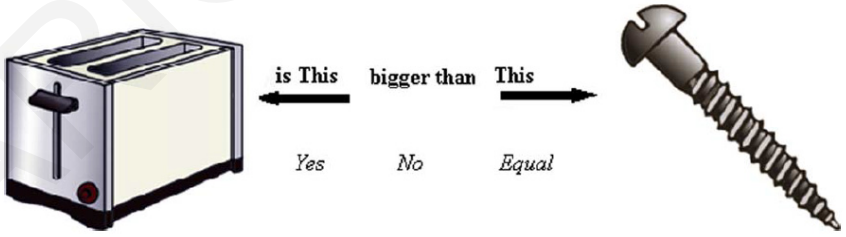


Figure 9. Example of an imagery item in the picture form (Peterson et al. 2005)

Measurement of Wholist/ Analyst tendencies primarily involves the dis-embedding of a shape from its surrounding field (Riding and Cheema 1991). Some of the earliest methods include the Rod-and-Frame Test in which participants are required to determine the upright position of a rod; the Body Adjustment Test, in which subjects judge their body position in different fields (e.g., defining their body position in rooms with tilted walls and chairs); the Rotating Room Test, in which subjects adjust a room to the true vertical position; and the Group Embedded Figures Test (GEFT – Witkin et al. 1971), in which participants are required to find common geometric shapes in a larger design (Figure 10). Also, computerized tests include the CSA test (Riding 1991) and the E-CSA-

WA test (Peterson et al. 2005) in which participants are required to judge whether two geometrical figures are identical or not, and decide whether a geometrical figure is embedded in a larger complex figure. The reader may also refer to Kozhevnikov (2007) and Riding and Cheema (1991) for a review on older questionnaires and psychometric tests.

In recent years, there have been also many research attempts that employed computational intelligence techniques to dynamically extract and/or correlate cognitive styles with users' navigation behavior. Frias-Martinez et al. (2007) utilized a number of clustering techniques to understand human behavior and perception in relation with cognitive style, expertise and gender differences of digital library users; Antoniou and Lepouras (2010) studied the connection between the way people moved in a museum and the way they preferred to approach and process information cognitively; Hsu and Chen (2011) investigated how learners' cognitive style affect their navigation behavior through data mining techniques as well as analyzed how navigation behavior may influence performance in education environments; and Kinley et al. (2010) explored the relationships between Web users' searching behavior and their cognitive style. Finally, a more recent study of Belk et al. (2013b) revealed a relationship between the Wholist/ Analyst dimension and the users' navigation behavior in terms of linearity/ non-linearity. In particular, results revealed that Wholists tended to follow linear hyperlink sequences within online encyclopedia articles, in contrast to Analysts who did not reveal any significant differences in navigation behavior.

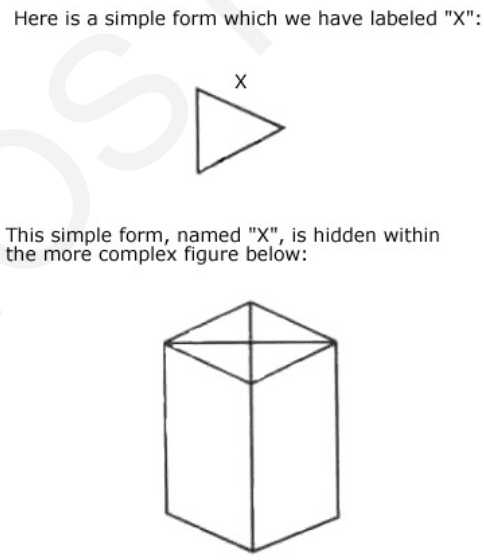


Figure 10. Sample item from the GEFT booklet (Witkin et al. 1971)

For the more elementary processes, a typical measure of cognitive processing control is the Stroop task which requires individuals to name the color in which a word has been printed, while ignoring the word itself (Stroop 1935). 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 control of

processing (MacLeod 1991; Stroop 1935). Individuals being faster indicating the printed color of the word tend to have more efficient controlled of processing.

As we have seen earlier, working memory is a system that consists of the central executive that controls the two slave systems (visuo-spatial sketchpad and phonological loop), plus the episodic buffer that provides a temporary interface between the slave systems and the long term memory. In order to identify the capacity/ storage of each subsequent sub-system, participants could go through a series of working memory span tests. At first, the test of Demetriou et al. (2013) could be used for measuring both the central executive function and the verbal storage ability (phonological loop span), providing an indication of individuals' working memory ability. Undertaking this assessment test, individuals are required to store the last word of a series of consecutively presented (written) sentences, while deciding at the same time whether the meaning of each sentence makes sense or not. The test gradually becomes more difficult, since the number of sentences increases from two (first level) to nine (last level). There are six series of sentences in each level, and the participants have to remember correctly the last words of four at least series in order to proceed to the next level. Secondly, a working memory test to measure the visuo-spatial sketchpad could be used (Demetriou et al. 2013). A total of 21 figures are presented to the individuals, with increasing complexity as the test progresses. Each figure is presented for about 2 seconds before it disappears, and thereupon the participant has to identify the figure among five highly resembling ones. Each correct answer allows the user to continue to the next figure, until he fails to retain the visual information due to the increased complexity. In total, individuals are classified as "low", "medium", or "high" accordingly, with respect to their ability, based on a calculated aggregated score of all tests.

4.1.7 Implications of Cognitive Aspects on Adaptation and Personalization

The discussion of the aforementioned individual differences leads to our proposal concerning the implementation of adaptation and personalization systems and interfaces that can appraise human cognitive factors. A short practical overview of selected theoretical dimensions/ models is discussed next. The implications of those in the hypermedia environments can be utilized as a set of personalization parameters and adaptive mechanisms that can reconstruct and adjust any content and/or service based on the capabilities and the condition of the user.

From the perspective of learning styles and more specifically of the LSI paradigm, Kolb's 4 types are drawn from two independent scales: Concrete experience vs. abstract conceptualization, and reflective observation vs. active experimentation. People-oriented types are those that tend to concrete experience rather than abstract conceptualization, which in terms of personality theories are rather 'feeling' than 'thinking'. Therefore, as it is clearly defined by the theory, divergers' and accommodators' individual characteristics demonstrate a strong preference in group working, since collaboration may be a necessary prerequisite for maximizing learning performance. It also could

be argued that the present modus operandi of E-Learning systems in general favors types of learners that prefer working alone (convergers and assimilators), than those who are people-oriented. Implications for designers could be summarized in the equal distribution of the different types of learners, and in further motivating convergers and assimilators to participate. For example, if for any reason a group of learners consists only of these latter two types, then a Web-based educational environment's functionality may be impaired.

As described previously, Riding and Cheema (1991) identified two independent dimensions of cognitive styles, by integrating a large volume of pre-existing style research into their theory: Verbal/ Imager, and Wholist/ Analyst. The first dichotomy represents individuals' preference for receiving and processing information in either visual or verbal mode, while the second refers to a corresponding preference for information in whole or in parts; individuals without preferences are classified in each scale as intermediates. The implications of the Verbal/ Imager dimension are rather clear; the Wholist/ Analyst dimension, however, is derived from Witkin's construct of "psychological differentiation" (Witkin et al 1971; Witkin et al 1977), and its implications are somehow more complex. In a nutshell, Analysts are better at active analysis and perception differentiation, tend to act independently, are self-oriented and self-reinforced, and develop their own strategies. Wholists prefer social interaction and collaboration, while they require external direction, reinforcement, feedback, defined goals and specific structures.

More specifically, various studies revealed that the Verbal/ Imager dimension is particularly related to the content representation within hypermedia systems (Ghinea and Chen 2008). Their different characteristics and implications on hypermedia systems are the following: (i) *Verbals,* represent information verbally, focus their attention externally and are stimulating. Individuals being Verbals prefer and perform better when 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); and (ii) *Imagers* represent information in mental pictures, focus their attention internally and tend to be passive. Imagers prefer and perform better 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). On the other hand, the Wholist/ Analyst dimension is particularly related to the way hypermedia content is structured, and has an effect on users' learning patterns and navigation behavior within hypermedia systems. A recent work of Chen and Liu (2008), which investigated the effect of field dependency dimension on users' learning patterns within Web-instruction programs, revealed implications of cognitive style on users' preferred ways of using different navigation tools and display options. In particular, field independent users tended to actively group relevant concepts utilizing an alphabetical index tool of the hypermedia system, while field dependent users tended to be passive and relied on hierarchical maps to build relationships among different concepts (Chen and Liu 2008). Regarding the available display options, field independent users were capable to extract relevant information from the detailed description because they have a tendency to use their own internal

references, while field dependent users preferred to get concrete guidance from examples, since they heavily rely on external cues. Finally, field independent users browsed fewer pages to directly get to relevant topics for completing their tasks, while field dependent users tended to build an overall picture by browsing more pages because they use a global approach to process information.

Regarding more elementary cognitive processes (i.e., working memory, controlled attention, speed of processing), existing research works have shown that individual differences in such human cognitive processing abilities have an effect on problem solving and comprehension (Conway et al. 2002; Shipstead et al. 2013; Demetriou et al. 2002; Unsworth and Spillers 2010; Klingberg 2009). Thus, bearing in mind that human-computer interactions are processed on a cognitive level, such individual differences could be important for personalizing content and functionality to the needs and abilities of users. Accordingly, we consider that adaptive interactive systems can be manipulated in a way that could compensate for certain individuals' limited levels of speed of processing, control of processing and working memory, mainly by restructuring the content; presenting more explanations; additional navigation support; reducing the number of simultaneously presented stimuli and the volume of content (preventing cognitive overload); and by providing information at a slower pace, to mention but a few techniques. These methods are essentially personalization techniques that could be employed in almost every (complex enough) interactive system, though their efficiency can only be validated through empirical research.

4.2 Summary

The basic objective of this chapter was to introduce a number of dimensions of individual difference, coming from different research areas but all of which have a distinctive impact when users interact with the hypermedia information space. We have attempted to approach the theoretical considerations and create a basic understanding at first with regard to cognition and those mechanisms that influence information processing, decision making, problem solving and learning. We have analyzed core high-level cognitive factors, such as learning and cognitive styles; and more elementary cognitive processes, like human memory (working memory and long-term memory), visual attention, and speed and control of processing. According to related findings, it may be supported that interactive systems that apply adaptation and personalization techniques that consider any of these cognitive characteristics in their user model have a significant positive effect on users' interactions, assisting them, amongst others, in locating and processing information more efficiently. Our rationale behind analyzing the respective cognitive constructs derives from the fact that their impact is compatible to the structure and form of the hypermedia content. Therefore, human-centered solutions should be able to match their environments to individuals' information processing preferences, increasing users' levels of comprehension, accuracy, performance, satisfaction while at the same time minimizing cognitive overload and disorientation.

Finally, we presented methods of extraction of specific cognitive processing factors and referred to the implications that the theoretical and empirical representations can have for the design of similar applications, interactions and user interfaces. We believe that this direction could be useful to the reader at a more theoretical level that investigates human cognitive differences in information processing and at a more practical one of how their impact can be translated into designs, adaptation rules algorithms that can generate more effective and usable interactions and systems.

CHAPTER 5: Supporting Users in Security Interactions through Adaptation and Personalization: Approach and Methodology

This thesis aims to support users' task usability and improve the user experience during security-related interactions, motivated by the interdisciplinary and emerging research fields of Human-Computer Interaction and Security (HCI-SEC), Cognitive Psychology, and User Modeling, Adaptation and Personalization. In particular, this thesis attempts to revisit the definition of *"usable security"* by advocating an alternative to the *"one-size-fits-all"* approach currently utilized by predominant user authentication and CAPTCHA mechanisms. Driven by the analysis conducted throughout chapters 2-4, existing state-of-the-art research in knowledge-based user authentication and CAPTCHA mechanisms reveals that a plethora of textual and graphical mechanisms exist and that several factors (human, technology and design) affect usability of both user authentication and CAPTCHA tasks (chapter 2). Furthermore, existing theories in cognitive psychology reveal that users have different cognitive backgrounds, styles and abilities (chapter 4), while user authentication and CAPTCHA tasks are in principal processed on a cognitive level (users are required to recognize and/or recall, recall, process and comprehend verbal and graphical information). Finally, stimulated by research outcomes in the areas of User Modeling, Adaptation and Personalization (chapter 3), this work attempts to incorporate the peculiarities of human behavior and cognitive processing to the user authentication and CAPTCHA process with the aim to personalize such user interactions and provide a positive user experience and improve the user's task efficiency and effectiveness.

More specifically, the main aim of this thesis is to propose and evaluate a framework for achieving personalization on the most prominent HCI-SEC tasks related to user authentication and CAPTCHA. Human cognitive factors will play the most important role during the entire research process incorporating theories of human cognitive differences in information processing within the context of HCI-SEC. In principle, the aim is to *personalize the users' security tasks based on their individual cognitive characteristics and diversified perceptual preferences*.

Throughout this thesis we emphasize on the fact that human-centered adaptation and personalization designs and techniques should be adopted by researchers and practitioners, so to build security mechanisms that will have an added value predominantly to the benefit of the end-user. In today's multi-purpose and dynamic technological reality, the starting point for this endeavor is to define a user model that, depending on the scope and the area of application, will incorporate a number of individual characteristics under a common representation schema that will guide the whole adaptation and personalization process.

Building on this premise, this chapter initially presents a suggested mapping between the factors of a user model (consisting of a set of human factors) and security design factors identified. This user model serves as the main module of the PAC framework (detailed in chapter 6), whereas the rationale behind the selected security design factors and human-centered dimensions respectively

has its basis on the discussion in chapter 2 and chapter 4. The chapter further presents the approach and methodology followed for realizing the main objectives of this thesis. We also present a high-level adaptation and personalization architecture that resulted from the analysis made in chapter 3, and will be used as a guide to design and develop the PAC framework (chapter 6).

5.1 Identifying Human Factors for Personalizing User Authentication and CAPTCHA Tasks

One of the key technical issues in developing adaptation and personalization systems is the problem of how to construct accurate and comprehensive user models and how these can be used to identify significant intrinsic characteristics of users that describe their behavior. The way people perceive and process information is widely varied on the basis of individual differences that, from a psychological point of view, can explain the significant divergence in the information processing, learning, performance, perception, etc., between them. Henceforth, driven by existing theories in human cognitive differences in information processing (discussed in chapter 4), we suggest a mapping between a set of human factors and a set of security design factors for adapting and personalizing user authentication and CAPTCHA tasks (Figure 11).

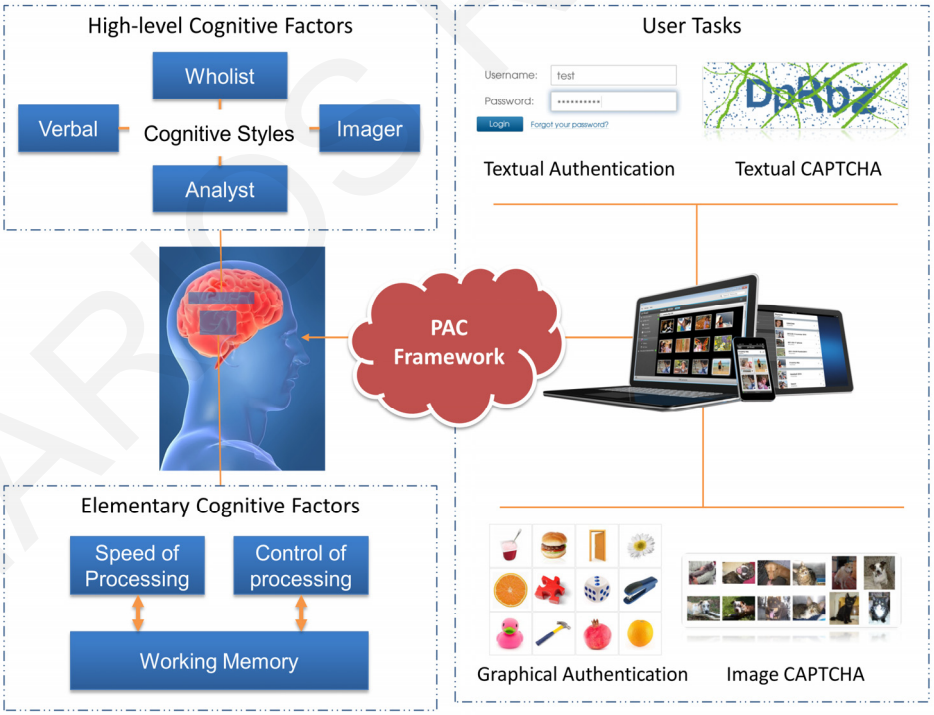


Figure 11. Human cognitive factors, user authentication and CAPTCHA tasks

The proposed user model takes into account cognitive parameters; high-level cognitive factors such as cognitive styles and more elementary factors of the human mind such as speed of processing, control of processing and working memory. The selected design factors of user authentication and CAPTCHA are primarily driven by the state-of-the-art analysis conducted on user authen-

tication and CAPTCHA (chapter 2). In particular, the analysis revealed that text-based and graphical-based mechanisms (and their variations in terms of type and complexity) are the most prominent and highly researched and applied types of design factors for authentication and CAPTCHA. Accordingly, we have selected a set of design factors (security type and complexity), since based on the theoretical analysis of human cognitive differences (chapter 4), these can be related with the selected cognitive dimensions of theories in cognitive processing styles and abilities. The user model could be considered as a vital component of the proposed personalization framework (chapter 6) since it identifies the aspects of the users that might determine their exact perceptual preferences and lead to a more concrete, accurate and optimized human-centered segmentation (or one-to-one treatment). Its main elements are overviewed below:

Cognitive Styles. Cognitive styles reflect the particular set of strengths and preferences that an individual or group of people have in how they perceive and process information; representing typical or habitual modes of problem solving, thinking, perceiving or remembering. By taking into account these preferences and defining specific cognitive, and learning strategies, empirical research has shown that more effective information processing and more efficient interactions in Web-based environments can be achieved (Boyle et al. 2003; Wang et al. 2006). In our user model, we use the construct of cognitive rather than learning style because it is more stable (Sadler-Smith and Riding 1999), and to the extent that there is a correlation with hemispherical preference and EEG measurements (Glass and Riding 1999; McKay et al. 2003), the relationship between cognitive style and actual mode of information processing is strengthened. Amongst the numerous proposed cognitive style theories and typologies (a selection of the most appropriate and technologically feasible ones – those that can be projected to the Web-based content selection and presentation, the tailoring of navigational tools, the interaction design, etc. – presented in chapter 4), we favor Riding's Cognitive Style Analysis (CSA – Riding 2001), since it can be mapped on the information space more precisely (the implications consist of distinct scales that respond to different aspects of the World Wide Web) and can be applied in most cognitive informational processing tasks (rather than strictly educational). The CSA implications are quite clear in terms of hypermedia design (visual/ verbal content presentation and wholist/ analyst pattern of navigation and interaction), and is probably one of the most inclusive theories, as it is actually derived from the common axis of a number of previous theories (Riding and Cheema 1991).

Cognitive Processing Abilities. It consists of three main parameters: (i) The *speed of processing* which refers to the maximum speed at which a given mental act may be efficiently executed; (ii) the *control of processing* which refers to the processes that identify and register goal-relevant information and block out dominant or appealing but actually irrelevant information; and (iii) the *working memory span* which refers to the processes that enable a person to hold information in an active state while integrating it with other information until the current problem is solved (see chapter 4 for a more detailed discussion around these constructs and suggestions for further reading). Since research has shown that individuals differ in cognitive processing abilities, and these

affect problem solving and information processing, we will examine whether such cognitive processing abilities have an effect in information processing of tasks such as user authentication and solving CAPTCHA challenges, and whether these can be utilized to personalize these tasks.

5.2 A High-level Adaptation and Personalization Architecture

Following the analysis made in chapter 3 that focused on existing state-of-the-art research works in user modeling, adaptation and personalization, we have designed a high-level adaptation and personalization architecture. Figure 12 illustrates a generic architecture of an adaptation and personalization system which is conceptually composed of two interconnected modules; the *user modeling* and the *personalization module*. The user modeling module entails data about its users, their interactions and the context in which communication or computation takes place. This information can be provided to the system either explicitly by the users (e.g., through registration forms, questionnaires, psychometric tests, etc.) and/or implicitly retrieved through user's interactions with the system aiming to enrich the user model and to infer information which is considered valuable in order to provide adaptive features (e.g., track how many times the user has logged in the system to extract his level of experience in the system). In this context, various data and cluster analysis techniques are performed on the raw data acquired in order to generate the actual user models which, combined with various decision making and adaptation mechanisms, decide on the adaptation effects to be performed that are further communicated to the adaptive user interface.

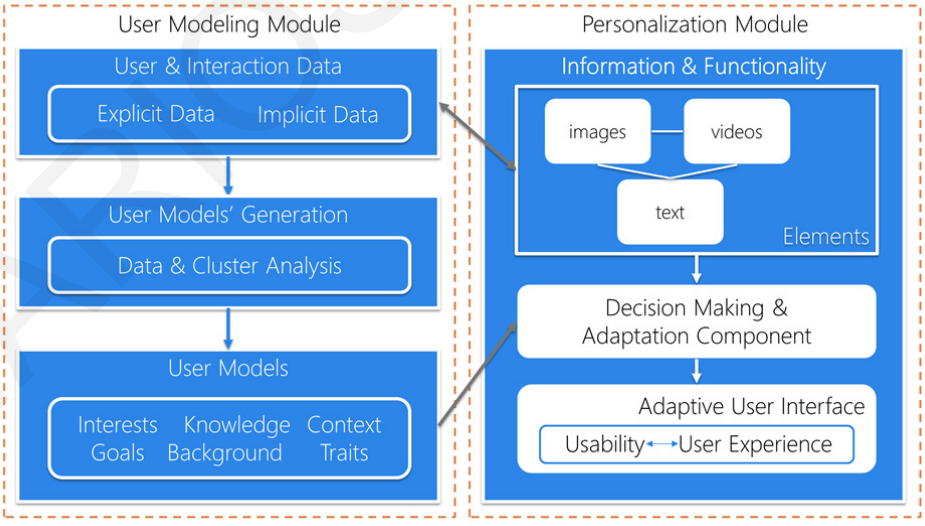


Figure 12. High-level adaptation and personalization system architecture

To this end, the high-level research goals of adaptation and personalization systems involve accurately modeling the users' characteristics for building comprehensive user models for specific

application domains, and effectively adapting content and functionality of interactive systems aiming to provide a personalized and positive user experience.

5.3 Methodology

The research work adopted a User-Centered Design (UCD) methodology throughout the entire research, design and development process. Multiple design iterations and a significant amount of evaluation were incorporated into the thesis' lifecycle, with the active participation of end-users in evaluation studies that were both *formative* (during the thesis' course, with the aim of improving the framework design) and *summative* (final framework design, with the aim of measuring the quality of the final thesis' results).

The key idea was to apply a UCD approach and to *partially move our focus away from the technical issues of security towards understanding the users and developing new approaches for offering solutions based on users' cognitive factors*. The Ph.D. work adopted a three-phase methodological approach to fulfill the main objectives as illustrated in Figure 13.

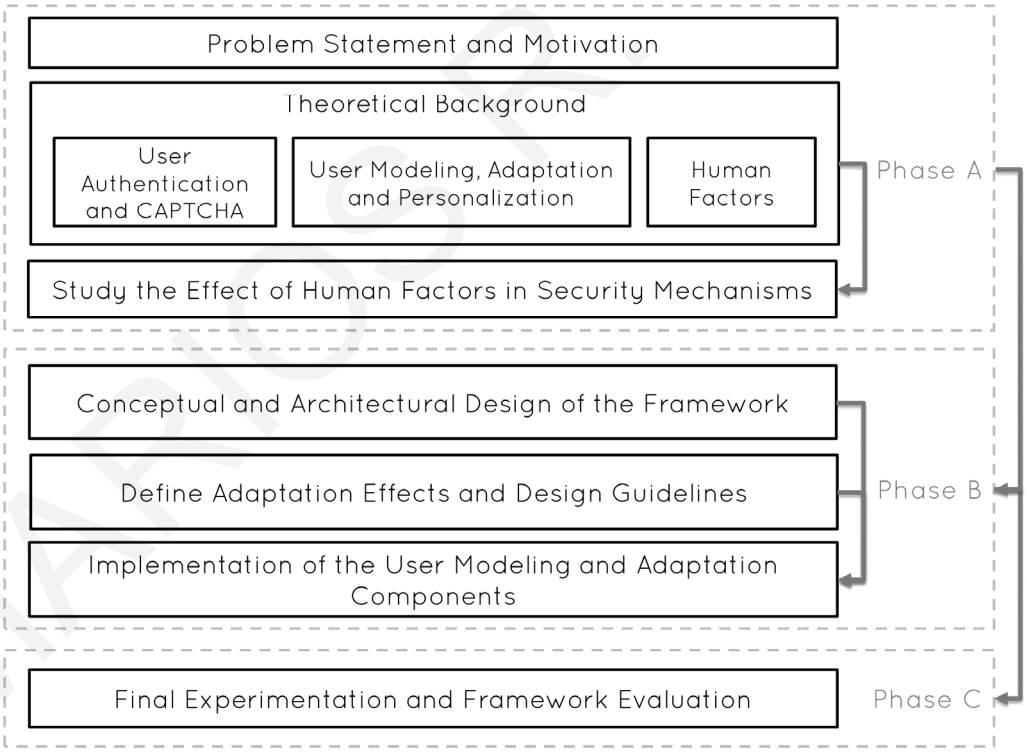


Figure 13. Phases of research work

5.3.1 Phase A: Investigate the Main Research Areas and Study the Effect of Human Cognitive Factors with regards to User Authentication and CAPTCHA (Objective 1)

As presented in the aforementioned sections, emphasis has been given on high-level cognitive factors of the human mind, such as, *cognitive styles* were investigated that suggest individuals have differences in the way they process and remember information and primarily affect preference and performance in hypermedia systems. In addition, emphasis has been given to elementary perceptual and cognitive factors of the human mind, such as, *speed of processing*, *control of processing* and *working memory*.

High-level Cognitive Factors of Individuals: High-level cognitive factors, such as *cognitive styles* were elicited through valid psychometric tests that measure response times of participants on specific aptitude tasks (Riding and Cheema 1991), as well as an attempt to implicitly elicit the users' cognitive styles based on their navigation behavior. Depending on the response time of each answer, the ratio of means or medians between different cognitive stimuli were computed and further used to classify the participant to a particular cognitive style group. Two broad style dimensions were utilized in our research which have shown a main effect on users' preference and performance in hypermedia systems: (i) The Verbal/ Imager dimension which refers to how individuals process information and indicates their preference for representing information verbally (Verbals) or in mental pictures (Imagers); and (ii) the Wholist/ Analyst dimension which refers to how individuals organize information and indicates a preference of structuring information as a whole to get the big picture (Wholists) or structuring the information in detail (Analysts).

Elementary Cognitive Factors of Individuals: In the same line with cognitive styles, a series of psychometric instruments were utilized to highlight differences of users in cognitive processing abilities targeting on speed of processing, control of processing and working memory. *Speed of processing* refers to the maximum speed at which a given mental act may be efficiently executed (MacLeod 1991; Posner 1997). *Control of processing* refers to cognitive processes that can identify and concentrate on goal-relevant information and inhibit attention to irrelevant stimuli (Posner 1997; Stroop 1935). *Working memory* capacity is defined as the maximum amount of information that the mind can efficiently activate during information processing which is considered essential for performing cognitive tasks (Baddeley 2012; 1992). In order to elicit the cognitive processing abilities of individuals, the response times for recognizing and processing a number of stimuli were measured utilizing valid psychometric instruments.

Perform User Studies: Several standalone and targeted user studies were conducted throughout the thesis, which investigated various and different human cognitive processing factors, aiming to understand and identify which individual characteristics are considered important enough and might affect users' interactions in user authentication and CAPTCHA mechanisms. These studies aimed to guide and contribute to the design of personalized user authentication and CAPTCHA mechanisms that take into consideration such intrinsic human factors.

5.3.2 Phase B: Design and Develop a Multilayer Personalization Framework (Objective 2)

This phase focused on the elaboration and design of a multilayer personalization framework that performs explicit and implicit user modeling and adaptation mechanisms that consist of intelligent processes and techniques for the elicitation of the user's cognitive factors in which computation takes place. The work that was performed within this phase provided the specifications and therefore laid the foundations and guided the implementation of the framework.

Conceptual Design of the Framework: This action focused on gathering the requirements and core research development based on the work conducted in Phase A. It focused on creating a generic formalization of a human factor-based user model (including cognitive styles, speed of processing, control of processing, working memory capacity) for personalizing security-related tasks, as well as a formalization of an adaptation engine for recommending a particular user authentication and CAPTCHA type and complexity level based on the combination of the user modeling factors.

Architectural Design of the Framework: The outcome of this sub-phase provided valuable input for setting the specifications of the proposed personalization framework. In particular, it set the specifications of the user model focusing on: (i) How to represent the selected human factors; and (ii) how to extract and maintain these factors in the user model. This sub-phase also set the specifications of the security and adaptation mechanisms of the user interface. The outcome of this phase was further utilized for the design and development of the framework.

Define Adaptation Effects and Design Guidelines: Based on the outcome of the user studies conducted in Phase A, we have interpreted and translated the observed main effects into adaptation rules in order to map human cognitive factors with design factors of user authentication and CAPTCHA mechanisms. Accordingly, this action delivered innovative guidelines on how current practice can be enriched with adaptation and personalization techniques incorporating users' cognitive characteristics as the core filtering parameters for adaptation purposes.

Implementation of the User Modeling and Adaptation Components: Given the theoretical analysis and decisions made in previous phases all the components were designed under a common framework. These components incorporated user modelling and adaptation mechanisms that personalize security-related tasks according to the users' cognitive factors. Emphasis was given to the interoperability of the system's components and to ensure the maximization of the efficiency and effectiveness of the system running on different platforms.

5.3.3 Phase C: Final Experimentation and Framework Evaluation (Objective 3)

This phase aimed to validate the proposed framework through an ecological valid user study aiming to examine the added value of the framework in terms of user performance with relation to user

authentication and CAPTCHA challenges. In particular, this action used the methods and software developed to carry out a final user study. Main aim was to evaluate the proposed adaptation effects and design guidelines in order to discover if there is any deviation from the specifications drawn from Phase A. Furthermore, the study provided empirical evidence about the feasibility and added value of adapting security-related tasks taking into consideration users' individual differences. The final validated set of guidelines can be used from designers of corresponding applications, since the cognitive user model and the experimental results have been academically published.

5.4 Summary

In this chapter we made an effort to propose the methodological approach of this doctoral thesis that lead us to the design and development of a proposed personalization approach in security-related interactions, with the aim to improve the usability of such interactive systems and provide positive user experiences while interacting with them.

In this context, a number of research questions have been tackled such as:

- Do cognitive styles and cognitive processing factors of users have a main effect on users' preference and task performance of different designs of security mechanisms? Specifically, are there any significant differences with regard to time (efficiency) and total number of attempts (effectiveness) needed to complete the task of a different design type and complexity of security mechanisms among users having differences in cognitive styles and processing?
- Does the provision of a particular combination of security type and complexity level to users' cognitive styles and processing factors has a significant effect on their performance?
- How to extract the cognitive processing characteristics through explicit and implicit user data collection methods?
- How to design and develop a multi-layer framework specializing on personalizing security tasks?

In order to elucidate the abovementioned issues, throughout this work we conducted a number of user studies to investigate main effects of cognitive characteristics of users on preference and performance of security mechanisms, in parallel with the development of the framework. Our efforts were focused on "translating" a theoretical framework into adaptation rules. The mapping of such user characteristics into usable security mechanisms may be a complex and challenging process, primarily due to the unforeseen interactions of human traits. Nevertheless, this is the main challenge of our research work; *successfully integrating theory into practice in a coherent way*.

CHAPTER 6: Personalized Authentication and CAPTCHA – The PAC Framework

The idea of developing adaptation and personalization systems (also referred as adaptive interactive systems) has been mainly supported by arguments focusing on the drawbacks of the "one-size-fits-all" approach (Brusilovsky and Maybury 2002) and essentially the complexity and vagueness of the ever-expanding World Wide Web (De Bra et al. 2004). In parallel, researchers and practitioners in the field of user modeling, adaptation and personalization underline the heterogeneity of the user population, while it is often implied that "static", non-personalized systems fail to satisfy the needs and support the goals of different users (Brusilovsky 2001).

In this realm, since the early days of the World Wide Web, many research works have proposed a number of personalization strategies with the aim to alleviate "one-size-fits-all" issues in interactive systems (Goy et al. 2007; Brusilovsky and Millán 2007). Various factors for personalization have been suggested over time, among others, users' interests, preferences, needs and goals (user information), users' device screen sizes and input types (device information), and users' physical and social factors (contextual information – Goy et al. 2007; Brusilovsky and Millán 2007). In this line, several techniques for modeling such factors were introduced, either based on explicit (e.g., questionnaires) or implicit user data collection methods (e.g., according to users' navigation behavior within the system (Frias-Martinez et al., 2005), or based on collaborative filtering techniques (Linden et al. 2003; Karat et al. 2004).

However, a rather obvious question is still in the center of attention: Is it worth to develop extensive personalized services, considering that their technical complexity and requirements far surpass those of static systems (Tsianos et al. 2013)? During the incubation period of adaptive hypermedia, Dieterich et al. (1993) and Brusilovsky (1996) identified certain criteria in order to analyze and document the usefulness of adopting a personalized approach (Figure 14): (i) The area of application; (ii) the goals of the personalized approach; (iii) the target user group; (iv) the characteristics of the users to be taken into account; (v) when should the adaptation process be initiated; (vi) the aspects of the system that can be manipulated and adapted; and finally on a technical level (vii) what techniques should be used for user modeling and adaptation. E-Learning, for instance, qualifies rather easily according to these criteria, since it is a very wide area, the learner population is much diversified (with different goals, needs, and abilities), while the educational content and the instructional methods are highly directive and controllable and can be comparably easily manipulated. However, even in this case, the high cost of designing personalized courses for popular and free to use E-Learning platforms has resulted in a poor exploitation of this kind of solutions outside the research community (Hauger and Köck 2007). Also, Paramythis and Loidl-Reisinger (2004) stress that in many cases adaptive educational hypermedia are not standard compliant. Therefore, the move towards personalized Web applications and services is not expected to be an easy one, especially without the support of high profile service providers.

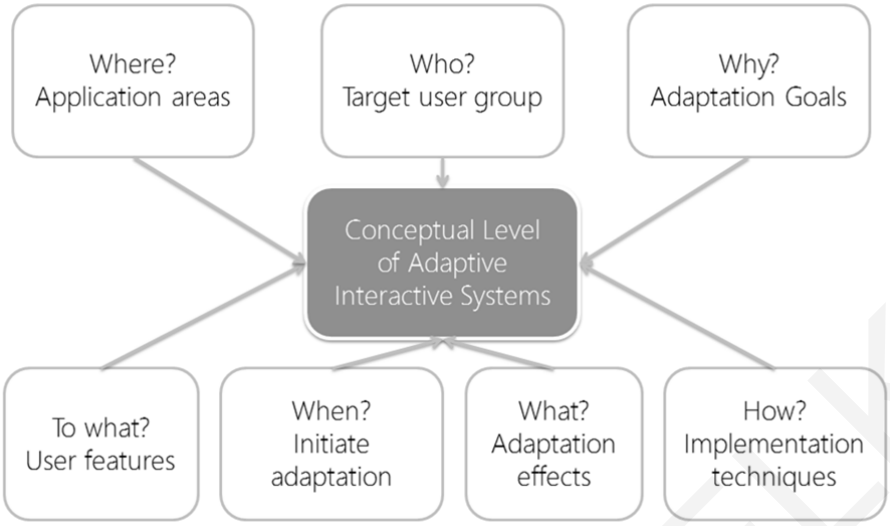


Figure 14. A conceptual frame of reference framework for developing and adaptation and personalization systems

But, even if this is the case, and in the end personalization is the key to more efficient interactions and a satisfying experience for the users, still one undeniable issue is, how and why would users benefit? Additional research should focus even more on measuring the actual benefit for the end-users and their unique characteristics, instead of merely developing advanced personalization and user modeling techniques. Individuals are certainly different from each other, but which would be the underlying theories that could guide research endeavors in producing measurable gains? A first approach would be to identify the levels in which individuals demonstrate a considerable divergence, such as demographics, social, mental abilities, personality, goals, needs, and experience, and to build a cohesive user model by including characteristics that could be proven of importance in affecting behavior and performance. Probably, this could be achieved only by conducting extensive empirical work, driven by grounded psychological and sociological theories, and by gradually developing an interdisciplinary framework that would bridge technical possibilities with human factors.

In this context, we introduce the notion of individual differences as a core element of adaptation and personalization, focusing mainly on users' cognitive characteristics. In particular, human-computer interactions within user authentication and CAPTCHA are in principal tasks that embrace perception, recognition, recalling and reasoning. Taken into consideration the diversity of humans in cognitive processing styles and abilities as seen in chapter 4 (Riding and Cheema 1991; Kozhevnikov 2007; Demetriou et al. 2013), adapting and personalizing content and functionality of such interactive systems, bootstrapped on the users' cognitive processing characteristics, could provide a promising alternative to current state-of-the-art practices, aiming to support the users' efficiency and effectiveness of processing information as well as decrease cognitive load, and eventually improve the user experience.

The basis of such an approach lies in an initial understanding of how such intrinsic human factors affect user interactions in specific domains and contexts of use and investigate the feasibility and efficacy of incorporating them in the user model and accordingly adapt the content and functionality of the system. In particular, the first steps of any similar approach is to initially design and conduct several standalone and targeted user studies that investigate various and different human factors, aiming to recognize and identify which individual characteristics are considered important enough and might affect users' interactions in various application domains. Consequently, depending on the findings of each study, the next step is to interpret and translate the observed main effects into adaptation rules in order to map human factors with design factors of interactive systems. These adaptation rules are further realized and incorporated in an interactive system.

In this respect, based on the theoretical analysis on human factors in chapter 4 and several targeted user studies that were conducted aiming to understand the impact of human factors on specific design characteristics of user authentication and CAPTCHA (chapter 7), we have formalized the main effects and interactions into adaptation rules that unfold this mapping relationship (chapter 8). We have further incorporated those under an extensible personalization framework, namely PAC (Personalized Authentication and CAPTCHA) that is reported in this chapter. The chapter is organized as follows: We first present the PAC framework and its main modules for personalizing content and functionality of interactive systems based on specific human factors. Next, following the conceptual design and formalization of the framework, we detail the design and development of a real-life Web-based adaptive interactive system with all the necessary technologies and components. Throughout this chapter we place special emphasis on the user modeling and personalization modules by presenting a formalization of a human factor-based user model (including cognitive styles, speed of processing, control of processing, working memory capacity), a formalization of an adaptation engine and a set of adaptation rules for personalizing specific design characteristics of user authentication and CAPTCHA mechanisms.

6.1 Conceptual Design of PAC

Following the technical and design considerations of adaptation and personalization systems (chapter 3), we have designed at a conceptual level, an extensible human-centered personalization framework, namely PAC for adapting and personalizing user authentication and CAPTCHA tasks. The framework was designed in a way to incorporate modules and components that are essential for the whole personalization process. In particular it includes: (a) Explicit and implicit data collection methods, for eliciting the users cognitive characteristics (and consequently composing the user model); (b) management tools, for managing various entities of the framework (e.g., user models); and (c) an adaptation engine, for mapping specific human factors of the user models with design characteristics of user authentication and CAPTCHA.

Following the aforementioned conceptual frame of reference and the high-level system architecture (presented in chapter 5), we have designed PAC to include two main modules, the *User Modeling module* and the *Personalization module*. The *User Modeling module* is responsible to collect and process information about the users aiming to elicit their cognitive characteristics and the *Personalization module* is responsible to personalize the user's task by following particular adaptation rules for achieving the appropriate mapping with selected design characteristics. Figure 15 depicts the conceptual design of PAC. We next describe the formalization of the user modeling and personalization modules.

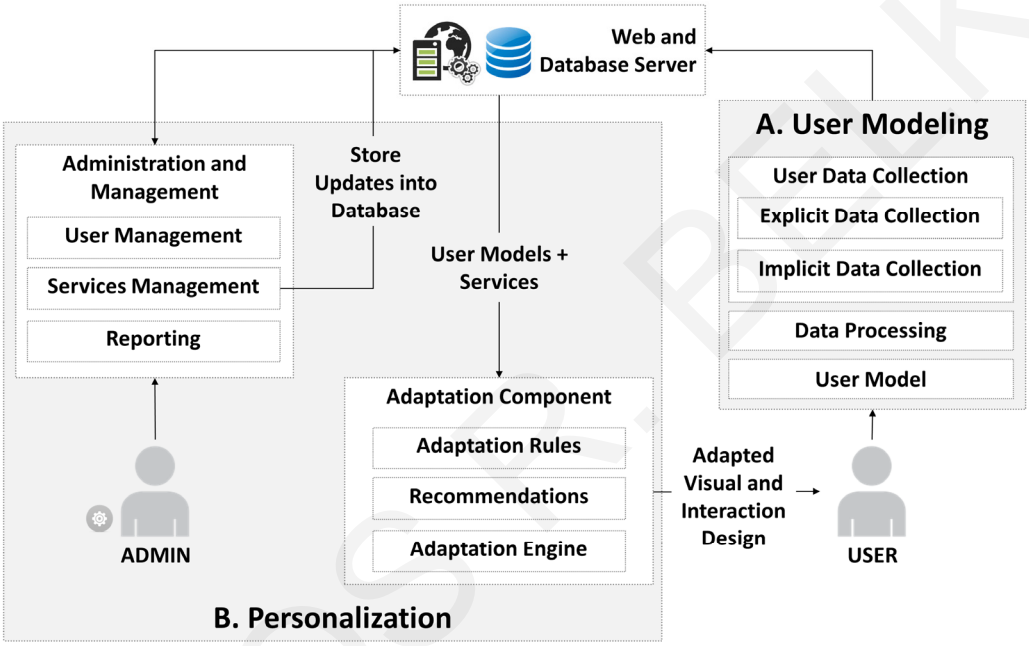


Figure 15. Conceptual design of the PAC framework

6.1.1 Module 1 - User Modeling

The user modeling module is responsible to generate the user models of the framework which are necessary for the adaptation behavior of an interactive system. In our case, two cognitive factors are used, *cognitive styles* and *cognitive processing abilities* for modeling the users' individual differences. The module supports the management and maintainability of user data collected, enabling the administration and extension of methods and factors of the user model. Explicit and implicit user data collection methods are used for eliciting the user models' characteristics. Explicit user data collection methods include accredited and standardized psychometric tests in which users are required to respond to a series of cognitive aptitude tasks. Depending on the users' responses (accuracy and speed), algorithms are applied for highlighting their cognitive processing characteristics. In particular, the users' Verbal/ Imager and Wholist/ Analyst cognitive styles are elicited by exploiting two tests of Riding's Cognitive Style Analysis (CSA – Riding 1991; Riding and Cheema

1991) since it is based on a strong theoretical justification and is a widely applied psychometric test for eliciting cognitive styles of users (Rezaei and Katz 2004). The users' cognitive processing abilities are elicited by exploiting two Stroop-like tests for extracting the users' speed of processing and control of processing; and two working memory capacity tests as utilized in Demetriou et al. (2013).

Given that explicit user data collection methods (e.g., psychometric tests, questionnaires) may decrease the user acceptance of such a personalization approach, we also attempted initially to design several Web interaction metrics for inferring the cognitive styles of users through their interactions with specific divisions in an interactive system. In the next sections we describe both explicit and implicit user data collection methods under a unified formalization.

Cognitive Aptitude Tasks

This section describes the cognitive tasks of each psychometric test; Verbal/ Imager cognitive style, Wholist/ Analyst cognitive style, speed of processing, control of processing, visual working memory and verbal working memory.

Verbal/ Imager Cognitive Styles' Task. The Verbal/ Imager CSA test 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., color) 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 color of two objects (e.g., *"Are cream and paper the same color?"*). It is assumed that Verbals respond faster than Imagers in the conceptual types of stimuli (verbal-type) 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 (imager-type) 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).

Wholist/ Analyst Cognitive Styles' Task. The Wholist/ Analyst CSA test indicates an individual's tendency to process information as a whole or analytically. An individual's style on the Wholist-Analyst dimension is obtained by presenting a series of 40 questions on judging and comparing geometrical figures made up of three basic geometric shapes (i.e., square, rectangle, and triangle). 20 of these questions include wholist-type stimuli that require the users to compare whether a pair of figures are identical or not (e.g., *"Is shape X the same as shape Y?"*). As this task involves judgments about the overall similarity of the two figures, it is assumed that Wholists will respond faster than Analysts (Riding 1991).

The remaining 20 questions include analytic-type stimuli that require the users to judge whether a single figure is part of another complex figure (e.g., *"Is shape X contained in shape Y?"* – see

Figure 16). This task requires the users to dis-embed the simple shape from within the complex geometrical figure in order to establish that it is the same as the stimulus shape displayed. It is assumed that Analysts will respond faster in this task (Riding 1991).

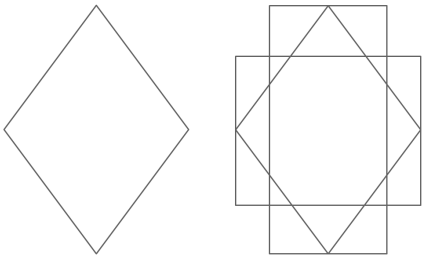


Figure 16. Example of an analyst-type stimulus (Riding 1991).

In this example, users are required to respond with true/ false on whether the left simple figure is embedded within the right complex figure. It is assumed that Analyst users will solve this challenge faster than Wholists

Speed of Processing and Control of Processing Task. Two Stroop-like tasks are devised to measure reaction time to address speed of processing and control of processing. For measuring speed of processing, users are required to read a number of words denoting a color written in the same or different ink color (e.g., the word “Red” illustrated in red ink color). For measuring control of processing, similarly, a Stroop-like task is devised, but instead of denoting the written word itself, users are required to recognize the ink color of words denoting a color different than the ink (e.g., the word "Red" illustrated in green ink as illustrated in Figure 17). In each test, a total of 18 words are illustrated to the users illustrating the words "Red", "Green" or "Blue" either written in red, green or blue ink color. The users are required to press the R keyboard key for "Red", the G key for "Green" and the B key for "Blue".

Red

Figure 17. A Stroop-like task.

The user is required to recognize the ink color of the word (green) which denotes a color different than the ink (“Red”)

Users' Visual Working Memory Capacity Task. This test illustrates a geometric figure on the screen and the user is required to memorize the figure. Thereafter, the figure disappears and 5 similar figures are illustrated on the screen, numbered from 1 to 5 (Figure 18).

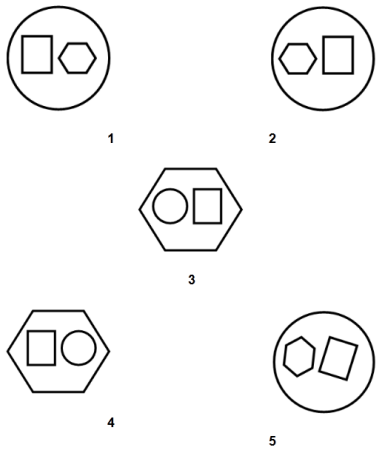


Figure 18. Visual working memory task (Demetriou et al. 2013)

The user is required to provide the number (using the keyboard) of the corresponding figure that was the same as the initial figure. The test consists of 21 figures (seven levels of three trials each). As the user correctly identifies the figures of each trial, the test provides more complex figures as the levels increase indicating an enhanced visual working memory capacity.

Users' Verbal Working Memory Capacity Task. This test illustrates a series of statements and users are required to respond whether they are true or false. In addition, users are required to remember the last word of each sentence and then write the last word of the sentence. The test includes six levels of difficulty, e.g., in level three, users are required to respond true or false on three successive sentences and have to remember and provide the last word of each sentence. For example, for the sentences *"Knives are sharp"*, *"The sun is shining"*, and *"Fish have fur"* the user should respectively respond *true*, *true* and *false*, and then provide the word *"sharp"*, *"shining"* and *"fur"* to the system (Figure 19). The level each user reaches indicates his verbal working memory capacity.

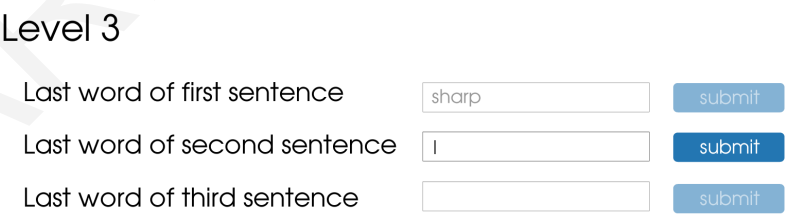


Figure 19. Verbal working memory task (Demetriou et al. 2013)

Web Interaction Metrics

The reasoning behind the design of the Web interaction metrics was based on the assumption that cognitive styles may correspond ideally to the structure of Web environments (Germanakos et al. 2009; Tsianos et al. 2013); the content is essentially either visual or verbal and the manipulation of

hyperlinks can lead to a more analytic and segmented structure, or to a more holistic and cohesive environment (Germanakos et al. 2009; Tsianos et al. 2013). Thus, differences in cognition are likely to be reflected in users' interactions and navigation with a system. In this respect we reproduced a Web application based on Wikipedia (2015) including additional functionality and content representations. The application monitors the Web interaction of users on the client-side utilizing a browser-based logging facility to collect the interaction usage data from the hosts accessing the Web application. The following Web interaction data are monitored: (i) Total view time of articles representing content either verbally or graphically; and (ii) the hyperlink interactions. These are described next.

Monitoring Users' Content Representation Preference. Given that the Verbal/ Imager dimension has implications on the content representation (verbal or visual) of Web environments, we monitored the users' preference towards content representation, by enriching the Web application to include both verbal-based content, i.e., content in textual form without images/ visuals (Figure 20A), and image-based content, i.e., content represented with images/ visuals and diagrammatical representations of text (Figure 20B). The users have the option to either view the article in its textual version or in its graphical version. The total time spent in each version (viewing time) is recorded during the user's interaction with the system aiming to extract information about their preference towards a particular type of content representation.

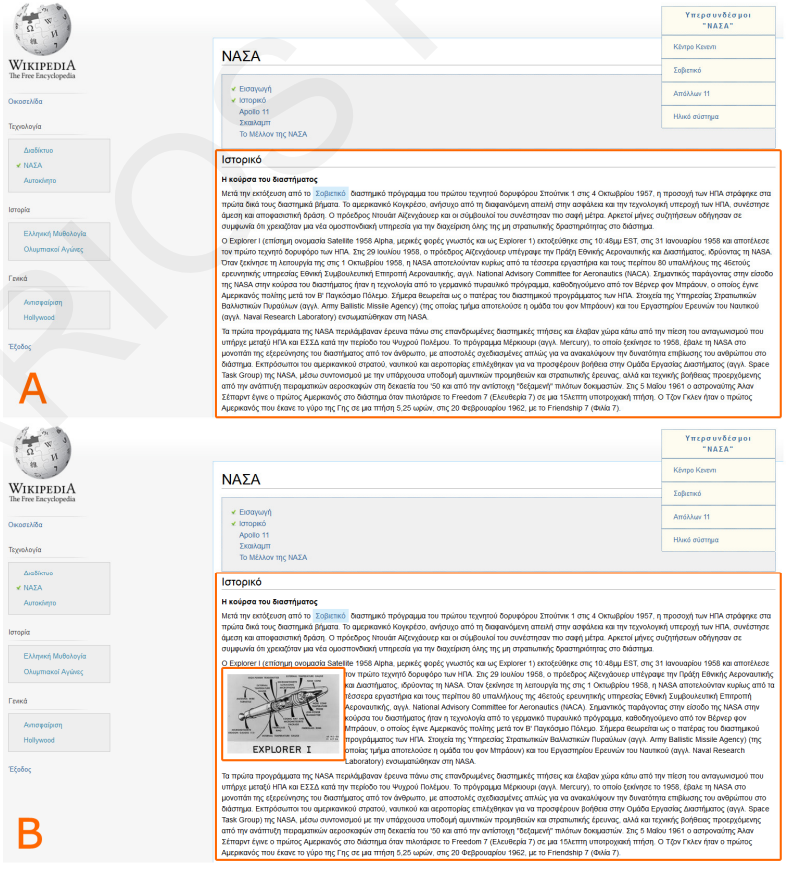


Figure 20. Verbal- and image-based user interface of the Web-site (based on Wikipedia (2015))

Monitoring Users' Hyperlink Navigation Paths. For implicitly eliciting the Wholist/ Analyst cognitive styles of users, we monitor the users' actual sequences with the hyperlinks of the Web application and accordingly calculate their linearity, i.e., whether a user navigates linearly from one link to the other or in a non-linear manner. For this purpose, as mentioned earlier, we have developed an exact replica of Wikipedia since it is considered a representative example in terms of content structure and hyperlinks that enabled us to track the navigation behavior of users. In particular, given that the structure of Wikipedia articles contains hyperlink anchors that point to specific sections within each article, we measure the actual sequence of visited hyperlinks and the linearity of user interactions with the hyperlinks within each article. Two types of interactions (Figure 21) are considered for monitoring the users' interactions: (i) *Navigation Menu Interactions:* The interactions of users with a navigation menu of each article in which every hyperlink is connected with a particular section in the article; and (ii) *Content Link Interactions:* The interactions of users with hyperlinks within the article that are connected with another article in the system. The reasoning behind this choice is based on the fact that the information behind each hyperlink has close semantic relationship with its previous hyperlink. Accordingly, the usage of the hyperlinks of each interaction type can be used to measure the degree of linear behavior a user has within the Web environment, i.e., whether the user tends to visit successive hyperlinks or not.

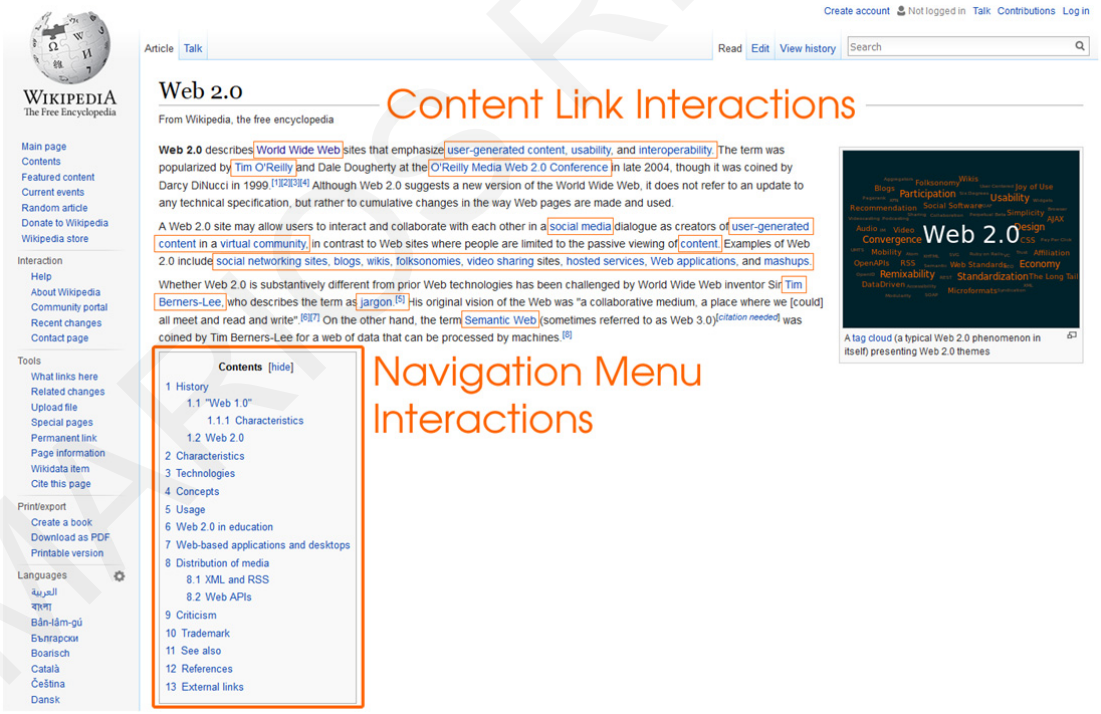


Figure 21. Types of user interactions (based on Wikipedia (2015))

We designed a Web navigation metric that calculates the degree of linearity the users follow (linear or non-linear). In this context, in order to represent the users' interactions, all hyperlinks within each article were automatically annotated with an attribute, meaningful to the system. In particular, the hyperlinks of a given HTML document were annotated with a unique incremental

identifier, in the following format: *nav_n_m*, in which *n* identifies the article in which the user currently navigates and *m* the hyperlink clicked. Each time a user clicks on the annotated hyperlink, the unique identifier, as well as the time of hit is sent to the Web server. For example, for article with *ID*=1 consisting of 4 hyperlinks, the following identifiers are assigned to each hyperlink from top to bottom: *nav_1_1*, *nav_1_2*, *nav_1_3*, *nav_1_4*.

Data Processing

For each stimulus of the aforementioned tasks (e.g., verbal-type or imager-type stimulus), the response time and the provided answer are recorded and processed. In this section, we formalize the user modeling data process. The main symbols and their respective definitions are summarized in Table 3. Accordingly, let U denote a set of users $\{u_1, u_2, \dots, u_n\}$. Let $q_j^{cs}(u_i)$ denote a question j that is part of a psychometric test for a specific stimulus cs and is performed on user u_i. The result of $q_j^{cs}(u_i)$ is a quintuplet of the form (cs, j, u_i, val, t), where cs is the stimulus, j is the question number, u_i is the user, val is the answer ($true$ or $false$) to the question and t is the response time ($0 < t \leq timeout$) for some predefined timeout period (e.g., 3 seconds). In this work, the stimulus cs can be v (i.e., verbal), g (i.e., imager), w (i.e., wholist), a (i.e., analyst), s (i.e., speed of processing), c (i.e., control of processing), ma (i.e., visual working memory) or mb (i.e., verbal working memory). Additionally, let the set of all correct questions (i.e., $val = true$) for user u_i for a specific stimulus cs be denoted as $Q^{cs}(u_i) = \{q_j^{cs}(u_i) : q.val = true, \forall j\}$.

Table 3. Table of symbols

Symbol	Description
U	Set of user $\{u_1, u_2, \dots, u_n\}$
cs	Set of stimuli $\{v, g, w, a, s, c, ma, mb\}$
t	Response time to answer a question
val	Answer of a question ($true$ or $false$)
$q_j^{cs}(u_i)$	Set of answered questions $\{q_1, q_2, \dots, q_n\}$ for user u_i of a particular stimulus cs
$Q^{cs}(u_i)$	Set of all correct questions for user u_i of a particular stimulus cs
$cr^{cs}(u_i)$	Number of correct responses of a specific stimulus cs for user u_i
CR^{cs}	Average correct responses for a psychometric test of a specific stimulus cs for all users
DCR^{cs}	Standard deviation of correct responses for a psychometric test of a specific stimulus cs for all users
$rt^{cs}(u_i)$	Average response time for a psychometric test of a specific stimulus cs for user u_i

Symbol	Description
U	Set of user $\{u_1, u_2, \dots, u_n\}$
cs	Set of stimuli $\{v, g, w, a, s, c, ma, mb\}$
t	Response time to answer a question
val	Answer of a question ($true$ or $false$)
$q_j^{cs}(u_i)$	Set of answered questions $\{q_1, q_2, \dots, q_n\}$ for user u_i of a particular stimulus cs
RT^{cs}	Average response time for a psychometric test of a specific stimulus cs for all users
DRT^{cs}	Standard deviation of response time for a psychometric test of a specific stimulus cs for all users
$\lambda^{v:g}(u_i)$	Verbal/ Imager ratio for user u_i
$\lambda^{w:a}(u_i)$	Wholist/ Analyst ratio for user u_i
$\mu^{sc}(u_i)$	Average response time of stimulus s and c for user u_i
$z^{cs}(u_i)$	Normalized z-score value of the average response time of stimulus cs for user u_i
$z^{ma}(u_i)$	Normalized z-score value of the number of correct responses of stimulus cs for user u_i
$\mu^{mab}(u_i)$	Average of normalized correct responses of stimulus ma and mb for user u_i
$cpa(u_i)$	Cognitive processing ability of user u_i based on $z^s(u_i)$, $z^c(u_i)$, $z^{ma}(u_i)$ and $z^{mb}(u_i)$
$vt^t(u_i)$	Viewing time in article sections illustrating textual information for user u_i
$vt^g(u_i)$	Viewing time in article sections illustrating graphical information for user u_i
$\lambda^{vt:vg}(u_i)$	Ratio of preferred viewing version for user u_i
$nav^{adl}(u_i$	The total absolute distance of links for user u_i

We define the number of correct responses of a specific stimulus cs for user u_i to be:

$$cr^{cs}(u_i) = |Q^{cs}(u_i)|$$

We define the average number of correct responses (CR) for a psychometric test of a specific stimulus cs for all users to be:

$$CR^{cs} = \frac{\sum_{\forall u_i} cr^{cs}(u_i)}{|\{u_i : cr^{cs}(u_i) \geq 0\}|}$$

We define the standard deviation of correct responses (DCR^{cs}) for a psychometric test of a specific stimulus cs for all users to be:

$$DCR^{cs} = \sqrt{\frac{(\sum_{\forall u_i} cr^{cs}(u_i) - CR^{cs})^2}{(|\{u_i : cr^{cs}(u_i) \geq 0\}| - 1)}}$$

We define the average response time (rt) for a psychometric test of a specific stimulus cs for user u_i to be:

$$rt^{cs}(u_i) = \frac{\sum_{\forall q_j^{cs}(u_i) \epsilon Q^{cs}(u_i)} q_j^{cs}.t}{cr^{cs}(u_i)}$$

We define the average response time (RT) for a psychometric test of a specific stimulus cs for all users to be:

$$RT^{cs} = \frac{\sum_{\forall u_i} rt^{cs}(u_i)}{|\{u_i : rt^{cs}(u_i) > 0\}|}$$

We define the standard deviation of response time (DRT^{cs}) for a psychometric test of a specific stimulus cs for all users to be:

$$DRT^{cs} = \sqrt{\frac{(\sum_{\forall u_i} rt^{cs}(u_i) - RT^{cs})^2}{(|\{u_i : rt^{cs}(u_i) \geq 0\}| - 1)}}$$

We define the Verbal/ Imager Ratio $\lambda^{v:g}$ for user u_i to be:

$$\lambda^{v:g}(u_i) = \begin{cases} \frac{RT^v}{RT^g} & rt^v(u_i) = 0, rt^g(u_i) = 0 \\ \frac{RT^v}{rt^g(u_i)} & rt^v(u_i) = 0 \\ \frac{rt^v(u_i)}{RT^g} & rt^g(u_i) = 0 \\ \frac{rt^v(u_i)}{rt^g(u_i)} & \text{otherwise} \end{cases}$$

We define the Wholist/ Analyst Ratio $\lambda^{w:a}$ for user u_i to be:

$$\lambda^{w:a}(u_i) = \begin{cases} \frac{RT^w}{RT^a} & rt^w(u_i) = 0, rt^a(u_i) = 0 \\ \frac{RT^w}{rt^a(u_i)} & rt^w(u_i) = 0 \\ \frac{rt^w(u_i)}{RT^a} & rt^a(u_i) = 0 \\ \frac{rt^w(u_i)}{rt^a(u_i)} & \text{otherwise} \end{cases}$$

The cognitive style ratios ($\lambda^{v:g}(u_i)$ and $\lambda^{w:a}(u_i)$) indicate the users' cognitive style on the scales of Verbal-Imager and Wholist-Analyst. Users with a low value of $\lambda^{v:g}$ are considered to respond faster to the verbal types of stimuli, whereas users with a high value of $\lambda^{v:g}$ are considered to respond faster to the imager types of stimuli. Similarly, users with a low value of $\lambda^{w:a}$ are considered to respond faster to the wholist types of stimuli, whereas users with a high value of $\lambda^{w:a}$ are considered to respond faster to the analyst types of stimuli. The cognitive style ratios of each user are then provided as input for cluster analysis aiming to classify each user to a cognitive style group.

Next we define the cognitive processing efficiency of user u_i as the average response time of stimulus s and c for user u_i to be:

$$\mu^{sc}(u_i) = \frac{\left(rt^s(u_i) + rt^c(u_i)\right)}{2}$$

We define the normalized value (by z-score) of the average response time of stimulus s for user u_i to be:

$$z^s(u_i) = \frac{(rt^s(u_i) - RT^s)}{DRT^s}$$

We define the normalized value (by z-score) of the average response time of stimulus c for user u_i to be:

$$z^c(u_i) = \frac{(rt^c(u_i) - RT^c)}{DRT^c}$$

We define the normalized value (by z-score) of the number of correct responses of stimulus ma for user u_i to be:

$$z^{ma}(u_i) = \frac{(-1) * (cr^{ma}(u_i) - CR^{ma})}{DCR^{ma}}$$

We define the normalized value (by z-score) of the number of correct responses of stimulus mb for user u_i to be:

$$z^{mb}(u_i) = \frac{(-1) * \left(cr^{mb}(u_i) - CR^{mb}\right)}{DCR^{mb}}$$

We define the working memory of user u_i as the average of normalized number of correct responses of stimulus ma and mb for user u_i to be:

$$\mu^{mab}(u_i) = \frac{\left(z^{ma}(u_i) + z^{mb}(u_i)\right)}{2}$$

The average response time of stimulus s and c ($\mu^{sc}(u_i)$) indicates a user's cognitive processing speed with a low value of μ^{sc} indicating an enhanced cognitive processing speed of that user, and a high value of μ^{sc} indicating a limited cognitive processing speed of that user. The average of normalized number of correct responses of stimulus ma and mb ($\mu^{mab}(u_i)$) indicates a user's working memory capacity with a low value of μ^{mab} indicating a limited working memory capacity of that user, and a high value of μ^{mab} indicating an enhanced working memory capacity of that user.

We further define the cognitive processing ability of user u_i as the average of normalized values of stimulus s, c, ma and mb for user u_i to be:

$$cpa(u_i) = \frac{\left(z^s(u_i) + z^c(u_i) + z^{ma}(u_i) + z^{mb}(u_i)\right)}{4}$$

Finally, we define the users' preferred viewing version as the ratio between the total viewing time of the textual version $vt^t(u_i)$ and the total viewing time of the graphical version $vt^g(u_i)$ for user u_i to be:

$$\lambda^{vt:vg}(u_i) = \frac{vt^t(u_i)}{vt^g(u_i)}$$

The linearity of users' navigation is modeled through the absolute distance of links (*ADL*), which is the total absolute distance between the links visited by a user u_i to be:

$$nav^{adl}(u_i) = \frac{|x_1 - 1| + \sum_{i=2}^{N} |x_i - x_{i-1}|}{N}$$

In the aforementioned equation, x_i represents the identifier of links visited, i.e., i=1 is the first link visited (x_1 is equal to 1), i=2 the second (x_2 is equal to 2) and so on, and N is the number of total links clicked. Thus the distance between sequential links is assumed to be equal to 1.

User Grouping

For classifying users into specific groups (e.g., Verbal or Imager group), two widely used methods exist in the literature: (i) grouping users based on a predefined threshold value for each psychometric test or questionnaire which is suggested and standardized by the creator of each inventory (e.g., based on the aforementioned processed responses of a user (e.g., Verbal/ Imager ratio), the user is grouped in a particular group, given a predefined range of thresholds); and (ii) grouping users based on cluster analysis which aims to divide a set of users into cluster groups that are different from each other and whose members are similar to each other according to each of the aforementioned processed values. In the context of PAC, we classify users based on cluster analysis for the following reasons: (i) the suggested thresholds are standardized and evaluated based on a specific population which might not be representative for different populations under investigation; and (ii) cluster analysis could yield very good results in our case since the data being processed represent a scale with two end points (e.g., low and high values of the Verbal/ Imager ratio represent respectively Verbal and Imager users), and thus can effectively separate users from each other depending on the responses to each stimuli. Apparently, cluster analysis also entails practical limitations, such as initialization issues, i.e., when a limited number of users are registered in the system, making the cluster analysis difficult and ineffective to perform. However, dealing with issues related to effective and efficient cluster analysis is out of the scope of this thesis.

In this respect, depending on the aforementioned processed values of each user (i.e., $\lambda^{v:g}(u_i)$, $\lambda^{w:a}(u_i)$, $\mu^{sc}(u_i)$, $\mu^{mab}(u_i)$, $\lambda^{vt:vg}(u_i)$, $nav^{adl}(u_i)$), users with close distance values will be grouped in the same cluster. Accordingly, the following characteristics for each user are finally elicited based on the cluster the user is assigned: (i) A user is either a Verbal, or an Imager (based on $\lambda^{v:g}(u_i)$ or $\lambda^{vt:vg}(u_i)$); (ii) a user is either a Wholist, or an Analyst (based on $\lambda^{w:a}(u_i)$ or $nav^{adl}(u_i)$); (iii) a user has either limited or enhanced speed and control of processing (cognitive processing efficiency); and (iv) a user has either limited or enhanced working memory capacity.

For user grouping we utilize the *k*-means clustering algorithm since it is considered one of the most robust and efficient clustering algorithms (Wu et al. 2007). The *k*-means clustering algorithm is performed as follows: The algorithm initially sets the data point with the smallest value (e.g., Verbal/ Imager ratio) as the first cluster center and the data point with the largest value as the second cluster center. Given that the desired groups are known in our case (e.g., Verbal and Imager), the algorithm is set to k=2. The distance between all other data points and cluster centers are then

calculated, and each data point is assigned to the cluster whose distance from the cluster center is the 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 newly created cluster. Next, the distances between each data point and the newly obtained cluster centers are recalculated in an iterative approach until no data point is reassigned. The respective cluster group that users are assigned represent their cognitive processing characteristics. For example, all users that are grouped in the "Verbal" cluster are considered to have a verbal type of cognitive style.

User Model

The above process results in constructing the final structure of the user model. More specifically, the user model um of a user u_i ($um(u_i)$) is composed of demographics (*category=d*) and cognitive characteristics (*category=cc*), and contains triplets of the form (ct, ch, val), where ct represents an information category (e.g., demographics, cognitive characteristics, etc.), ch represents a characteristic (e.g., age, gender, verbal/ imager cognitive style, wholist/ analyst cognitive style, working memory, general anxiety, etc.) and val the value for the specific characteristic. For example, a user u_i may have the following user model:

$$um(u_i) = \{(d, age, 25), (cc, v/i, verbal)\}$$

indicating that u_i has an *age=25* in the demographics (*d*) information category and he is verbal (*v/i*) in the cognitive characteristics (*cc*) category.

6.1.2 Module 2 - Personalization

Upon user grouping, the Personalization module recommends a particular user authentication and CAPTCHA type and complexity based on the generated user models. To accomplish this, the Personalization module utilizes: (i) The cognitive characteristics inside the constructed user model $um(u_i)$ that was described in the previous section; (ii) the various design factors of user authentication and CAPTCHA mechanisms; and (iii) adaptation rules that decide the "best-fit" design for a specific user u_i according to his user model.

Adaptation Component

The adaptation component is composed of the adaptation rules' pool (AR), the recommendations' pool (R) and the adaptation engine (r). AR is the set of all adaptation rules that will be described shortly. R is the set of all recommendations in the form of triplets $(category, characteristic, val)$ (e.g., (design, authentication type, textual)). The adaptation en-

gine is responsible for generating a set of recommendations (R') for a user u_i using the user model $um(u_i)$ and a set of adaptation rules (AR).

The adaptation engine can be conceptually visualized as the following function:

$$r(um(u_i), AR) = R', R' \subseteq R$$

An adaptation rule attempts to map particular user model characteristics with specific recommendations. The adaptation rules involve mapping of cognitive factors (e.g., user is Verbal) to design factors of the user interface (e.g., textual or graphical representation). These rules can be extended according to the provider's custom requirements and application domain. An example of an adaptation rule can be *"if user u_i is Verbal (i.e., $(vi, verbal) \in um(u_i)$) then the user authentication type should be text-based"*. This is represented by the following rule:

Example Rule 1: ((*vi*, *verbal*), {(*security_type*, *textual*)})

More complex Boolean expressions can of course be expressed by the above format. Additional examples are presented below. Note that there are cases where a set of conditions may result in two or more recommendations (see Example 5), and that is why the recommendations appear as a set.

Example Rule 2: ((*vi*, *imager*) AND (*wm*, *limited*), {(*security_type*, *textual*)})

Example Rule 3: ((*vi*, *verbal*) OR (*wa*, *wholist*), {(*security_type*, *textual*)})

Example Rule 4: ((*vi*, *imager*) AND (*wa*, *analyst*) AND (NOT (*wm*, *limited*)), {(*security_type*, *graphical*)})

Example Rule 5: ((*vi*, *imager*) AND (*wm*, *limited*), {(*security_type*, *textual*), (*complexity*, *standard*)})

However, processing complex Boolean expressions is highly inefficient as it introduces parsing and recursive expression recognition and evaluation (e.g., decision trees). In order to alleviate this problem we have introduced a pre-processor step that transforms a Boolean expression into its logically equivalent conjunctive normal form (CNF) using components from the double negative law, De Morgan's laws and the distributive law. It then decomposes the expression into a set of subexpressions (i.e., linked with an *AND* as CNF dictates) that should all evaluate to *true* in order for the rule to be applied. In order to better facilitate our discussion we illustrate the usage of the preprocessor step in the above examples:

Example Rule 1: ({(*vi*, *verbal*)}, {(*security_type*, *textual*)})

Example Rule 2: ({(*vi*, *imager*), (*wm*, *limited*)}, {(*security_type*, *textual*)})

Example Rule 3: ({(*vi*, *verbal*)}, {(*security_type*, *textual*)}, {(*wa*, *wholist*), (*security_type*, textual)})

Example Rule 4: ({(*vi*, *imager*), (*wa*, *analyst*), (NOT (*wm*, *limited*))}, {(*security_type*, *graphical*)})

Example Rule 5: ({(*vi*, *imager*), (*wm*, *limited*)}, {(*security_type*, *textual*), (*complexity*, *standard*)})

Consequently, the adaptation component stores an adaptation rule $ar_i \in AR$ in the form of a tuple (E, RC), where E is a conjunction of Boolean expressions and $RC \subseteq R$ is a set of recommenda-

tions. We have selected to store the Boolean expressions in conjunctive normal form in order to allow for efficient evaluation of each expression in linear time as illustrated in Algorithm #1.

ALGORITHM 1. Recommendations (*r*)

Input: User model $um(u_i)$ and a set of adaptation rules *AR*

Output: Set of recommendations R', $R' \subseteq R$

```
1:  procedure: r(um(u_i), AR))
2:    // Initialize the recommendations for user u_i
3:    R' = ∅;
4:    // Test every adaptation rule ar in the set of adaptation rules AR
5:    for each ar(E, RC) in AR
6:      // Assume that the rule ar applies
7:      test = true;
8:      // Test every expression e in the set of Boolean expressions E
9:      for each e in E
10:       // If an expression cannot be found in the user model then ar does not apply
11:       if ( (e is NOT && e ∩ um(u_i) ≠ ∅) || ( !e is NOT && e ∩ um(u_i) = ∅)) )
12:         test = false;
13:         break;
14:       end if
15:     end for
16:     // If all expressions in ar apply then add the recommendations RC
17:     // to the set of final recommendations R'
18:     if ( test == true )
19:       R' = R' ∪ RC;
20:     end if
21:   end for
22:   // return the set of all discovered recommendations
23:   return R'
24: end procedure
```

Based on the aforementioned formalization, we have designed several adaptation rules (*AR*) that are based on specific design guidelines. A series of design guidelines and adaptation effects will be thoroughly presented in chapter 8.

Next, based on the generated recommendations, the adaptation engine is finally run to adapt the security mechanism according to the cognitive characteristics inside the user model $um(u_i)$ of a user u_i. More specifically, the adaptation engine can be visualized as a function $ae(um(u_i), R', s_j)$

where $um(u_i)$ is the user model of a user u_i, R' is a set of recommendations generated based on Algorithm #1, and s_j is a unique identifier for the security mechanism with particular predefined design characteristics.

6.2 Design and Development of PAC

The PAC framework has been realized in a two-tier architecture as depicted in Figure 22. It is comprised of the PAC Web server and the PAC Back-end. These are described next in detail.

6.2.1 PAC Web Server

The Web server serves primarily as an interface between the users and the back-end system and consists of three modules: (i) The administration and management module; (ii) the front-end user modeling module; and (iii) the adaptive user interface.

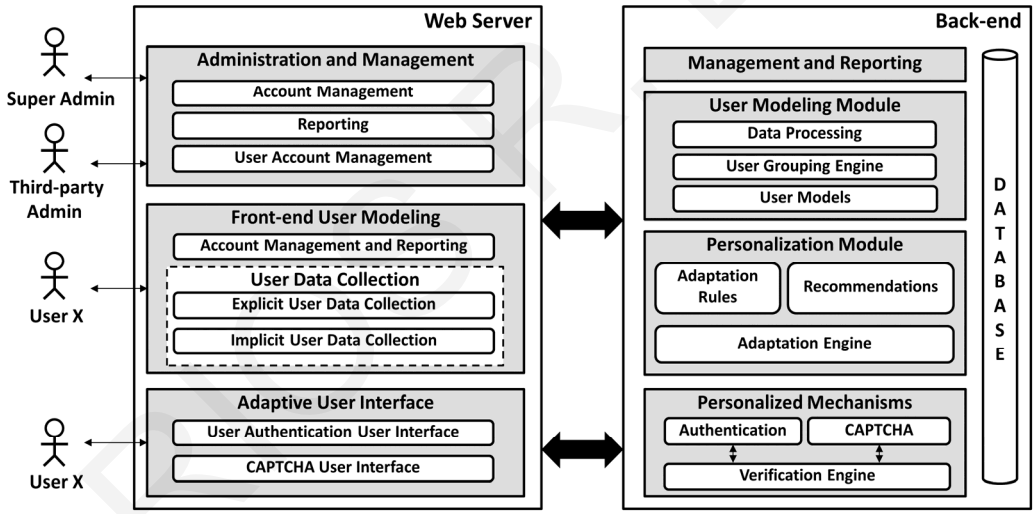


Figure 22. Architectural design of the PAC framework

Furthermore, from a technical perspective, personalizing the CAPTCHA mechanism entails an important challenge: *how to communicate the users' cognitive characteristics to the CAPTCHA mechanism*. Given that CAPTCHA are utilized as public security defense mechanisms to prevent malicious software attacks, an important challenge of the proposed personalization method in CAPTCHA is that the identity of a legitimate user is not known, and thus his/her characteristics need to be identified and communicated to the CAPTCHA mechanism for personalization. Given this technical challenge, we separately present the personalization method of CAPTCHA (Figure 23) to shed light on how we addressed this issue.

As described in the previous sections, the user modeling module is responsible to generate the user models by initially collecting and processing data about the users' cognitive characteristics. When users complete their user model generation, a persistent HTTP cookie is created on the us-

ers' device that is further utilized by the CAPTCHA mechanism to retrieve the users' cognitive characteristics and accordingly personalize the CAPTCHA tasks based on recommendations that decide which design characteristics of CAPTCHA to communicate to the users. The CAPTCHA mechanism is embedded as an HTML iframe element in any third-party Web-page. When users load the third-party Web-page with the CAPTCHA embedded, the CAPTCHA mechanism utilizes the HTTP cookie from their device and directly serves a personalized CAPTCHA to the users.

The use of an HTTP cookie for retrieving the user models was decided due to the fact that CAPTCHA in general serve as public security mechanisms and thus the identity of the users (and their respective user models) are not known for personalizing the task. Accordingly, the HTTP cookie is utilized by the mechanism to identify the users and retrieve their user models for deciding which design of CAPTCHA to communicate to the user interface. Furthermore, the use of HTML iframes for embedding the CAPTCHA mechanism into third-party Web-pages was decided due to the "same-origin policy" (W3C 2015) that prevents HTTP cookies from being shared across multiple domains that are hosted on different servers. Therefore, the CAPTCHA mechanism should run under the same server as the user modeling module for retrieving the user models, and is achieved thus by embedding the CAPTCHA mechanism as an HTML iframe in a third-party Web-page that points to the same server where the user modeling module is hosted.

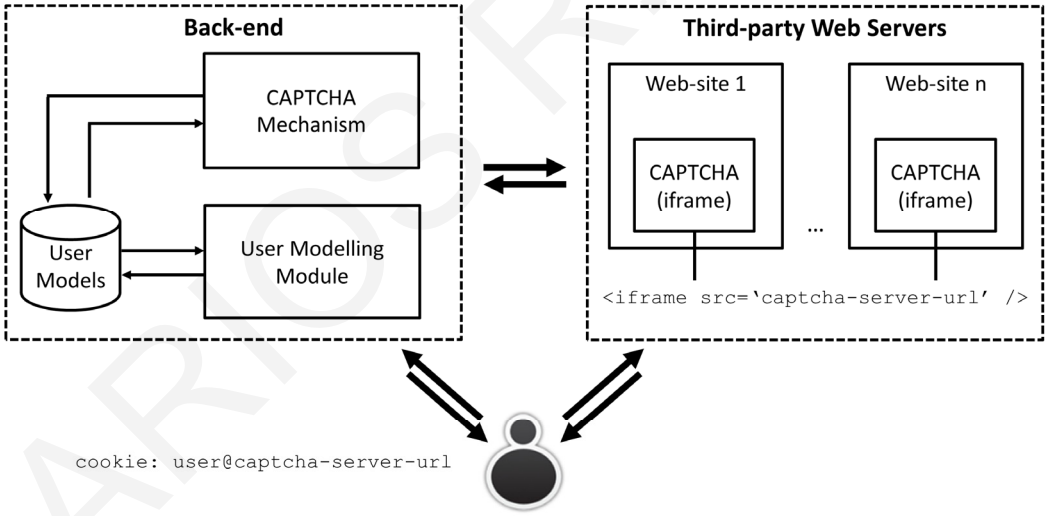


Figure 23. Architectural overview of the personalization method of CAPTCHA

Administration and Management

The administration and management serves as the main front-end system enabling the administrator of PAC to interact with the Back-end system in order to manage various components of the system such as view and manage the actual users' accounts. It also enables the administrator to manage the user data collection methods (e.g., psychometric tools). For the development of the administration and management component we have used as a basis the popular WordPress

(2015a) Content Management System and extended its main functionality based on the requirements of this thesis. We have selected WordPress since it is a widely used and accredited Content Management System (2015b). A reporting system is also provided for viewing the users' models and perform statistical analysis tests.

Account Management and Reporting. The account management and reporting component provides a tool to administrators of PAC to manage essential information about the system. Managing users is an important component of the administration system in which the administrator creates new users or manages existing user accounts, assigns roles to users (e.g., simple user) and access rights (e.g., read, write, or both). The administrator is also able to manage the elicitation tools by enabling or disabling specific elicitation tools that are displayed in the front-end user modeling component of the users. Figure 24 illustrates the elicitation tools' management component in which all the available elicitation tools of the system are displayed and the administrator is able to activate or deactivate a particular elicitation method by clicking on the corresponding icon of the method.

This component has been developed for enabling researchers and administrators to easily choose and enable the elicitation tools based on the aim and method of various user studies. For example, for a particular user study investigating only cognitive styles, all the other tests and methods (e.g., speed of processing) can be disabled so that these will not be displayed on the users' modeling front-end dashboard.

Name	Is Active Click image to Activate/Deactivate	Is Active For Study Click image to Activate/Deactivate	Date Added
CSA Wholist/Analyst	✓	✓	2013-08-12 20:24:03
Speed of Processing	✓	✓	2013-08-12 20:24:03
Controlled Attention	✓	✓	2013-08-13 16:38:03
Implicit/DPE	✓	✗	2014-04-09 20:19:54
VICS	✗	✗	2013-06-24 16:09:30
GEFT P1	✗	✗	2013-07-12 00:35:15
Visual Working Memory	✓	✓	2013-08-18 16:38:18
Extended CSA	✗	✗	2013-09-02 19:32:38
CSA Verbal/Imager	✓	✓	2013-09-06 13:38:33
Verbal Working Memory	✓	✗	2014-02-05 16:21:12
Personality Test	✓	✓	2014-02-05 16:12:11
Satisfaction Questionnaire	✗	✓	2014-02-05 16:13:07
General Anxiety	✗	✗	2013-08-29 17:25:04
Current Anxiety	✗	✗	2013-08-29 17:25:04
Emotion Regulation	✗	✗	2013-08-29 17:25:04

Figure 24. Enabling/ disabling psychometric tests to be displayed in the front-end user modeling dashboard

Next, the system provides easy to use tools for generating graphical reports in order to view the distributions of users based on their cognitive characteristics. Figure 25 and Figure 26 illustrate an example scenario of the reporting component in which the administrator first selects the grouping method (group users based on cluster analysis or based on predefined thresholds), then selects the first level dimension for grouping users, the drill-down dimension to further group the first-level grouping based on a second dimension, and the date range the users enrolled in the system. The graphical report can be generated in the form of columns (for drill-down option) or in the form of scatter plot in which the actual values of each human factor (e.g., based on the Verbal/ Imager ratio) is illustrated in order to visualize the distribution of each user group and their corresponding scores in the elicitation tool.

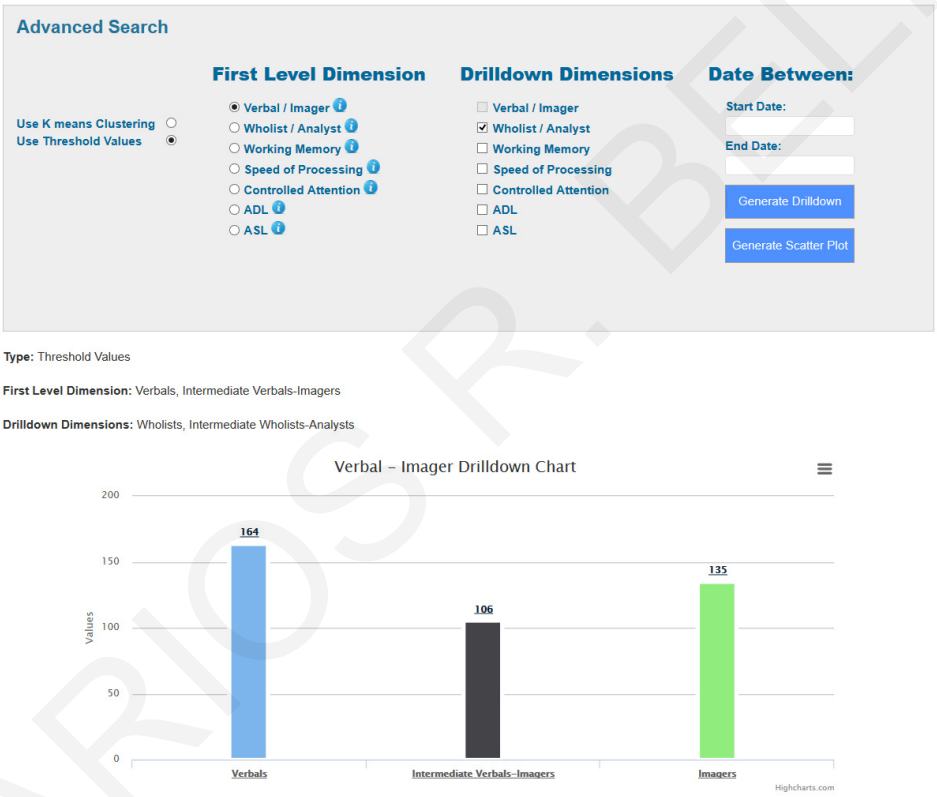


Figure 25. Viewing the total number of users for each cognitive style group (Verbal/ Imager) (HighCharts 2015)

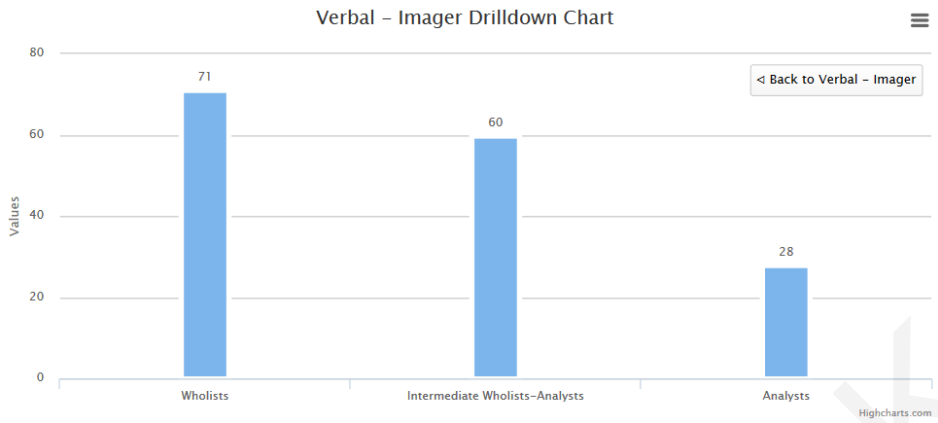


Figure 26. Performing a drill-down action on the Verbal group for viewing the distribution of Verbal users in regards with the Wholist/ Analyst cognitive style (HighCharts 2015)

User Account Management. The user account management component provides all the necessary tools and functionalities for managing information that is related to the users of the system. Administrators are able to search for enrolled users based on different keywords and criteria (e.g., name) and further view information about each user. In particular, the administrator can view information about the users' accounts, their scores on the psychometric tests and Web interaction metrics. Figure 27 illustrates an example of listing users based on specific search criteria.

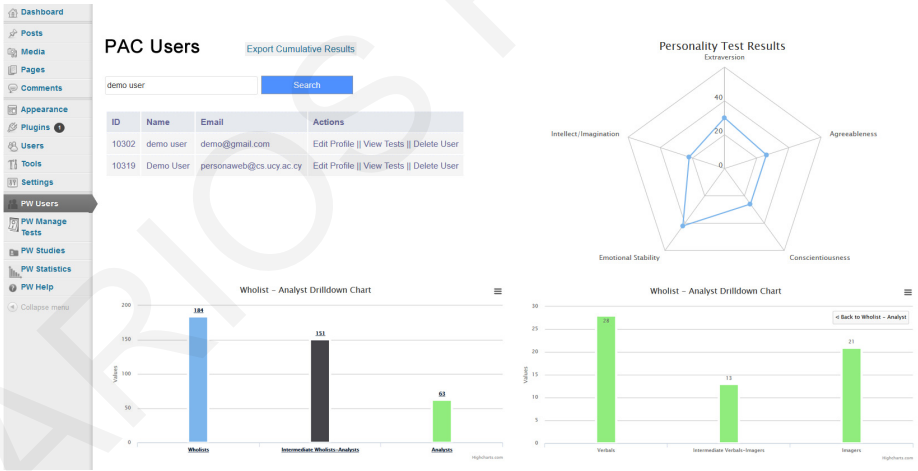


Figure 27. Listing user accounts and viewing information based on a search result (HighCharts 2015)

The administrator can further perform specific actions on the user model such as edit basic information about the user and generate new password keys for users that have forgotten their password combination (Figure 28). In the latter case, an email is sent to users with specific steps for resetting their password and creating a new authentication key. An option for deleting the user account and respective model permanently from the database is also available. The system also provides tools for exporting the user's information into different formats for third-party software applications (e.g., MS Excel).

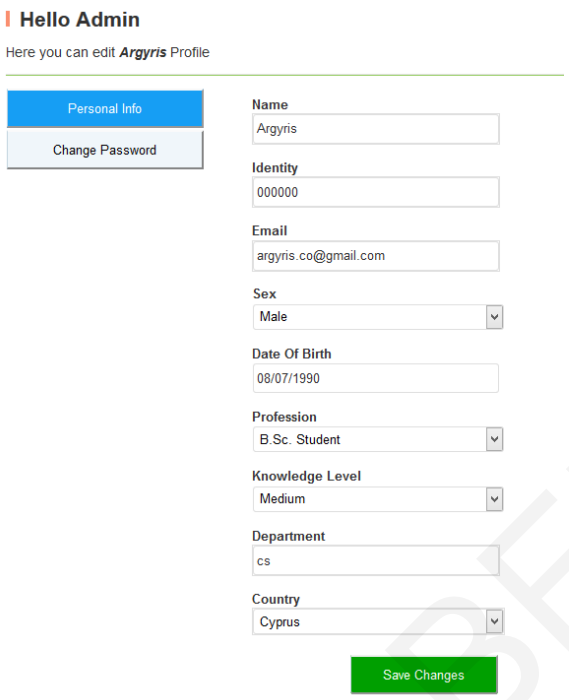


Figure 28. Editing basic information of a selected user

Front-end User Modeling

The front-end user modeling is responsible to generate the users' models through explicit and implicit data collection methods. Users initially enroll in the user modeling module, by providing basic account information and their demographics (gender, date of birth, email), and further elicit their cognitive processing characteristics by running specific human factor elicitation tools or through a controlled implicit user data collection method (as seen in section 6.1.1). Reporting tools are also available for viewing the results of the users' actual responses to the stimuli (i.e., time to respond to the test, whether the answer was correct or not, view the actual result, etc.) but as well compare their user model characteristics with other anonymous user models of the system. Figure 29 illustrates the starting page of the front-end user modeling module in which all the user data collection methods (psychometric tests and Web navigation environment) are accessible.

Explicit User Modeling – Psychometric Tests and Questionnaires. The primary method for eliciting the users' characteristics is through specially designed psychometric tests and questionnaires. Each psychometric test entails different cognitive aptitude tasks in which users are required to respond to and the system then processes the responses for generating the users' characteristics. A psychometric test initiates by clicking on the "Start" button which redirects to a Web-page providing instructions to the users for conducting the test. The nature of each psychometric test and stimulus are described in section 6.1.1. When the test is completed, the primary results of the test are illustrated in a summative form in the section of the corresponding test. In particular, the sec-

tion illustrates the following information about each test: Number of times the user conducted the test, the date of the last time the test was conducted, the number of correct responses (where applicable), the mean time or ratio required to answer the stimuli and the user's characteristic extracted.

Figure 29. Dashboard of the user modeling module for accessing the explicit and implicit user data collection methods

An additional option for viewing the analytical results of the tests is also available. The users click on the "Results" button which redirects to a Web-page with more information about the results of the test. Figure 30 illustrates an example of a visual working memory test in which the following information is illustrated to the user: The response time to each stimulus, the validity of the answer (true/ false), the user's given answer and the actual correct answer of the stimulus.

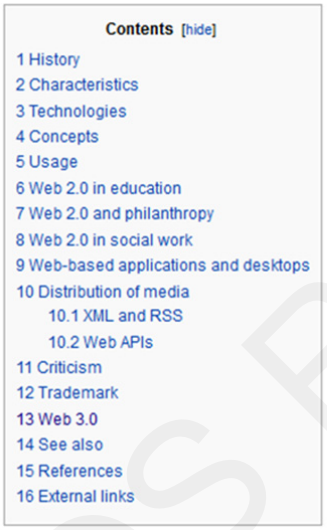
Date of test	Correct	Level
2015-04-17 15:16:14	12	MEDIUM
2015-04-17 15:14:20	0	LOW
2014-10-09 18:17:42	4	LOW

Question Number	Response Time (ms)	Is Right	Given Answer	Answer
1	1273	Correct	False	False
2	1087	Correct	True	True
3	898	Correct	False	False
4	805	Correct	False	False
5	2079	Correct	False	False
6	1173	Correct	False	False
7	1221	Correct	True	True
8	1189	Correct	True	True
9	879	Correct	False	False
10	1141	Correct	True	True
11	2893	Correct	False	False
12	1655	Correct	False	False
13	5435	Wrong	True	False

Figure 30. Analytical results of a session for eliciting the visual working memory capacity

Implicit User Modeling – Navigation Behavior. An option to elicit the users' cognitive styles is also available through the main dashboard. By initiating the implicit user data collection method the user is redirected to a controlled Web environment which entails a number of reproduced articles from Wikipedia. As described in section 6.1.1, the articles' content and hyperlinks have been enhanced with client-side and server-side scripts for recording the users' interactions with the articles.

In particular, in order to track the users' interactions, all hyperlinks (Navigation Menu and Content Hyperlinks) within each article have been annotated with an attribute, meaningful to the system. In particular, the hyperlinks of the Web-pages where annotated in the following manner: Navigation Menu hyperlinks and Content hyperlinks are respectively annotated with *"nav_x_y"* where *x* is the unique identifier of the current article and *y* the unique identifier of the navigation menu hyperlink, and *"content_x_y"* where *x* is the unique identifier of the current article and *y* the unique identifier of the content hyperlink. In both hyperlink types, *y* is used to calculate the distance between the hyperlinks visited by the user. A browser-based logging facility was developed to store all users' interactions with each annotated hyperlink in the server's database. Figure 31 and Figure 32 respectively illustrate the annotations made.

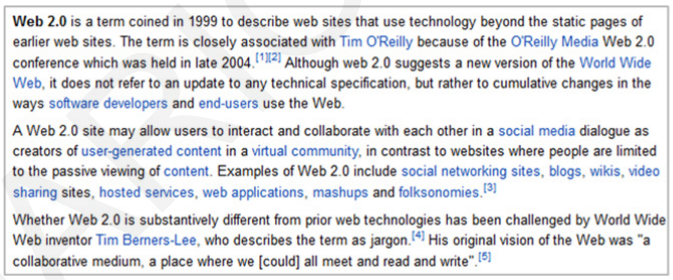


Contents [hide]

1 History
2 Characteristics
3 Technologies
4 Concepts
5 Usage
6 Web 2.0 in education
7 Web 2.0 and philanthropy
8 Web 2.0 in social work
9 Web-based applications and desktops
10 Distribution of media
10.1 XML and RSS
10.2 Web APIs
11 Criticism
12 Trademark
13 Web 3.0
14 See also
15 References
16 External links

Hyperlink	ID
History	nav_1_1
Characteristics	nav_1_2
Technologies	nav_1_3
Concepts	nav_1_4
Usage	nav_1_5
...	nav_x_y

Figure 31. Navigation menu hyperlink semantic annotations



Web 2.0 is a term coined in 1999 to describe web sites that use technology beyond the static pages of earlier web sites. The term is closely associated with Tim O'Reilly because of the O'Reilly Media Web 2.0 conference which was held in late 2004.[1][2] Although web 2.0 suggests a new version of the World Wide Web, it does not refer to an update to any technical specification, but rather to cumulative changes in the ways software developers and end-users use the Web.

A Web 2.0 site may allow users to interact and collaborate with each other in a social media dialogue as creators of user-generated content in a virtual community, in contrast to websites where people are limited to the passive viewing of content. Examples of Web 2.0 include social networking sites, blogs, wikis, video sharing sites, hosted services, web applications, mashups and folksonomies.[3]

Whether Web 2.0 is substantively different from prior web technologies has been challenged by World Wide Web inventor Tim Berners-Lee, who describes the term as jargon.[4] His original vision of the Web was "a collaborative medium, a place where we [could] all meet and read and write".[5]

Hyperlink	ID
Tim O'Reilly	content_1_1
O'Reilly Media	content_1_2
World Wide Web	content_1_3
software developers	content_1_4
end-users	content_1_5
...	content_x_y

Figure 32. Content hyperlink semantic annotations

To better explain the metric, we provide an example navigation, e.g., the click stream navigation pattern *"nav_2_4 | nav_2_2 | nav_2_3"*, indicates that the user visited article with *ID*=2 and then read the content of the fourth, second and third hyperlink of the navigation menu in the system. For this particular navigation, as defined in section 6.1.1, the *ADL* metric is then calculated as: *ADL*=(|4-1|+|2-4|+|3-2|)/3=2. Accordingly, a high number of the metric indicates that the user followed a non-linear navigation behavior, whereas a small number of the metric indicates a linear navigation behavior.

Adaptive User Interface

The adaptive user interface is responsible to communicate the adapted and personalized security mechanism based on the generated user model. We dedicate chapter 8 providing a detailed presentation of design guidelines and adaptation effects for the selected security mechanisms, and the added value of adapting content and functionality in terms of task usability and user experience.

6.2.2 PAC Back-end

The back-end system processes the collected data coming from the front-end modules and stores them in the database. It consists of four modules: (i) The management and reporting module; (ii) the user modeling module; (iii) the personalization module; and (iv) the personalized mechanisms.

The *management and reporting module* contains methods for managing and storing information such as the user account of the PAC administrator and the actual users of the PAC system. It also has a reporting engine that contains methods for generating reports (e.g., number of users registered) that are illustrated in tabular or graphical format.

The *user modeling module* contains methods for processing the user data based on the explicit and implicit user data collection methods and a user grouping engine that is responsible for generating the users' characteristics. The explicit user modeling contains a number of psychometric tests whose content (e.g., psychometric test type, questions, figures) is stored in the database and retrieved in a new test occurrence (user session). Each psychometric test and questionnaire corresponds to a particular human factor of the user that is modelled through a value (e.g., cognitive style ratio) that is the result of specific data processing described in section 6.1.1. Alternatively, the implicit user modeling contains methods for processing and storing user interaction data coming from a controlled Web environment that tracks the users' navigation behavior (i.e., the sequence of pages a user followed in a Web environment and how long he was reading specific content sections). The users' interaction data are modeled by utilizing a Web data metric that indicates a user's tendency to navigate linearly or non-linearly (correlated to the Wholist/ Analyst cognitive style dimension) and a user's tendency preferring to read content illustrated in a diagrammatic representation or textual representation (correlated to the Verbal/ Imager cognitive style dimension) (described in section 6.1.1). Furthermore, the resulting values of each user are provided as input to a user grouping engine that is responsible to classify the user to a particular cognitive factor group that consists of users sharing a similar value of the metric (representing a particular cognitive factor of that user).

The *personalization module* contains an adaptation engine that is responsible to map the elicited human factors with specific design factors (e.g., type of content, complexity of content). In particular, the adaptation engine applies specific adaptation rules and recommendations.

The *personalized mechanisms* (i.e., the user authentication and CAPTCHA mechanisms) are finally communicated to the user interface based on the recommendation of the personalization module.

User Authentication Personalization Mechanism

The user authentication personalization mechanism is executed only once during user enrolment with an interactive system in which the authentication type (textual or graphical) and complexity level (baseline or enhanced) is mapped to the user account. After enrolment, the user authenticates with the mapped authentication mechanism by first providing his username for identification. Figure 33 depicts the workflow of the personalization process of a user authentication mechanism during user enrolment with an interactive system. For the sake of presentation, we depict the whole process during enrolment, from user modeling to adapting the user authentication mechanism.

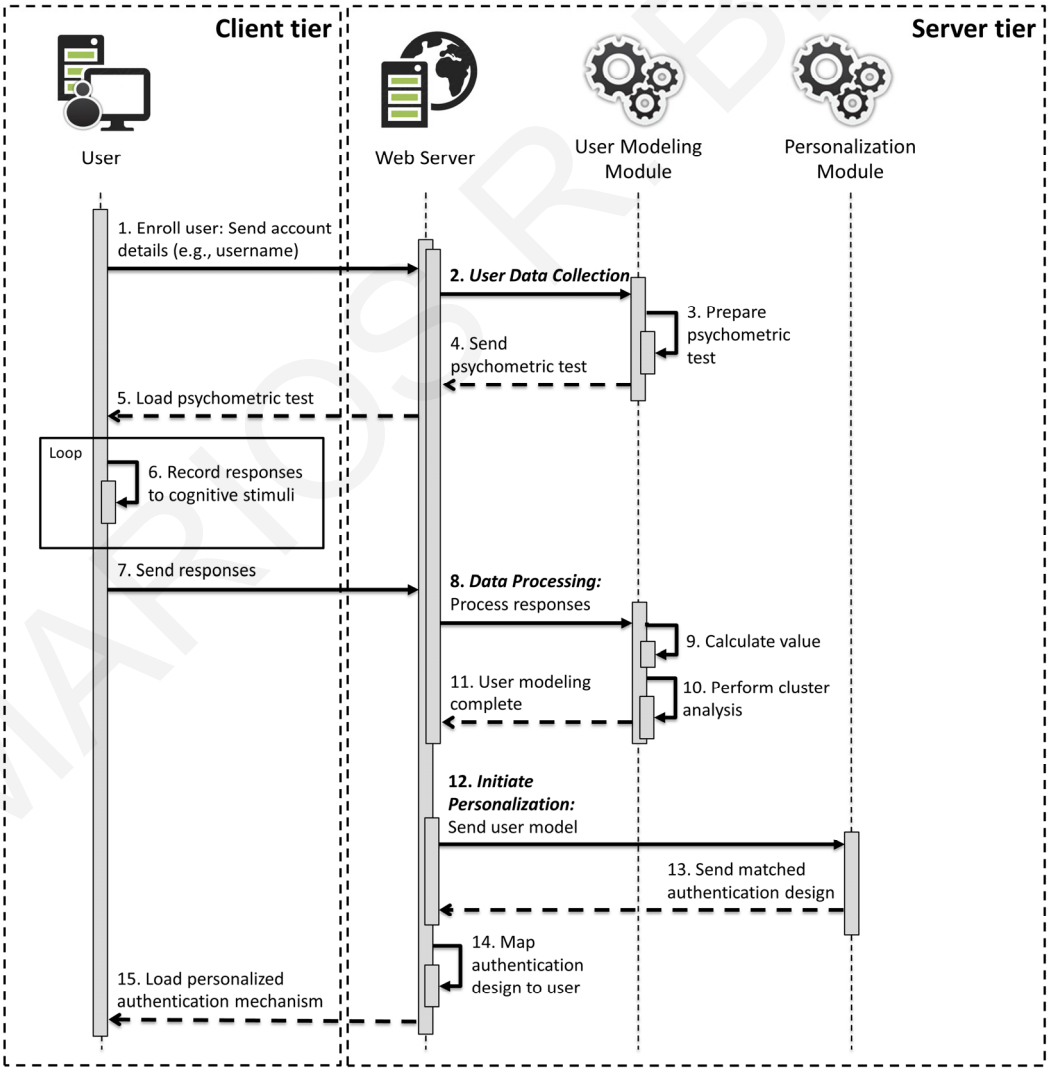


Figure 33. Sequence diagram of the user authentication personalization process during user enrolment

CAPTCHA Personalization Mechanism

The CAPTCHA personalization mechanism is responsible to retrieve the user models and accordingly provide a personalized CAPTCHA design based on the users' cognitive characteristics and interaction device type. Figure 34 illustrates the sequence diagram of a user's interaction with the CAPTCHA mechanism. Accordingly, the following steps are performed:

(1) The user requests and loads a third-party Web-page with the CAPTCHA embedded as an HTML iframe.

(2) The CAPTCHA is loaded through the HTML iframe. The HTML iframe requests the CAPTCHA challenge from the server and also sends the HTTP cookie stored on the user's device which contains a unique session ID of the user. In case an HTTP cookie does not exist on the user's device (either because the user has cleared the Web browser's cache, or the user is not logged in the user modeling module), the CAPTCHA mechanism provides an option to the user to login into the user modeling module in order to retrieve the user model. If the user decides to login, a new persistent HTTP cookie is stored on the device which is further utilized by the CAPTCHA mechanism.

(3) The Web server performs the following steps:

   a. Request the user model based on the user's unique session ID.
   b. Detect the user's device (standard IO or touch-based) based on the client's HTTP request.
   c. Decide a specific CAPTCHA type (text- or image-recognition) and complexity level (baseline or enhanced) based on the user's cognitive styles and abilities. If no session ID was sent by the client's Web browser in Step 2, the CAPTCHA mechanism decides a random CAPTCHA design.
   d. Based on the CAPTCHA design decision, generate the CAPTCHA challenge.
   e. Generate a unique verification code and relate it with the CAPTCHA challenge. The verification code is used by the CAPTCHA mechanism to identify the challenge for validating the user's response; whether the user solved correctly the CAPTCHA challenge or not.
   f. Send the CAPTCHA challenge and verification code back to the client's browser and illustrate the CAPTCHA challenge to the user.
   g. The verification code of the CAPTCHA mechanism is also set as a hidden HTML input element in its parent (third-party) Web-page by utilizing the *window.postMessage* method (Mozilla Foundation 2015) that safely enables cross-origin communication between the third-party Web application and the CAPTCHA mechanism. This is needed so that the third-party Web application can validate the user's response on its hosting server to decide whether or not to allow the user to complete the request.

(4) The user solves the CAPTCHA challenge; depending on the type, the user is required either to enter alphanumeric characters (text-recognition), or select specific images (image-recognition). The user submits the result back to the CAPTCHA mechanism along with the verification code.

(5) The CAPTCHA mechanism validates the answer, marks whether the answer was correct or wrong and responds back to the user with the decision.

(6) The user submits the form to the third-party application server.

(7) The third-party application server communicates with the verification component of the CAPTCHA mechanism and sends the verification code.

(8) The verification component checks the decision taken in Step 5 and communicates it back to the third-party application server.

(9) If the decision was positive (the user successfully solved the challenge), the third-party application server allows the user to access some service or information (e.g., allow to comment on a blog). Otherwise, the application server prevents access to the user and communicates an error message back to the user with a newly generated CAPTCHA challenge. In that case, the process repeats from Step 2.

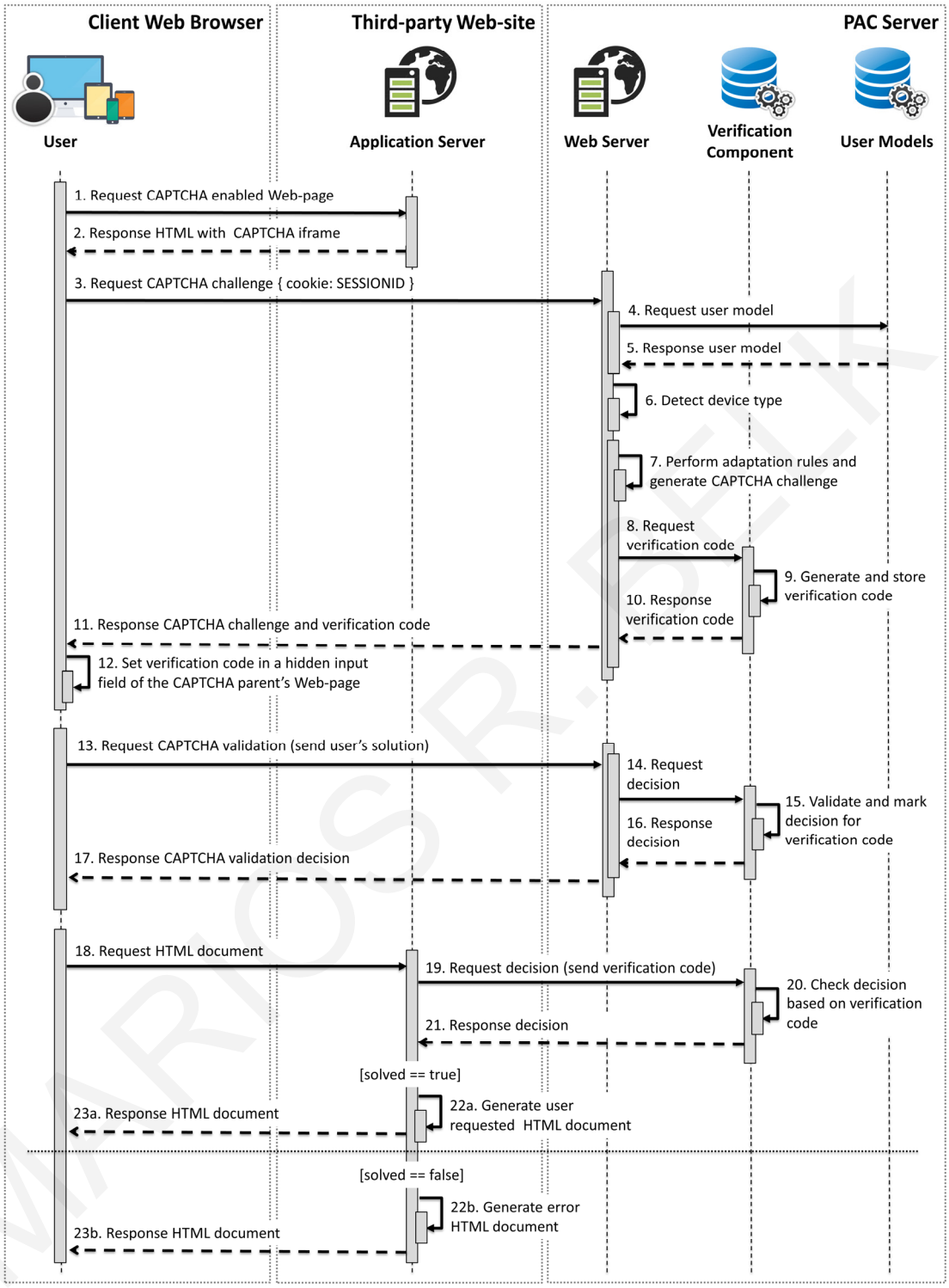


Figure 34. Sequence diagram of a user interacting with the CAPTCHA mechanism. The user is logged in the user modeling mechanism and a permanent HTTP cookie is stored on the users' device.

6.3 Technologies and Languages for the Design and Development of the PAC System

PAC is a dynamic Web-based adaptation and personalization system. All the information is stored in a database that is essential for eliciting the users' characteristics based on their responses on the online psychometric tests, questionnaires or their navigation behavior in the controlled implicit user modeling component. Accordingly the system personalizes the user authentication and CAPTCHA task. This section will present the main technologies and languages utilized for the design and development of the PAC system. We investigate existing Web languages and technologies (server-side and client-side) and data storage technologies and consequently, we present the ones that have been advanced justifying our decisions.

6.3.1 HTML - HyperText Markup Language

Hypertext Mark-up Language (HTML) is the primary mark-up language for the creation of Web-pages on the World Wide Web. It provides a means to describe the structure of text-based information in a document by annotating certain text as headings, paragraphs, lists, etc., and to supplement that text with interactive forms, embedded images, and other objects. HTML is written in the form of labels, called tags, surrounded by less-than (<) and greater-than signs (>). For example, *<h1>some heading text</h1>* and * some information * denotes that *"some heading text"* and *"some information"* are respectively a heading and a paragraph within the HTML document. HTML tags also contain specific attributes (depending on each tag) that denote further information for that tag. For example, ** is an image tag that contains the *src* attribute that points to the actual image file that is utilized by the Web browser to illustrate that image in the Web-page. Figure 35 illustrates an example HTML code snippet that is embedded within an HTML document.

```
<p>Age</p>
<select  style="font-size:14px; width:100%" class="m-wrap placeholder-no-fix" name="Age" id="s_age" class="span12 select2">
    <option selected value="">50+</option>
    <option value="1">&lt;20</option>
    <option value="2">20-25</option>
    <option value="3">26-30</option>
    <option value="4">31-35</option>
    <option value="5">36-40</option>
    <option value="6">41-45</option>
    <option value="7">46-50</option>
    <option value="8">50+</option>
  </select>
```

Figure 35. An example HTML code snippet

In this context, the main purpose of HTML is to display and format content, allowing very limited interaction with the Web-page. HTML also describes at some extent the semantics of a document and can include embedded scripting language code for manipulating at run-time the HTML elements of a document and the behavior of the Web-page. Since its proposal, HTML has undergone several changes and different versions exist. The following versions of HTML exist:

HTML 1.0 (1989 - 1994): HTML 1.0 is the first version of HTML and was supported by a non-graphical browser running on UNIX, called Lynx and Mosaic. HTML 1.0 supported inline images and text controls, without further capabilities for styling of content.

HTML 2.0 (1995): HTML 2.0 was specified by the World Wide Web Consortium (W3C) and was supported by more Web browsers. HTML 2.0 was extended to include elements such as tables, text boxes, buttons, and attributes for changing the Web-page background. Since HTML 2.0, Web browsers specified additional features that were not part of the official W3C specification.

HTML 3.2 (1997): HTML 3.2 included support for creating tables, extended options for form elements and cascade style sheets (CSS) as we will see in the next section.

HTML 4.01 (1999): HTML 4.01 further extended cascade style sheets and scripting capabilities. Further support for CSS was included enabling designers and developers to create CSS information in a different file aiming to separate the HTML elements and content structure from the styling information.

HTML 5 (2014): HTML 5 is the latest version of the HTML standard. HTML5 was extended to include new semantic elements (e.g., header, footer, article, section), form control attributes (e.g., number, date, time, calendar, and range), graphic elements (e.g., svg, canvas), multimedia elements (e.g., audio, video), application programming interfaces (e.g., geolocation, drag-and-drop, local storage).

To this end, PAC was implemented utilizing the latest version of HTML5 given its extended capabilities and to conform to the latest standards of today's HTML Web browsers.

6.3.2 CSS (Cascading Style Sheets)

As described above, HTML tags were originally designed to define the content and limited formatting of a document. The content of the document is parsed and its layout and formatting is handled by the Web browser. Given that the two early major browsers; Netscape and Internet Explorer, extended and interpreted differently the HTML tags and attributes (e.g., <*font*> tag and *color* attribute), one major issue of early versions of HTML was how to clearly separate the content from the presentation layout and design. In this context, W3C created a new means for styling HTML documents as part of HTML 4.0. In particular, W3C proposed Cascade Style Sheets (CSS) that provide a means for defining how HTML elements should be displayed, similarly to the font tag and the color attribute in HTML 3.2. CSS are either embedded inline within an HTML document using the *styles* tag or saved in an external text file (with .css file extension) and further embedded within the HTML document using the *link* tag. The CSS specification entails a high number of styling attributes (e.g., font family, font size, colors, element's positioning, width, height, etc.) that enable Web designers and developers to change the appearance and layout of Web-pages. Since its initial specification by W3C, CSS was released in three different versions. CSS1 was released in 1996, CSS2 was released in 1998, followed by CSS3 in 1999. Each release was extended with ad-

ditional support for styling Web-pages. In the context of PAC design and development, we utilized the latest version of CSS3 in order to take advantage of current state-of-the-art features for designing high quality user interfaces as well as to conform to the latest W3C Web design standards.

6.3.3 Client-side Languages

As mentioned previously, HTML defines the layout and formatting of the Web-page, allowing limited interactivity with elements. HTML is initially parsed by the Web browser, interpreted and then displayed within the Web browser. The HTML specification contains a *script* tag in which client-side scripting can be embedded within the document for manipulating the HTML elements and styles that have been loaded by the Web browser. Today's Web-sites typically combine HTML, CSS and client-side scripting for creating interactive navigation menus, highlighting effects, image effects, animation, form field validations, data manipulation and many other actions for manipulating HTML elements and styles for enhancing the users' interactivity with the system.

Since the early versions of HTML, various scripting technologies and languages were proposed including JavaScript, JScript, VBScript and others. JavaScript is currently the dominant and most applied scripting language on the World Wide Web. The most important advantages using JavaScript are: (i) JavaScript is fast because any code functions run immediately once loaded and interpreted by the Web browser; (ii) being a light-weight language, it is simple to learn and implement; (iii) it is versatile and can be inserted into any Web-page regardless of the file extension; and (iv) being client-side it reduces the demand on the Web server.

Nevertheless, due to its simplicity and due to the fact that it is a light-weight scripting language, building highly complex interactive systems on the client-side can be a challenging endeavor. In this context, over the past years, a JavaScript library called JQuery (2015) has been developed that enables an easy and effective way for building more complex scripts. JQuery's syntax is designed to simplify the development of client-side scripting by making it easier to navigate an HTML document, select elements, create animations, handle events, and develop AJAX (Asynchronous JavaScript and XML) applications. JQuery enables developers to create abstractions for low-level interaction and advanced effects.

Considering the aforementioned analysis, we have decided to use JavaScript, based on JQuery library as the main client-side scripting language for our system. The need for implementing the PAC system with JavaScript rose for multiple reasons:

1. *User Modeling:* The users' response time is of critical importance for eliciting their cognitive characteristics since the user grouping highly depends on the actual time users respond to a cognitive stimulus. In addition, the implicit user data collection method tracks the users' interactions with the hyperlinks, and these interactions must be stored in the system's database asynchronously without affecting the users' interaction with the system (without reloading the Web-page). In this context, we utilized JQuery with AJAX for processing all the required

information (e.g., response time) and asynchronously communicating the data to the system's database.

2. *Interactivity with Graphical-based Security Mechanisms:* Graphical-based security mechanisms (i.e., graphical authentication and image-recognition CAPTCHA) require users to select specific images among a grid of images.
3. *Management and Reporting:* Several JavaScript plugins have been utilized for managing and reporting the data stored in the database. For example, HighCharts (2015) reporting plugin has been utilized for generating graphical reports in the management and administration component.

6.3.4 Server-side Languages and Frameworks

Server-side scripting is a technique for Web development in which a script is created and run on a Web server which generates a customized response for each user's request to the Web-site. Server-side scripting enables the development of dynamic Web applications since the content presented in the Web-site can be different for different users. Server-side scripting is primarily used for content management in which the main content of the Web-site is stored in a database and retrieved and presented to each user on request. The main operations include the client user requesting data from the Web server, e.g., information retrieved from the database, and the client user sending information to the Web server, e.g., storing user information in the database.

Web-based adaptation and personalization systems are by definition dynamic Web applications since the user models need to be stored on a Web server (e.g., in a relational database), and retrieved for adapting and personalizing the content and functionality of the system to each request made by the client user. Similarly, in the context of PAC, we developed a number of methods both for the user modeling and personalization module.

Some of the most popular server-side technologies today are PHP (PHP: Hypertext Preprocessor), ASP (Active Server Pages) and JSP (Java Server Pages) which are used to pre-process pages and output HTML that is sent to the client user. Among these we have chosen to develop PAC using PHP which is an open-source and cross-platform server-side scripting language for creating dynamic Web-pages. PHP code is embedded in regular HTML documents (with .php extension) through PHP tags (*<?php some code ?>*). When a user requests a PHP Web-page, the Web server initially processes the PHP code snippets (which are essentially code commands) and then sends the results in HTML format back to the user's Web browser. PHP runs on Apache Web server under Windows NT or UNIX. PHP language syntax is similar to C and Perl, however is more lightweight. For example in PHP, developers are not required to declare variables before use. PHP entails a number of advantages and disadvantages. Its main advantages are: (i) It is fast, stable and easy to use; (ii) it is free, open source and cross-platform; (iii) it is easy to understand and learn; and (iv) it provides connective abilities with many databases and interface with a variety of librar-

ies. The main disadvantages are: (i) It has security flaws given its open-source nature, anyone can see the source code, so any weaknesses can be revealed more easily; (ii) it is hard to maintain due to its lack of modularity; and (iii) it is difficult to implement complex Web applications since presentation of content (HTML and CSS) and PHP code is embedded in the same file.

In this context, although developing the PAC system with other popular technologies and languages (e.g., ASP, JSP, servlets) would as well be a good development alternative, the rationale behind this choice was driven by the fact that, at this point in time, given that PAC is a proof of concept and research-oriented Web-based adaptation and personalization system, we decided to leverage the main advantages of PHP, being an open-source, cross-platform and free to use language.

The following main methods were developed as server-side scripts:

1. *User Modeling:* the users' response time to the psychometric tests, questionnaires and Web interaction metrics were processed and stored in a relational database on the Web server.
2. *Management and Reporting:* all the content stored on the Web server is requested by the client user, in which the stored information is retrieved from the database, processed and sent back to the client user in HTML form.
3. *Adaptation and Personalization:* the recommendation rules and user security mechanisms requested by the client user are retrieved from database, processed and sent to the user.

6.3.5 Storing and Retrieving Data

In PAC, the database is an integral component. It forms the core of the application, holding all of the system's information and data: user models, Web-page content (Web objects) and functionality. The database is an essential and an active component, with a high throughput of data. The database has thus been designed in a way to provide the facility to efficiently store the information as well as quickly retrieve it.

We used a relational database management system to store all the information and SQL computer language to effectively manage (create, retrieve, update and delete) the data. MySQL was used since PHP provides easy connectivity and interfaces for calling and retrieving data from MySQL databases.

Furthermore, an important concern is to ensure openness and interoperability within and between the system's components. In case an external component aims to access the user's models, either for adaptation, for historic or statistic calculations, the system must be able to support extraction of the user's model. In order to achieve this, the user's model must be easily extendible and easy to handle. Using JSON (JavaScript Object Notation) for communicating the characteristics of the user's model seems to be the best way to achieve this since it provides the extendibility we need and enhances interoperability and integration among systems' components. JSON is s a lightweight data-interchange format which is easy for humans to read and write and easy for ma-

chines to parse and generate. In this context, JSON has been used in several occasions for retrieving information from the database and provide the data as input to a client-side JavaScript function to illustrate the data (e.g., in graphical reports).

6.4 Summary

The science behind adaptation and personalization systems has undergone tremendous changes in recent years and due to the multidimensional nature of such systems, a concrete definition has not been given to date. Yet, the basic goal of all systems remains the same: To transparently adapt and personalize content and functionality of interactive systems to the unique preferences and needs of users. Based on various definitions given to date (Brusilovsky 2001; Mulvenna et al. 2000; De Bra et al. 2004; Perkowitz and Etzioni 2000; Cingil et al. 2000; Blom 2000; Frias-Martinez et al. 2005), we conclude that any adaptation and personalization system employs mechanisms that automatically or semi-automatically adapt its content, behavior and functionality according to user data (e.g., user's interaction with the system or the context of use) that have been extracted either implicitly or explicitly. The utter goal is to increase the functionality of a system and improve the users' experiences by providing personalized and bootstrapped functionalities.

In this context, this chapter presented an effort towards designing an open and extensible personalization framework for building comprehensive user models including intrinsic human factors, and accordingly adapt and personalize security mechanisms. The chapter presented the main modules and components of the framework, placing special emphasis on the formalization of a human factor-based user model (including cognitive processing characteristics of users), and the adaptation procedures and algorithms for communicating a personalized security mechanism to the user interface. Following the conceptual design and formalization of the framework, we further presented the design and implementation of a real-life Web-based adaptive interactive system, considering current technological features of Web interactive systems.

CHAPTER 7: Investigating the Impact of Human Cognitive Factors on User Authentication and CAPTCHA Tasks

Stimulated by different theories on individual differences (chapter 4), suggesting that individuals have different habitual approaches in processing, organizing and storing verbal and graphical information, a number of long-term ecological valid user studies were conducted that aimed to investigate the impact of specific cognitive factors of users towards preference and performance of user authentication and CAPTCHA tasks. Overarching aim of this phase was to increase the understanding about the interdependencies among specific user characteristics and security tasks in which human-computer interaction takes place, and accordingly lay the foundations for the design and development of the PAC framework for personalizing security-related tasks based on users' individual differences in cognitive processing.

In the rest of this chapter, we describe the method and the design of the user studies, and subsequently we analyze and discuss the findings of each study.

7.1 Research Questions

Research on user authentication and CAPTCHA has become a complex endeavor since it embraces several parameters (human and design specific) that need to be taken into account. Thus, there is a need for solid research frameworks which will assist in understanding human interactions in such settings. In this context, the question remains whether and how state-of-the-art socio-cognitive theories can be adopted as an analysis framework aiming to assist the design of more user-centered and usable security mechanisms. Motivated by the aforementioned rational, this work aims to contribute toward this direction by investigating: (i) Whether there is an observable main effect of users having a particular style of representing and processing information cognitively (verbal or visual, holistic or analytic), on user preference and task performance of two different security designs (textual or graphical); and (ii) whether there is an observable main effect of users having different cognitive processing abilities (e.g., enhanced speed of processing and high levels of working memory capacity), on different levels of complexity (e.g., number of characters/images, distortion of characters/images, etc.).

Accordingly, the following main research questions are investigated:

Related to User Authentication

- Are there significant differences between two user authentication designs (text-based password and graphical authentication) and various levels of authentication key policies regarding user preference, task efficiency and success rate among users with different cognitive styles and different cognitive processing abilities?

Related to CAPTCHA

- Are there significant differences between two CAPTCHA designs (text-recognition and image-recognition) and various levels of visual complexity regarding user preference, task efficiency and success rate among users with different cognitive styles and different cognitive processing abilities?

7.2 Experimental Instruments

A series of accredited Web-based psychometric instruments were developed in the frame of PAC (chapter 6), that highlight differences in cognitive styles and cognitive processing abilities. In regards with user authentication, two types of user authentication mechanisms were developed: a *traditional text-based password mechanism* and a *recognition-based graphical authentication mechanism*. Regarding CAPTCHA, two types of CAPTCHA mechanisms were developed: a *text-recognition CAPTCHA* that requires from users to recognize and enter distorted alphanumeric characters, and an *image-recognition CAPTCHA* that requires from users to recognize and select specific images of a particular theme.

The developed psychometric instruments, and user authentication and CAPTCHA mechanisms were applied in online University courses in the context of the user studies. The user studies followed a two-phase methodological approach that entailed a cognitive factor elicitation phase for highlighting the participants' cognitive characteristics, and a user interaction phase with the developed security mechanisms in which users authenticated and/or solved CAPTCHA challenges.

Next we present in detail the developed user authentication and CAPTCHA mechanisms and the psychometric instruments that were used in the experimental studies.

7.2.1 User Authentication Mechanisms used in the Studies

Two types of user authentication mechanisms were used: a text-based password mechanism (Figure 36) and a recognition-based graphical authentication mechanism (Figure 37). Traditional text-based password was chosen since it is currently the most popular and widely deployed user authentication mechanism (Herley and van Oorschot 2012; Chiasson et al. 2009). Recognition-based graphical authentication was intentionally chosen since the task of entering the graphical authentication key primarily involves a visual search task in which users are required to recognize their selected images among other decoy images, and thus might be affected by human cognitive differences in cognitive styles in the way they interact with the stimuli and locate pertinent information to their objective. For example, it might not be that straightforward for a particular user to recognize and recall a target object (e.g., basketball) among a number of heterogeneous objects. The two user authentication mechanisms are described next.

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 utilised 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 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.

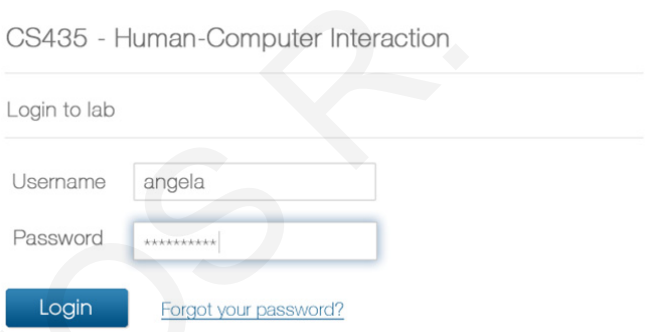


Figure 36. Textual authentication mechanism

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 were applied on the HTML form field: (i) The "autocomplete" attribute of the HTML form element was set to "off"; and (ii) given that the "autocomplete" attribute is not compatible with the Opera browser, a random name was 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.

Graphical Authentication Mechanism

The graphical authentication mechanism was designed and developed following guidelines of well reputed recognition-based graphical authentication mechanisms; such as DejaVu (Dhamija and Perrig 2000), PassFaces (2009) and ImagePass (Mihajlov and Jerman-Blazic 2011). In particular, during user enrolment, users created their authentication key by selecting a fixed number of 5 im-

ages out of 120 images in a specific order. The same image could not be selected multiple times in a single authentication key. Single-object images were used since studies have shown that these are more memorable than faces and abstract images (Mihajlov and Jerman-Blazic 2011; Chowdhury et al. 2013). During user authentication, the 5 user-selected images were shuffled with 20 stable, system-assigned decoy images, and users were required to select these 5 images based on the predefined order.

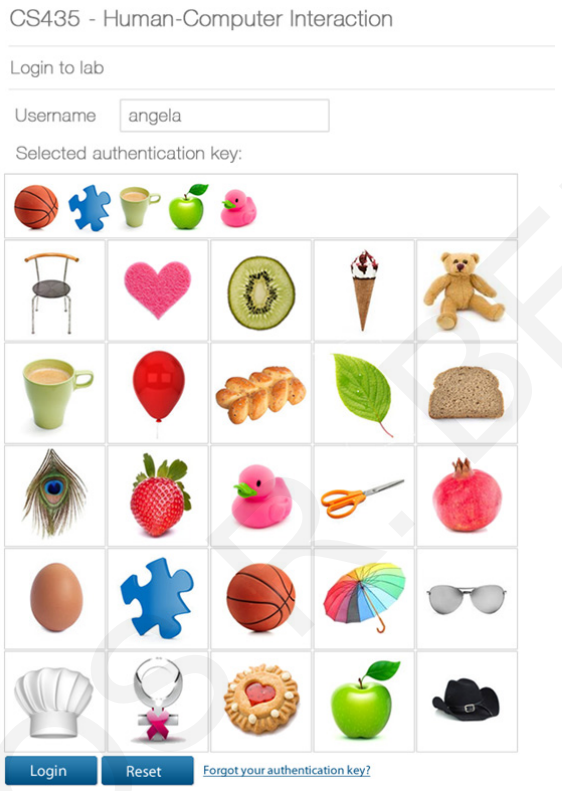


Figure 37. Graphical authentication mechanism

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

User Authentication Security Metrics

As seen in chapter 2, the security of the user authentication mechanism heavily depends on the number and type of characters/ images used in the key creation policy. For the studies conducted, we utilized standard policies that are currently used in practice, such as using a minimum number of 8 characters as the password key (von Zezschwitz et al. 2013) and not allowing the creation of a dictionary word by performing widely used dictionary checks (Komanduri et al. 2011). Accordingly, depending on the procedure of each user study, different policies were applied. For example, in some user studies, we aimed to control the policy by keeping the length and type of characters/ images of the authentication mechanism the same, while in others we provided less complex and highly complex policies to users with different cognitive processing abilities (the type of policy used in each user study will be discussed in the procedure of the corresponding study in the following sections of this chapter).

Regarding the graphical authentication mechanism, the possible authentication key space of selecting 5 images in a specific order from a set of 25 images is ~6.3x106 possible combinations, which is typical for recognition-based graphical authentication (Biddle et al. 2012; Renaud et al. 2013; Ma et al. 2013). The theoretical key space could be further increased and eventually reach the same levels of traditional text-based passwords. However this would dramatically decrease the usability of the graphical authentication task, which is a common issue in recognition-based graphical authentication mechanisms (Biddle et al. 2012). Therefore in practice, depending on the application domain and custom security requirements of the service provider, recognition-based graphical authentication mechanisms can be further enhanced with additional security methods to minimize the threat of brute force guessing attacks (both online and offline attacks) (e.g., TwoStep authentication (van Oorschot and Wan 2009), one-time password authentication (Mihajlov and Jerman-Blazic 2011)).

7.2.2 CAPTCHA Mechanisms used in the Studies

By following state-of-the-art literature in CAPTCHA, at a first level we chose to investigate traditional text-recognition and image-recognition CAPTCHA mechanisms (Figure 38) since these are currently the most widely researched and applied CAPTCHA scheme categories (Bursztein et al. 2010; Zhu et al. 2010; Moradi and Keyvanpour 2014). In particular, the choice was based on the fact that solving each CAPTCHA challenge (text- and image-recognition) requires processing and recognition of text or images in which users utilize their verbal and image cognitive sub-systems that are related to the Verbal/ Imager cognitive style theory referred in this work (Riding and Cheema 1991). We intentionally did not investigate hybrid or alternative approaches at this stage (e.g., drag-and-drop interactions, semantic approaches, etc.) since we aimed to isolate and control the type of content illustrated in the challenge (textual or graphical) so that users would utilize their

verbal and image cognitive sub-systems while processing information and solving the challenge. Furthermore, a speech-recognition mechanism was also intentionally not investigated in this work since it is considered a significantly more demanding task in terms of solving time and is mostly used for users with physical impairments (Bigham and Cavender 2009).

Figure 38. Text-recognition CAPTCHA (left) and image-recognition CAPTCHA (right)

In the analysis that follows, we describe both CAPTCHA mechanisms that were utilized focusing on their respective design and development choices, security metrics and visual design.

Text-recognition CAPTCHA Mechanism

A traditional text-recognition CAPTCHA mechanism was developed that requires from users to recognize and enter the correct sequence of alphanumeric characters that are illustrated in a distorted form on the screen. The CAPTCHA mechanism also includes a refresh button that initializes a challenge by reloading a new set of characters. The development of the text-recognition CAPTCHA mechanism was based on a similar technical and architectural approach followed by reCAPTCHA (von Ahn et al. 2008) as well as freely available open-source software (Securimage 2014). We intentionally chose an existing open-source CAPTCHA mechanism that would be extensible and customizable in order to design and customize the text features (font size, length, color, rotation etc.) for the purpose and aim of each user study. This enabled us to control the design factors and security metrics of the challenges utilized in the studies (e.g., keep the visual complexity at the same level for all participants, or adjust the complexity level for specific groups of participants). The design and customization of the text features illustrated in the CAPTCHA challenge was based on design and security guidelines proposed in Bursztein et al. (2011).

Image-recognition CAPTCHA Mechanism

The development of the image-recognition CAPTCHA mechanism was based on Microsoft ASIRRA which presents to the users 12 images (40 pixels X 40 pixels per image) illustrating cats and dogs requiring from them to recognize and select the images that display cats (Elson et al. 2007). The same interaction design was used as the one provided by ASIRRA in which users need to hover over each image in order to view the larger version of the image. The CAPTCHA mechanism also includes a refresh button that initializes a challenge by reloading a new set of images. Among a high number of existing image-recognition CAPTCHA mechanisms (Zhu et al. 2010), the choice of ASIRRA was based on the following reasons: (i) Solving an image-based challenge in

ASIRRA primarily entails a visual search task (that is affected by cognitive styles (Angeli et al. 2009)) in which users are required to search, find and recognize images of a particular theme by utilizing their image cognitive sub-system. Thus we aimed to isolate this human cognitive processing task and investigate whether cognitive styles affect the preference and task performance of this particular challenge; (ii) ASIRRA belongs to a broad image-recognition CAPTCHA category (the distinguishing CAPTCHAs) which is among the three main image-recognition CAPTCHA scheme categories (i.e., naming images, distinguishing images, identifying anomalies) (Chew and Tygar 2004); (iii) ASIRRA is a highly cited and considered a representative image-recognition CAPTCHA scheme (Zhu et al. 2010); and (iv) according to various usability evaluations and CAPTCHA reviews (Elson et al. 2009; Zhu et al. 2010), the mean task completion time is more efficient and solving accuracy is higher in contrast to other image-recognition CAPTCHA mechanisms that exist in the literature (Zhu et al. 2010).

CAPTCHA Security Metrics

The success rate of an attack is the primary metric to evaluate CAPTCHA attack effectiveness (Zhu et al. 2010). Strictly, attackers should not have a success rate higher than 0.01%; automated scripts should not be able to successfully solve more than 1 CAPTCHA challenge in 10,000 attempts (Chellapilla et al. 2005). Nevertheless, researchers have reported that such a security goal is very ambitious and challenging when designing CAPTCHA mechanisms (Bursztein et al. 2011; Zhu et al. 2010). Accordingly, the success rate of attacks are also acceptable at a value of 1% (Bursztein et al. 2011) when IP monitoring is used in combination with the CAPTCHA challenge, such as the token bucket scheme proposed in Elson et al. (2007). In essence, the token bucket scheme "punishes" users that fail to solve the challenge at first attempt by requiring them to solve two or more consecutive CAPTCHA challenges.

In this context, the security issues for the design and development of the text-recognition CAPTCHA were addressed based on design guidelines and suggestions proposed by Bursztein et al. (2011). Based on the guidelines, the success rate of an attack is estimated to be less than 1%. For the image-recognition CAPTCHA utilized in this work (ASIRRA), results reported in Elson et al. (2007) have shown that the probability of attack success is estimated to be 0.2%. On the contrary, machine learning attacks on the original version of ASIRRA, developed by Golle (2008), showed a high attack success rate (10.3%). Nevertheless, Golle (2008) suggested that with appropriate safeguards (e.g., token bucket scheme), ASIRRA *"continues to offer an appealing balance between security and usability"* (Golle 2008). Specifically, attacks with the token bucket scheme enabled have revealed that the success rate of an attack on a 12-image ASIRRA challenge is estimated to be approximately 1%. This success rate value could be further decreased by including a larger number of images in the challenge as well as using greyscale images, instead of color images (Golle 2008).

CAPTCHA Visual Designs

Based on the aforementioned security considerations, the security of CAPTCHA mechanisms is highly affected by the added complexity of the visual design of the CAPTCHA challenge (Bursztein et al. 2011; 2014; Zhu et al. 2010). Thus, in this work we primarily focus on the visual complexity of CAPTCHA mechanisms (that principally require users' cognitive processing of information) with the aim to investigate how users (with limited or enhanced cognitive processing abilities) are affected in terms of task completion performance. In this context, we have designed the two CAPTCHA challenges to entail different complexity levels.

The complexity levels of both text-recognition and image-recognition CAPTCHA were respectively based on the design and security guidelines suggested by Bursztein et al. (2011) and Golle (2008). According to Bursztein et al. (2011), increasing the security of text-recognition CAPTCHA could be achieved with the following design principles: (i) Randomize the CAPTCHA length and font size; (ii) rotate the characters in a wave fashion; (iii) use lines with the same width and color as the characters; and (iv) collapse the characters. Using a background image with noise in the challenge has shown to be insecure and therefore we excluded this technique from our text-recognition CAPTCHA design. Regarding the image-recognition CAPTCHA, based on Golle (2008), increasing the security of the ASIRRA CAPTCHA could be achieved as follows: (i) Increase the number of images in the challenge; and (ii) use greyscale instead of colored images. We intentionally did not degrade the quality of the images, nor used distortion since this is unlikely to increase the security of the particular image-recognition mechanism, but rather only decrease its usability (Golle 2008).

Two different levels in terms of visual complexity have been designed; a design with baseline security and a higher complex design. In the case of text-recognition CAPTCHA, the criteria for developing the different levels of complexity were based on the number of characters presented, and the percentage of text distortion and noise illustrated in each CAPTCHA challenge. The baseline complexity CAPTCHA entailed a random number of 5-7 characters and 40% character rotation, collapsing and lines, while the higher complex CAPTCHA entailed 8-10 characters, and 60% character rotation, collapsing and lines, as illustrated in Figure 39.

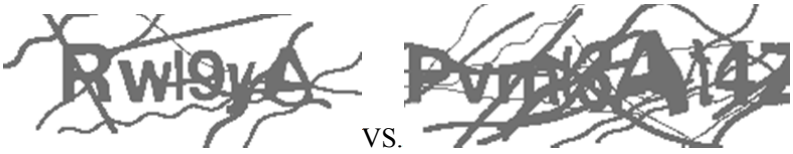


Figure 39. Baseline vs. higher complexity text-recognition CAPTCHA

In the case of image-recognition CAPTCHA, the criteria for developing the different levels of complexity were based on the number of images illustrated in each challenge and the type of image color used (greyscale or color). The low complex CAPTCHA illustrated a 12-image challenge with colored images (same as the baseline ASIRRA CAPTCHA) while the higher complex CAPTCHA illustrated a 14-image challenge with greyscale images, as illustrated in Figure 40.

Figure 40. Baseline (colored) vs. higher (greyscale) complexity image-recognition CAPTCHA

7.2.3 Cognitive Factor Elicitation Tools used in the Studies

A number of online psychometric tests were utilized (described in chapters 4 and 6). The users' Verbal/ Imager and Wholist/ Analyst cognitive styles were elicited by exploiting Riding's Cognitive Style Analysis test (CSA) (Riding 1991; Riding and Cheema 1991). The users' cognitive processing abilities were elicited by exploiting two Stroop-like tests for eliciting the users' speed of processing and controlled attention, and two working memory capacity tests as utilized in Demetriou et al. (2013). In principal, all tests measure response times of users on specially designed aptitude tasks that require cognitive processing. Depending on the response time and the provided answer to each task, the users' cognitive characteristics are highlighted on a specific scale (e.g., Verbal-Imager, Wholist-Analyst, Limited-Enhanced cognitive processing ability).

7.3 Experimental Procedures

In this section we describe the overall method and experimental procedure of several user studies conducted that aimed to investigate the effects of users' cognitive differences in information processing, on preference and task performance related to different designs of user authentication and CAPTCHA mechanisms.

All studies followed a two-phase methodology, in which the users first interacted with the developed psychometric tests to elicit their cognitive processing styles and abilities (*user modeling phase*), and further interacted with various types of user authentication and CAPTCHA mechanisms as part of real-life tasks (*user interaction phase*). In particular, for the user modeling phase, with the aim to apply the psychometric tests in a scientific right manner, we conducted several controlled laboratory sessions with a maximum of 10 participants by following the protocols 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 characteristics. For the purpose of the study, in order to proceed with next phase, all participants interacted first with the user modeling module in order to elicit the values of the psychometric tests for all users and further perform a cluster analysis for mapping each security type to users based on the generated clusters and the particular design of the user study. The clustering algorithm was applied on an existing representative sample with undergraduate students of the same universi-

ty whose cognitive characteristics were elicited in past user studies of our research laboratory. Next, users interacted with a particular security mechanism and the corresponding mapped design factors (e.g., text vs image).

The participation in all user studies was voluntary and all individuals agreed to an online consent form before participating. In particular, participants were informed that the data they provided and their interactions with the system would be processed and used anonymously as part of an experimental user study of the researchers' group. No further details about the aim of the study, nor the type of interaction data recorded (e.g., time to complete a CAPTCHA challenge) were provided to the participants in order to avoid bias effects.

Further to this section we will present more specifically the investigated factors and security mechanisms, the individuals that participated in each study and the analysis of results. Throughout the studies, the familiarity factor of our sample in text-based passwords and text-recognition CAPTCHA challenges should be carefully considered when interpreting the results, since all participants of all studies have experience in text-based than image-based security mechanisms.

7.3.1 Procedure followed for User Authentication-related Studies

The studies that were related to the user authentication mechanisms embraced a between-subject design, aiming to examine whether cognitive characteristics of users affect preference and performance (task efficiency and effectiveness) on different types of user authentication; text-based and graphical, and different complexity levels; baseline and higher complexity.

The user studies were typically applied in the frame of a university Computer Science course in which students would authenticate through a login form for accessing their daily course's material (i.e., daily lab exercise). Main aim of this process was to increase the ecological validity of the users' interactions with the authentication mechanism since the Web-site would be used by the students in a real-life scenario to view and download information about their course.

Participants initially enrolled in the course's Web-site through a registration form. Depending on the aim of each study, the user authentication types were either provided randomly to each user, or a matched and mismatched condition was randomly assigned to specific 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, following a particular theoretical hypothesis, in case of a matched condition, a 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. Furthermore, in cases where the aim was to study the effect of cognitive factors on user authentication type (text and image), the complexity level of each authentication key was the same (e.g., text passwords: 8 alphanumeric characters with the same requirements of upper-case, lower-case letters, special characters, etc.; graphical

authentication: 5 out of 25 images). On the other hand, in cases where the aim was to study the effect of cognitive factors on authentication complexity, the type (text-based or graphical) was controlled and the complexity level was balanced across users.

7.3.2 Procedure followed for CAPTCHA-related Studies

The studies that were related to the CAPTCHA mechanisms embraced a between-subject design, aiming to examine whether cognitive characteristics of users affect preference and performance (task efficiency and effectiveness) on different types of CAPTCHA challenges; text-recognition and image-recognition, and different complexity levels; baseline and higher complexity.

The user studies were typically applied in the frame of a real-life task of a university Computer Science course, e.g., as part of students' enrolment in the course's Web-site, or as part of downloading material from the course's Web-site. Main aim of this process was to increase ecological validity of the studies since the CAPTCHA challenges were solved as secondary tasks within real-life tasks of the users.

The participants interacted with the CAPTCHA mechanisms that were embedded in a Web-page. Depending on the aim of each study, the CAPTCHA types were either provided randomly to each user, or all variations of CAPTCHA (i.e., text- vs. image-recognition) were provided for users to choose which CAPTCHA challenge to solve in order to elicit their preference. Furthermore, in cases where the aim was to study the effect of cognitive factors on CAPTCHA type (text and image), the complexity level of each CAPTCHA challenge was the same (i.e., 8 characters with the same percentage of noise and distortion was used in the text-recognition challenge, whereas 12 colored images were used in the image-recognition challenge). On the other hand, in cases where the aim was to study the effect of cognitive factors on CAPTCHA complexity, the type (text-recognition or image-recognition) was controlled and the complexity level was balanced across users.

7.3.3 Data Recording

In all studies, client-side and server-side scripts were developed for measuring the users' interactions with the system. The data captured during the user studies are grouped as follows:

User Data consists of data about the users' individual cognitive processing characteristics. In particular, based on the users' interactions with the psychometric tests, users were classified as Verbals, Imagers (or Intermediates), Wholist, Analysts (or Intermediates), having limited or enhanced cognitive processing abilities. Furthermore, *user preference* was also collected typically at the end of the studies through semi-structured focus groups, through post-study questionnaires or

through users' explicit choice of a security type, aiming to elicit the users' subjective preference and perceptions regarding the various security mechanisms.

Task Data consists of data about the task performed by the users. This includes the type of user authentication (text or graphical), the type of CAPTCHA (text or image), the level of complexity (baseline or higher), the total time to complete the security task (in seconds) and total number of attempts to successfully complete the task. For total time to complete the task, in studies when users freely used the security mechanisms (i.e., when the frequency of access was not controlled), the task completion time for each participant was measured as the median time of all successful sessions for each of the conditions (Chowdhury et al. 2013). In these cases, 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) (Chowdhury et al. 2013). On the other hand, when the frequency of access was controlled, the actual time to complete the task was used or the repeated measures effect was considered for studies that entailed more than one sessions. Furthermore, based on the total number of attempts, the success rate (in percentage) of each session was also calculated. For example, a user that solved the challenge at first attempt had a success rate of 100%, whereas a user that solved the challenge at third attempt (the first and second attempt failed and the third succeeded) had a success rate of 33%. Failure rate was also calculated which is considered as the total number of sessions that included a failed attempt, divided by the total number of all sessions (Brostoff and Sasse 2000). A session is considered as failed in case the participant needed more than one attempt to successfully authenticate. Additional data were recorded such as the total number of authentication key resets and the number of times a CAPTCHA challenge was refreshed (in which a new challenge was reloaded). Finally, in some studies, the generated text-based and graphical authentication keys were gathered in plaintext in order to perform a security analysis and accordingly contextualize the usability evaluation results. To avoid security and privacy issues related to the generated keys of the users, the plaintext authentication keys were anonymously stored in a separate database (along with the assigned user classification and assigned conditions), than the actual system's database which encrypted the authentication keys accordingly. As such, the plaintext could not be correlated to any actual user.

In the analyses, the total time, number of attempts, success rate, failure rate, number of authentication key resets, and number of refreshes are the dependent variables, whereas the users' cognitive styles, cognitive processing abilities, type of user authentication, type of CAPTCHA and the level of complexity are the independent variables. Finally, in some studies, the generated text-based and graphical authentication keys were gathered in plaintext in order to perform a security analysis and accordingly contextualize the usability evaluation results. To avoid security and privacy issues related to the generated keys of the users, the plaintext authentication keys were anonymously stored in a separate database (along with the assigned user classification and assigned conditions), than the actual system's database which encrypted the authentication keys accordingly. As such, the

plaintext could not be correlated to any actual user. Table 4 illustrates the variables used in the analyses.

Table 4. Variables used in the analysis.

Data Categories	Variables
User Data	Cognitive styles (Verbal/ Imager/ Intermediate) Cognitive styles (Wholist/ Analyst/ Intermediate) Cognitive processing abilities (limited/ enhanced) Preference (nominal)
Task Data	Type of User Authentication (text/ graphical) Type of CAPTCHA (text/ image) Level of complexity (baseline/ higher) Authentication key creation (seconds) Anonymous plaintext authentication key (characters) Total time to complete (seconds) Number of attempts (ordinal) Success rate (percentage) Failure rate (percentage) Number of CAPTCHA refreshes (ordinal)

7.4 Investigate the Effect of Verbal/ Imager Cognitive Styles on User Preference and Performance of User Authentication Type

Main aim of this section is to present a study that investigated the effect of cognitive styles (Verbal/ Imager) on user preference and performance of user authentication types (textual vs. graphical). In this study we followed a match-mismatch approach, testing the hypothesis that the matched (in contrast to the mismatched) user authentication type would improve task performance and user preference. Matched condition means providing a text-based password mechanism to Verbal users and graphical authentication mechanism to Imager users, whereas the mismatched condition the opposite. The condition was based on an early study that showed a significant main effect of users' cognitive styles on user preference and performance of different types of user authentication (Belk et al. 2013c). The study was conducted with a total of 153 participants (43.79% male, 56.21% female, age 17-22) for a four month period. Participants were undergraduate students of Psychology and Social Science Departments. The sample included users that were rather experienced and average than novice users with respect to user authentication and therefore, the research design was setup in order to avoid inference errors. 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.

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 three months of the study, excluding the user interactions of the last month. In particular, the users' interactions with the assigned security mechanisms were recorded for a period of three 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 that 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.

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 differences between ordinal data (authentication key requests), and the Chi-square 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 analyze and discuss findings of each measure.

7.4.1 User Groups

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 that belong to the Verbal and Imager class, respectively. 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 5). 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.

Table 5. 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

7.4.2 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 7 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 Analysis of Variance was run to determine if there were differences in key length between Verbal and Imager users per user authentication type. The test revealed that there were no significant differences in key length among 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 seconds (SD=9.20) to successfully create a text-based password key, while Imagers spent on average 36.04 seconds (SD=9.65). Regarding the graphical authentication key creation, Verbals spent on average 87.01 seconds (SD=25.17) to successfully create a graphical authentication key, while Imagers spent on average 79.55 seconds (SD=28.19). A two by two way factorial Analysis of Variance did not reveal significant differences in regards with time spent for creating an authentication key between Verbals and Imagers and user authentication type (F(1,153)=1.387, p=0.241).

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

7.4.3 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 **6** summarizes the login time measures per cognitive styles group and user authentication type.

Table 6. Login time measures

Time Spent	Verbals		Imagers	
	Textual (p)	Graphical (np)	Textual (np)	Graphical (p)
Overall Login	12.54	14.46	14.28	13.14
Username	1.79 (0.83)	1.59	1.73	1.84
First to Last	9.26	11.17	10.98	9.84
Between Clicks	1.08	1.37	1.31	1.2

** p: personalized condition, np: non-personalized condition*

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 41 illustrates the means of performances for each condition.

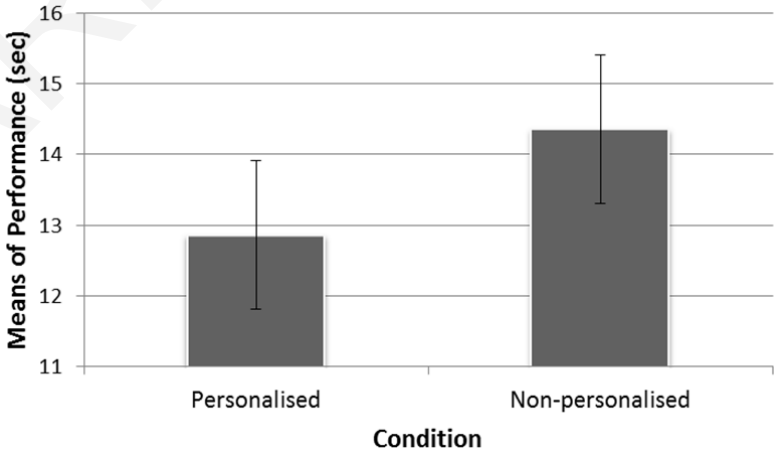


Figure 41. Means of overall login time per personalization condition

Furthermore, a two by two way factorial Analysis of Variance 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 42 illustrates the means of performances of each cognitive style group and authentication types.

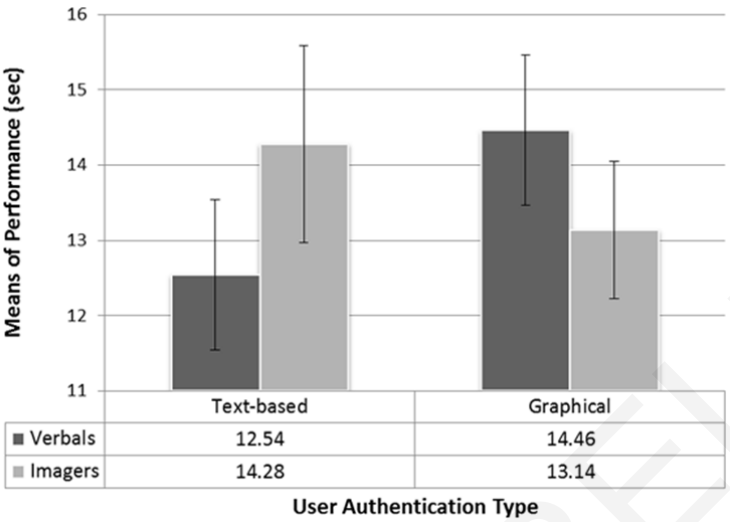


Figure 42. Means of overall login time per cognitive style group and authentication type

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 to Imagers that had a mean of 14.28 seconds ($MD=1.746$, $SE=0.263$; $F(1,149)=44.123$, $p<0.01$). Similarly, in the case of user interactions with the graphical authentication mechanism, significant differences were observed with Imagers having a mean of 13.14 seconds (the graphical authentication mechanism being the personalized condition for Imagers), compared to Verbals that had a mean of 14.46 seconds ($MD=1.318$, $SE=0.264$; $F(1,149)=24.850$, $p<0.01$). 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 to 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 to 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.

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 Analysis of Variance revealed that 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 ($F(1,153)=1.144$, $p=0.287$). Given that the username length was the same for all users (7 characters long university identity number), such a result was expected.

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 analyzed with the aim to investigate differences in authentication key recall time between cognitive style groups and authentication types. A two by two factorial Analysis of Variance 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 which supports that individual differences in cognitive styles affect task efficiency of particular types of authentication mechanisms.

Learning Effects on Task Efficiency

The impact of trials was analyzed on the overall login time aiming to investigate whether learning effects exist and whether they correlate to 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 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). Figure 43 and Figure 44 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: $F(2, 149)=1.391$, $p=0.184$).

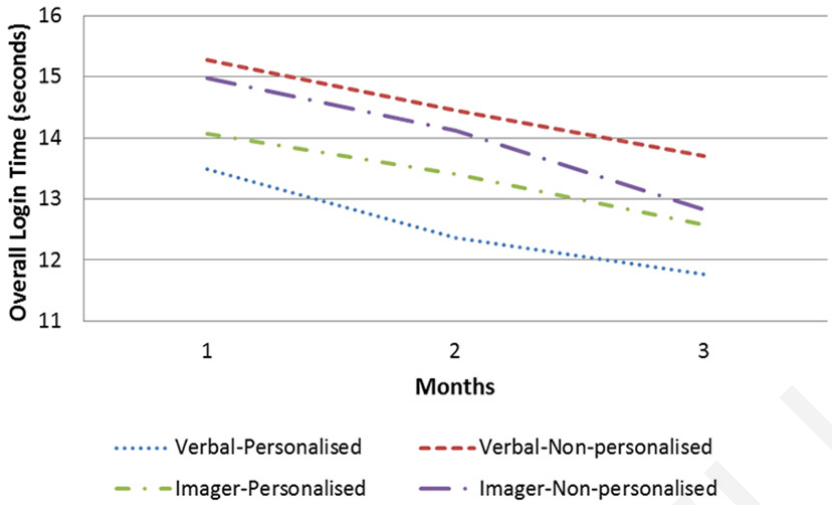


Figure 43. Means of overall login time per cognitive style group and authentication type over three months

In the monthly comparison we have observed a decline of login time throughout the three months for all users, with all cognitive style groups having steady differences, i.e., Verbals that received a personalized condition were every month faster at login, followed by Imagers with a personalized condition and then respectively with Imagers and Verbals that 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 that received a personalized condition spent the lowest time throughout all the twelve weeks.

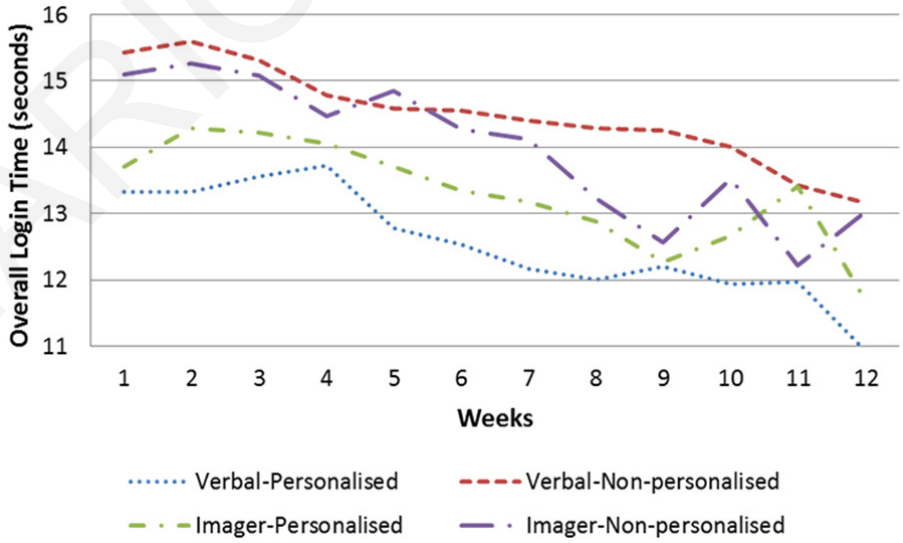


Figure 44. Means of overall login time per cognitive style group and authentication type over twelve weeks.

7.4.4 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.

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 to non-personalized user authentication tasks.

Furthermore, a two by two way factorial Analysis of Variance was conducted using cognitive styles (Verbal and Imager) and user authentication type (text-based and graphical) as independent variables and user authentication success rate as the dependent variable. Figure 45 illustrates the success rate per cognitive style group and authentication type.

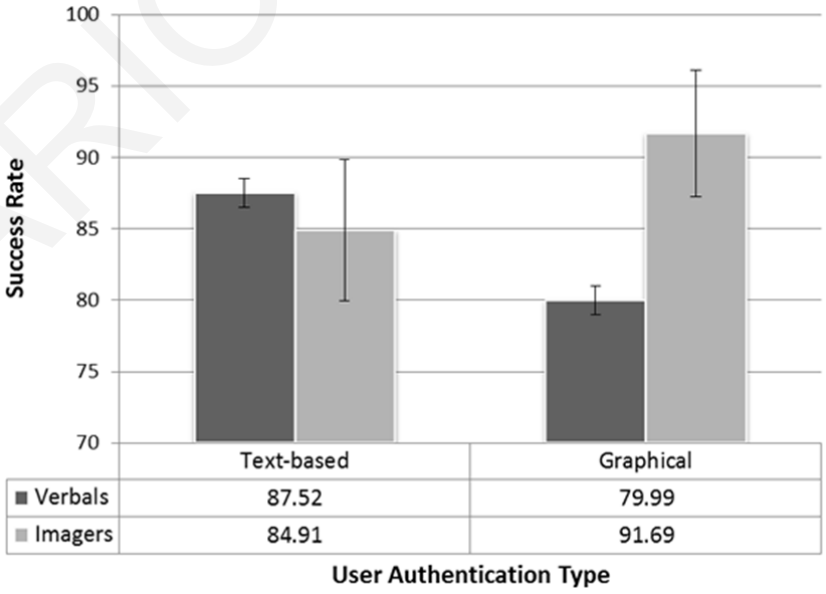


Figure 45. Success rate per cognitive style group and authentication type

Results revealed a main interaction effect between cognitive styles and user authentication type on 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 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).

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 to 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). Figure 46 and Figure 47 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.

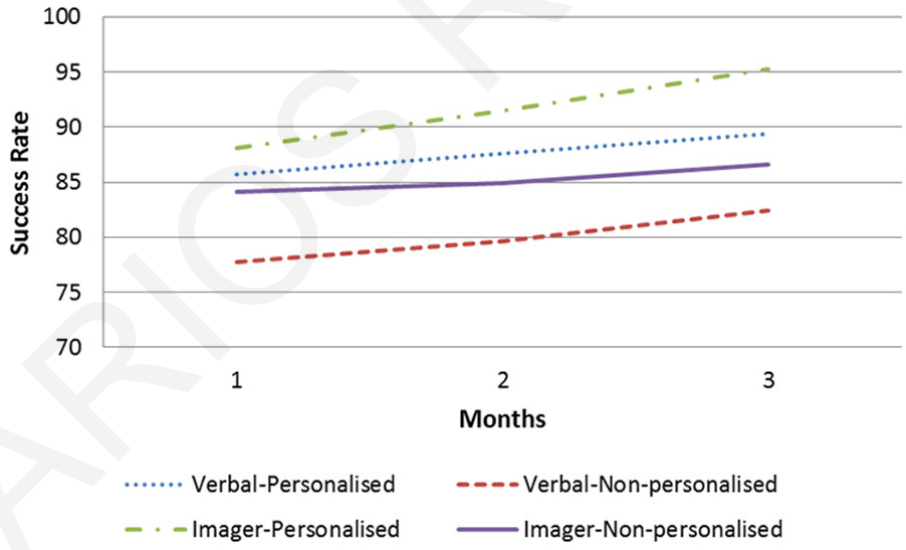


Figure 46. Success rate per cognitive style group and authentication type over three months

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).

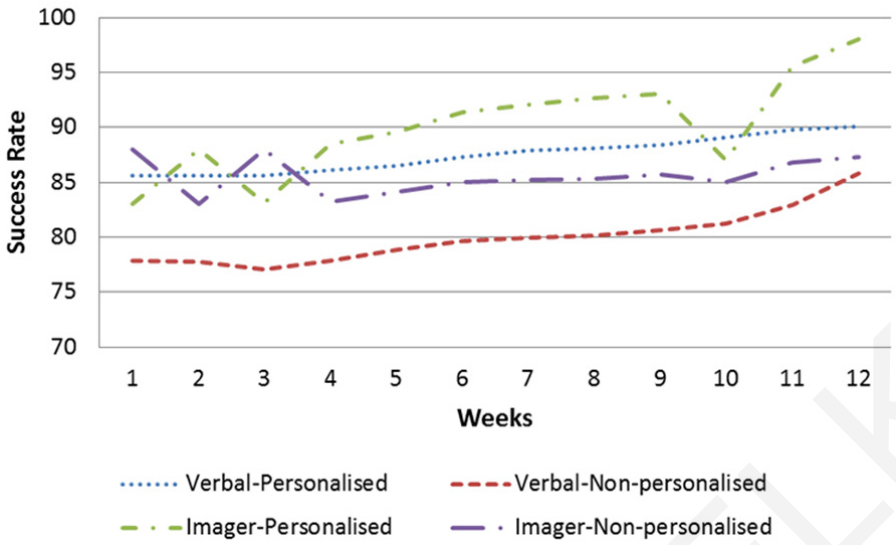


Figure 47. Success rate per cognitive style group and authentication type over twelve weeks

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 that received a non-personalized condition (graphical) had the lowest success rate throughout the twelve 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 to 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 four weeks. After the four weeks however, Imagers that 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 Imagers, initial trials did not reveal clear differences between success rates, however with more trials Imagers had significantly higher success rates compared to the non-personalized condition.

Authentication Key Resets

The number of authentication key resets was counted. Table 7 summarizes the total number of authentication key requests per cognitive styles group and condition. We conducted the rank-based nonparametric Mann-Whitney U test to determine if there were differences in authentication key requests between personalized and non-personalized conditions. The test revealed no significant differences in number of authentication key requests between the groups (U=1, z=-0.775, p=0.439).

Table 7. 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
Month3	2	3	3	5	13
Total	6	13	7	12	38

** p: personalized condition, np: non-personalized condition*

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 if there were differences in number of authentication key requests between the two user authentication conditions. The test revealed no significant differences in 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.

7.4.5 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 approximately 20 minutes. 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; (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 repre-

sent their first and second choice. Table 8 lists the number of participants who chose a specific method as their first choice for each factor.

Table 8. Participants who chose a specific authentication type as their first choice for each evaluation factor. Numbers in italic revealed significant differences between the two methods for each 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

** p: personalized condition, np: non-personalized condition*

Factor 1 - Authentication Preference

There is 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 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.

Factor 2 - Authentication Efficiency

Similarly, there is 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 to 7 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.

7.4.6 Main Findings

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 four months. The results of this study can be interpreted under the light of cognitive styles' theory as they demonstrate a **main effect of cognitive styles on both performance and preference related to authentication mechanisms. Results have shown that users of a particular cognitive style (Verbal or Imager) prefer and perform differently on text-based and graphical-based user authentication tasks. In graphical authentication, Imagers perform significantly faster than Verbals**, whereas in text-based authentication, Verbals performed faster than Imagers. Regarding effectiveness, no safe conclusions can be drawn at this time whether they are significantly affected by cognitive styles since in both user groups, most of the users completed the authentication task at first attempt. **Furthermore, participants in general preferred graphical authentication mechanisms; with the Imager group significantly preferring graphical authentication mechanisms.** Based on the results of this study, along with the results reported in Belk et al. (2013c), we summarize below the main findings and conclusions derived from the studies:

- Imagers performed significantly faster in graphical authentication than Verbals did, however in the case of text-based passwords performance of both cognitive style groups was not considerably different, with Verbals being faster than Imagers based on descriptive sta-

tistics. An interpretation of this result can be based on the fact that all users were more familiar and experienced interacting with text-based passwords, hence no significant difference was observed between the Verbal and the Imager. On the other hand, since the familiarity factor did not affect the graphical authentication mechanism, we have observed that the visual approach of processing and organizing information of the Imagers has positively affected their performance compared to the Verbals.

- Regarding effectiveness, we conclude that both authentication mechanisms were effective in use throughout the study. Nevertheless, both number of attempts and number of authentication key resets reveal that graphical authentication mechanisms have positively affected users belonging to the Imager class as they needed less attempts and key resets in graphical authentication mechanisms compared to Verbal users.
- Participants in general preferred graphical authentication mechanisms. Results also demonstrate that users categorized in the Imager group prefer graphical authentication mechanisms. A possible interpretation of this result might be based on the novelty effect of graphical authentication. However, results suggest that if this would be the main factor that influences users' preference then it would be observed across all user groups regardless their cognitive style, which in the current sample is not the case, since users categorized into the Verbal group did not significantly prefer a particular authentication type.

7.5 Investigate the Effect of Wholist/ Analyst Cognitive Styles on User Performance of User Authentication Type and Device Type

This section presents a user study that aimed to investigate the effect of users' cognitive styles (Wholist/ Analyst), on task completion efficiency and effectiveness of two complementary types of user authentication mechanisms (textual and graphical), and how the device type used for interaction (standard desktop and mobile touch-based device) affects these parameters. For the purpose of this study we have used an alternative cognitive style elicitation test; the pioneer Witkin's GEFT paper-and-pencil test. The selection of the GEFT was based on a high number of researchers that have correlated the Wholist/ Analyst dimension to Witkin's field dependence-independence and have used the tests and terms interchangeably in various user studies (Ling and Salvendy 2009; Chen and Liu 2008; Kinley et al. 2014; Clewley et al., 2011; Warner and Demick 2009). In particular, Wholist users are correlated with field dependence (FD), whereas Analyst users are correlated with field independence (FI).

7.5.1 User Groups

A total of 164 user accounts have been created during the enrolment phase. Based on the users' scores on the GEFT, 78 participants were classified as FD and 86 participants were classified as FI. Figure 48 illustrates the frequencies of users' scores on the GEFT. The mean score was 10.95 correct items (*SD*=3.91). The lowest GEFT score was 3 correct items and the maximum 17 correct items.

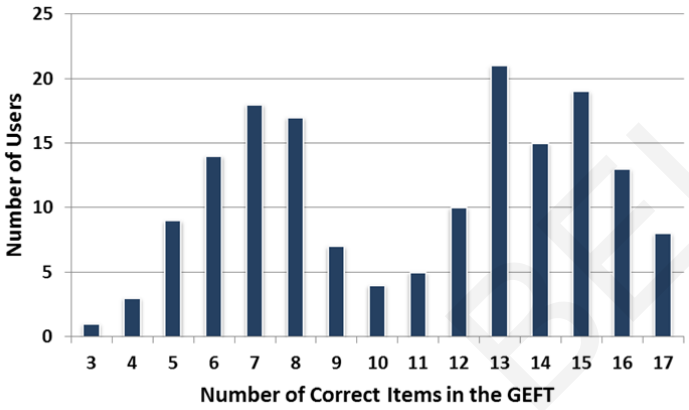


Figure 48. Frequencies of users' scores on the GEFT

Throughout the period of the study, 3674 authentication sessions have been recorded. A mean of 22.4 sessions were recorded per user (*SD*=1.65; *MIN*: 15; *MAX*: 24) along the three months (two sessions per week). Table 9 summarizes the number of authentication sessions per group for all combinations of field dependence-independence groups, user authentication type and device type.

In the analysis that follows, we used as independent variables, field dependence-independence (FD or FI), user authentication type (textual or graphical) and device type (desktop or touch), and as dependent variables the time to successfully authenticate (task completion efficiency) and failure rate (task completion effectiveness).

Table 9. Number of authentication sessions per group combination.

	Textual		**Graphical**	
	Desktop	**Touch**	**Desktop**	**Touch**
FD	426 (11.59%)	441 (12%)	428 (11.65%)	460 (12.52%)
FI	478 (13.01%)	475 (12.93%)	473 (12.87%)	493 (13.42%)

The familiarity factor of our sample in using text-based passwords should be carefully considered when interpreting the results, since all participants have prior experience with text-based password mechanisms, and no prior experience with recognition-based graphical authentication mechanisms.

7.5.2 Task Completion Time Comparisons

A three-way factorial analysis of variance (ANOVA) was conducted aiming to examine main effects and interactions between users' field dependence-independence (FD and FI), user authentication type (textual and graphical) and device type (desktop and touch) on the time needed to successfully authenticate. Figure 49 illustrates the means of task completion time (seconds) and between-subjects effects of field dependence-independence (FDI), user authentication type (UA) and device type (Device) on time to successfully authenticate.

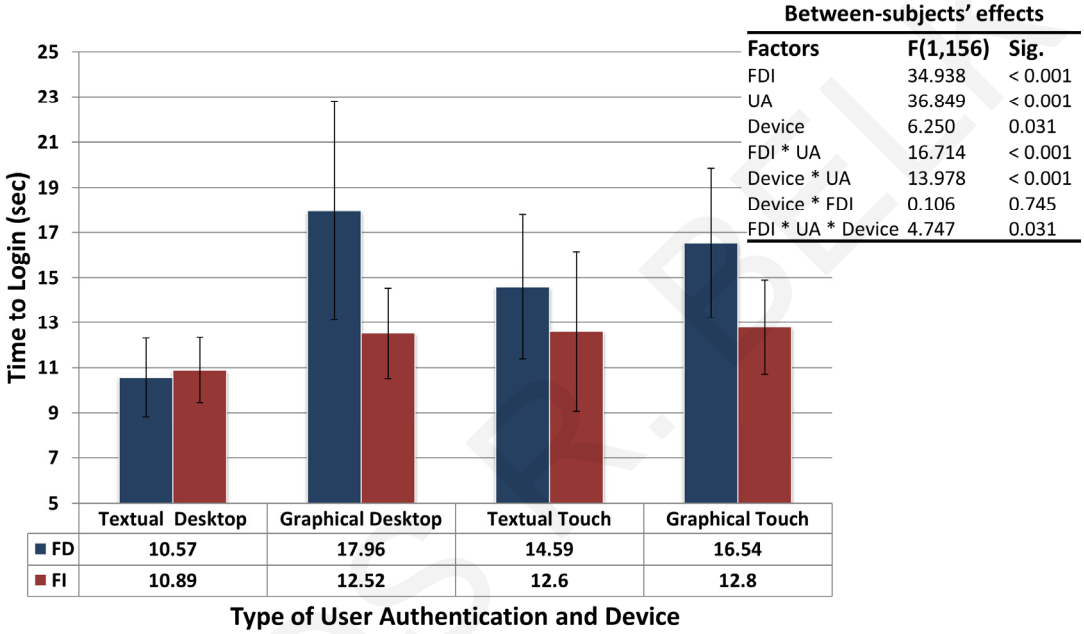


Figure 49. Means of task completion time per field dependence-independence group, user authentication type and device type

Main Effects of Single Factors on Task Completion Time

The analysis revealed that there is a main effect of users' field dependence-independence on time needed to authenticate ($F(1,156)=34.938$, $p<0.001$, *partial* $\eta^2=0.183$). FI users were significantly faster in completing the authentication task than FD users. Furthermore, the authentication type (textual vs. graphical) has a main effect on authentication task completion time ($F(1,156)=36.849$, $p<0.001$, *partial* $\eta^2=0.191$). Interactions with textual password mechanisms were more efficient than graphical authentication mechanisms. Finally, there was an effect of the device type towards time needed to authenticate ($F(1,156)=6.250$, $p<0.02$, *partial* $\eta^2=0.039$). Desktop-based user interactions were significantly faster than touch-based interactions.

Main Interaction Effects of Field Dependence-Independence and User Authentication Type on Task Completion Time

There was a statistically significant interaction effect between users' field dependence-independence and user authentication type ($F(1,156)=16.714$, $p<0.001$, *partial* $\eta^2=0.097$). Pairwise comparisons between FD and FI users revealed that in the case of graphical authentication mechanisms, FI users significantly outperformed FD users in task completion time (FD-FI: $MD=4.596$, $SE=0.65$; $F(1,156)=49.991$, $p<0.001$, *partial* $\eta^2=0.243$). In the case of textual password mechanisms, no significant differences in task completion time were recorded (FD-FI: $MD=0.838$, $SE=0.65$; $F(1,156)=1.661$, $p>0.05$, *partial* $\eta^2=0.011$). A possible interpretation of the latter result might be based on the fact that all users were familiar with textual password mechanisms since the sample included experienced users and all of them had already registered in at least one online password protected account in the past. Furthermore, pairwise comparisons between user authentication types for each user group revealed the following: for FD users, significant differences in task completion time were observed between textual and graphical authentication mechanisms (FD: Textual-Graphical: $MD=-4.67$, $SE=0.66$; $F(1,156)=49.196$, $p<0.001$, *partial* $\eta^2=0.24$). In particular, FD users were significantly faster in authenticating on textual passwords compared to graphical authentication mechanisms. In the case of FI users, no significant differences were observed between the two authentication types since FI users were more efficient in authenticating through graphical authentication mechanisms compared to FD users (FI: Textual-Graphical: $MD=-0.911$, $SE=0.634$; $F(1,156)=2.065$, $p>0.05$, *partial* $\eta^2=0.013$).

Main Interaction Effects of Device Type and User Authentication Type on Task Completion Time

The analysis revealed a statistically significant interaction between device and authentication type on the time to authenticate ($F(1,156)=13.978$, $p<0.001$, *partial* $\eta^2=0.082$). Pairwise comparisons of user authentication types revealed that text-based and graphical authentication interactions on standard desktop computers had significant differences in task completion time (Desktop: Textual-Graphical: $MD=-4.509$, $SE=0.65$; $F(1,156)=48.109$, $p<0.001$, *partial* $\eta^2=0.236$), whereas in the case of touch-based interactions, no significant differences where observed between the two user authentication types (Touch-based: Textual-Graphical: $MD=-1.072$, $SE=0.65$; $F(1,156)=2.718$, $p>0.05$, *partial* $\eta^2=0.017$). The latter result has been caused by the significant increase of time to complete the text-based authentication task on touch-based devices as revealed by a pairwise comparison of device type which showed that text-based passwords were completed significantly faster on standard desktop computers compared to touch-based devices (Text-based: Desktop-Touch: $MD=-2.868$, $SE=0.65$; $F(1,156)=19.461$, $p<0.001$, *partial* $\eta^2=0.111$). In contrast, in graphical au-

thentication no significant differences were observed between desktop and touch-based interactions (Graphical: Desktop-Touch: *MD*=0.569, *SE*=0.65; $F(1,156)=0.767$, $p>0.05$, *partial* $\eta^2=0.005$).

Main Interaction Effects of Field Dependence-Independence, User Authentication Type and Device Type on Task Completion Time

The analysis revealed a statistically significant three-way interaction between users' field dependence-independence, user authentication type and device type ($F(1,156)=4.747$, $p<0.04$, *partial* $\eta^2=0.03$). Next, a simple two-way interaction was carried out to determine the statistical significance of the simple two-way interaction (authentication type*device type) for FD users and for FI users. There was a statistically significant simple two-way interaction between user authentication type and device type for FD users ($F(1,156)=16.693$, $p<0.001$, *partial* $\eta^2=0.097$), but not for FI users ($F(1,156)=1.279$, $p>0.05$, *partial* $\eta^2=0.008$). Given the statistically significant simple two-way interaction, we followed these with simple main effects. We investigated the effect of device type at every level of user authentication type. There was a statistically significant simple main effect of device type for FD users in text-based password authentication ($F(1,156)=18.219$, $p<0.001$, *partial* $\eta^2=0.105$), but not for FD users in graphical authentication ($F(1,156)=2.279$, $p>0.05$, *partial* $\eta^2=0.014$). All simple pairwise comparisons were run for FD users in text-based interactions with a Bonferroni adjustment applied. Time to authenticate in desktop-based interactions was 10.57±1.74 seconds and 14.59±3.21 seconds in touch-based interactions, a statistically significant difference of 4.019 seconds (95% Confidence Interval, 2.159 to 5.879), $p<0.001$. Such a result provides initial evidence that the device type affects FD users when interacting with text-based passwords since the shift from a standard keyboard to a virtual keyboard significantly affects the users' visual field and context of use.

Over Time Effects on Task Completion Time

The task completion time was analyzed per month aiming to investigate the impact of experience on time to complete the authentication task. A Repeated Measures Analysis of Variance (ANOVA) was conducted on the time to authenticate over the period of three months. Figure 50 illustrates the task completion time comparison between FD and FI users for all combinations.

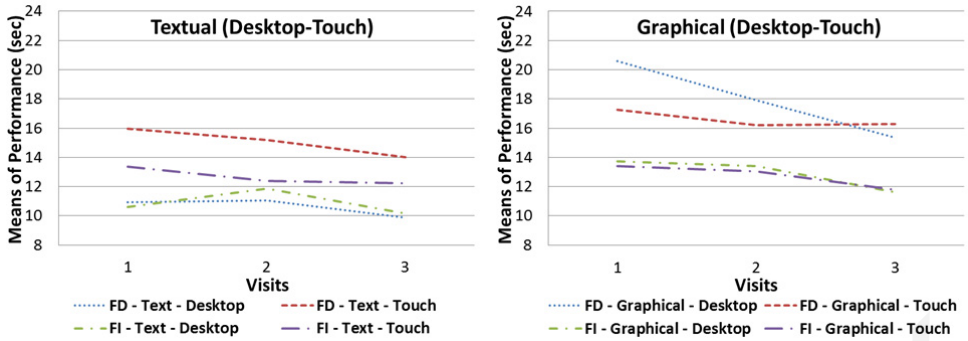


Figure 50. Task completion time comparison between FD and FI users for all combinations of user authentication and device types over a three month period

The analysis revealed a main effect of monthly trials on the time to successfully authenticate indicating that task completion efficiency improves as users gain more experience with the user authentication mechanisms and the device ($F(2,312)=37.043$, $p<0.001$, *partial* $\eta^2=0.192$). Descriptive statistics reveal that in text-based password interactions (Figure 50, left), FD users recorded consistently the highest times to authenticate on touch-based devices across the three months (FD-Text-Touch), compared to all other combinations (FD-Text-Desktop, FI-Text-Desktop, FI-Text-Touch). Such a result further indicates the increased difficulty of FD users in interacting with text-based passwords on touch-based devices due to the interaction shift from standard keyboard input to touch-based virtual keyboard input. Furthermore, graphical-based interactions (Figure 50, right) revealed that FD users recorded consistently the highest times to authenticate on both desktop-based and touch-based devices throughout the three months compared to FI users, indicating their increased difficulty, compared to FI users, in completing the graphical authentication task.

7.5.3 Failure Rate Comparisons

The number of sessions with failed attempts was counted. A session is considered as failed in case the participant needed more than one attempt to successfully authenticate. For example, in case the participant needed three attempts to authenticate (i.e., the first and second attempt failed and the third succeeded), this session is considered as failed. In contrast, a session is considered as successful when the participant authenticated successfully in the first attempt. The failure rate of each user was calculated as the number of failed sessions divided by all sessions of the user. Among 3674 user authentication sessions, 503 attempts failed (13.69% overall failure rate). Table 10 summarizes the total number of sessions with failed attempts, categorized by field dependence-independence group, user authentication type and device type.

We conducted a three-way factorial analysis of variance (ANOVA) aiming to examine main effects and interactions between users' field dependence-independence (FD and FI), user authentication type (textual and graphical) and device type (desktop and touch) on the failure rate (percentage). The analysis revealed that field dependence-independence has a main effect on failure rate

$F(1,156)=5.222$, $p<0.03$, *partial* $\eta^2=0.032$), as FI users needed less attempts to authenticate than FD users. Furthermore, a main effect of user authentication type on failure has been identified $F(1,156)=4.807$, $p<0.04$, *partial* $\eta^2=0.03$), since users scored higher failure rates on graphical authentication than text-based authentication. Furthermore, the analysis revealed that FD users had high failures rates in graphical authentication on both desktop and touch-based devices. In particular, 33.8% of all failed attempts (15.9% on desktop computers, 17.89% on touch-based devices) were caused by FD users interacting with graphical authentication mechanisms.

Table 10. Sessions with failed attempts per user field dependence-independence group, user authentication and device type

	Textual		**Graphical**	
	Desktop	**Touch**	**Desktop**	**Touch**
FD	48 (9.54%)	59 (11.73%)	80 (15.9%)	90 (17.89%)
FI	53 (10.54%)	55 (10.93%)	71 (14.12%)	47 (9.34%)
Total	101 (20.08%)	114 (22.66%)	151 (30.02%)	137 (27.24%)

7.5.4 Authentication Key Resets

The total number of authentication key resets was counted along the study. Table 11 summarizes the total number of authentication key requests per user field dependence-independence groups and user authentication type.

Table 11. Number of authentication key resets.

	Textual	**Graphical**
FD	5	10
FI	3	7
Total	8	17

In total, 25 authentication key requests were initiated throughout the study, among those requests, 4 users requested the authentication key reset two times, and the rest users requested the key reset 1 time. Table 11 reveals a higher number of authentication key resets in graphical authentication across user groups compared to text-based password. The non-parametric Mann-Whitney U test did not reveal significant differences in authentication key requests between all combinations of field dependence-independence and user authentication type.

7.5.5 Users' Perceived Usability

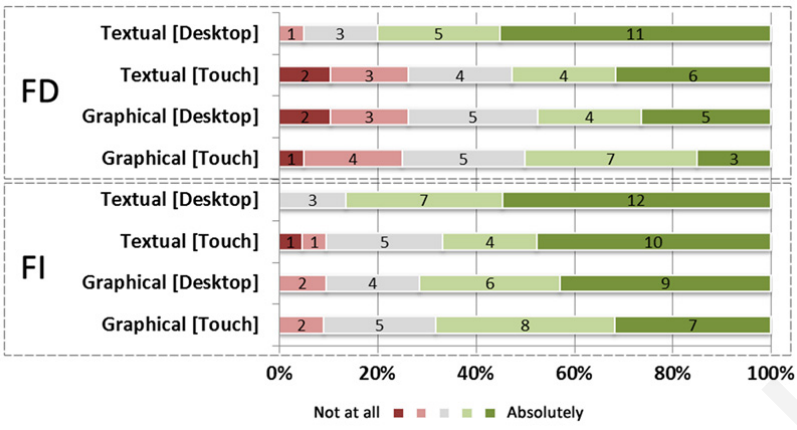
At the end of the study, we conducted a survey aiming to validate findings of the quantitative analysis as well as to enrich our understanding about the users' perceptions, perceived usability and

memorability based on their interactions with the authentication mechanisms during Phase B. The survey investigated the following factors: (i) Perceived speed; (ii) perceived ease-of-use; and (iii) perceived memorability. Example statements of the survey were: *"The [device x authentication] is easy to use"* and *"The [device x authentication] is fast to use"*, where device and authentication was respectively the device and authentication type used by each particular user. Users rated the statements through a 5-point Likert scale (1: Not at all – 5: Absolutely).

In the analysis that follows, the non-parametric Mann-Whitney U test was run on specific group combinations (field dependence-independence X user authentication type X device type) in order to correlate these with the main findings of the quantitative analysis, aiming to increase the internal validity and triangulate the results of the study.

Effects of User Authentication and Device Type on Perceived Speed

A high number of participants rated the authentication mechanisms as fast to use (65.85%), whereas 20.73% rated these as neutral (Figure 51). Among the FD user group, a high number of participants rated the graphical authentication mechanism as inefficient to use (12.82%). In addition, a considerable high number of FD users rated touch-based interactions (both text-based and graphical) as not fast to use (12.82%). The Mann-Whitney U test was run in order to determine if the users' responses significantly differ between specific groups. The results revealed that a high number of FD users rated text-based passwords as faster to use on desktop computers than touch-based devices, however, these differences were not significant (U=124.5, z=-1.942, p=0.065). Furthermore, comparisons between text-based passwords and graphical authentication on desktop computers revealed that FD users rated text-based passwords as faster to use (U=112.5, z=-2.283, p<0.05). In contrast, in the case of FI users no significant differences in ratings were observed between all combinations. The results further support the quantitative measures since FD users recorded high times in completing the graphical authentication task across device, and text-based passwords that were deployed on touch-based devices. In contrast, as revealed through the quantitative analysis, FI users did not score significant differences in ratings between user authentication types and device types.



Mann-Whitney U test statistics

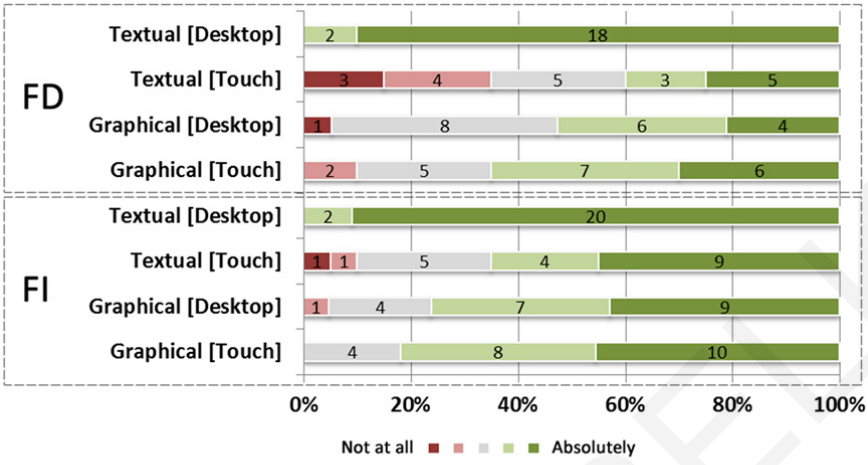
Group 1	Group 2	U	z	p
FD-Textual-Desktop	FD-Textual-Touch	124.5	-1.942	0.065
FD-Textual-Desktop	***FD-Graphical-Desktop***	***112.5***	***-2.283***	***0.028***
FI-Textual-Desktop	FI-Graphical-Desktop	189	-1.106	0.269
FI-Textual-Desktop	FI-Textual-Touch	193.5	-0.992	0.321

Figure 51. Users' responses on the statement: *"The [device x authentication] is fast to use"*

Effects of User Authentication and Device Type on Perceived Ease-of-use

Analogous to perceived speed, the majority of participants (73.17%) agreed that the user authentication mechanisms they interacted with were easy to use. 18.9% provided a neutral rate whereas 7.92% stated that the user authentication mechanism was not easy to use. Among those negative statements, 5.48% (FD users: 7; and FI users: 2) were rated by participants that interacted with textual authentication mechanisms deployed on touch-based devices (Figure 52). The Mann-Whitney U test was run to determine whether differences exist between several groups on the users' responses regarding ease of use. The analysis further confirms that users (both FD and FI) had increased difficulties in text-based authentication on touch-based devices, compared to desktop computers, as significant differences were observed between desktop-based and touch-based interaction for both user groups. In particular, FD users had significant more positive rates on desktop-based interactions than touch-based interactions (U=58, z=-4.281, p<0.001), so did FI users (U=112, z=-3.331, p<0.02). Furthermore, comparisons of graphical authentication between FD and FI users revealed no significant differences in user responses for both desktop-based and touch-based interactions. Comparisons between text-based and graphical authentication mechanisms that were deployed on desktop computers revealed that in both FD and FI user groups, text-based passwords were rated as more easy-to-use (FD: U=50, z=-4.388, p<0.001; FI: (U=115, z=-3.409, p<0.02). Such results indicate that although FI users were significantly more efficient and effective in graphical authentication than FD users, their scores in perceived ease of use did not significantly differ. Furthermore, FI users perceived text-based passwords as more easy-to-use than graphical authentication in desktop-based interactions, although the quantitative analysis revealed that FI

users interacted similarly well on both mechanisms. In the same line, for text-based passwords deployed on touch-based devices, FI users had higher negative rates than in desktop-based interactions.



Mann-Whitney U test statistics

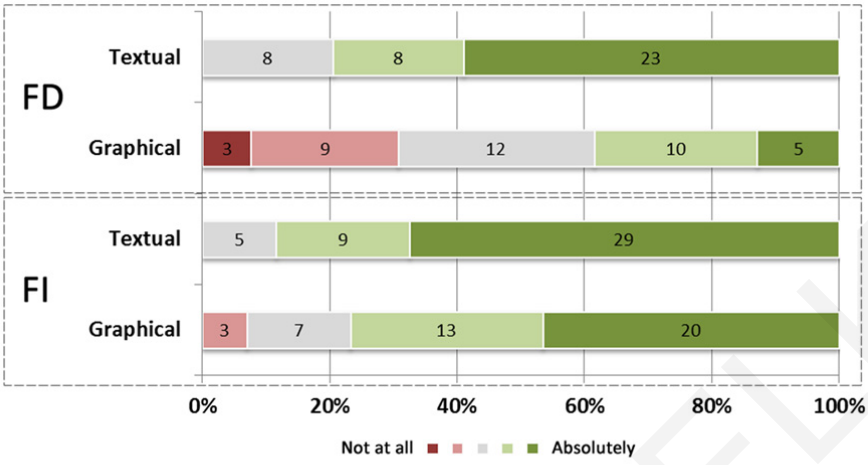
Group 1	Group 2	U	z	p
FD-Textual-Desktop	***FD-Textual-Touch***	***58***	***-4.281***	***<0.001***
FI-Textual-Desktop	***FI-Textual-Touch***	***112***	***-3.331***	***0.001***
FD-Graphical-Desktop	FI-Graphical-Desktop	141	-1.666	0.117
FD-Graphical-Touch	FI-Graphical-Touch	168	-1.388	0.165
FD-Textual-Desktop	***FD-Graphical-Desktop***	***50***	***-4.388***	***<0.001***
FI-Textual-Desktop	***FI-Graphical-Desktop***	***115***	***-3.409***	***0.001***

Figure 52. Users' responses on the statement: *"The [device x authentication] is easy to use"*

Effects of User Authentication Type on Perceived Memorability

Comparison of ratings were conducted across device types since the recall and memorability of authentication key is primarily affected by human cognitive functions and not task execution (Baddeley 1992; 2012). Therefore, we grouped the users' responses based on field dependence-independence and user authentication type across device types. The results can be interpreted based on the quantitative analysis (task completion time and failure rate) given that a considerable number of FD users rated graphical authentication keys as not memorable, in contrast to textual password mechanisms, where no user rated low memorability. Figure 53 depicts the users' ratings regarding the memorability of their user authentication key. In particular, a total of 9.14% rated the graphical authentication as not memorable, among them 7.31% were rated by FD users (12) and 1.82% by FI users (3). The Mann-Whitney U test revealed significant differences in memorability ratings between text-based passwords and graphical authentication across FD and FI users. In particular, a significant higher number of responses rated the text-based password as memorable in contrast to graphical authentication (FD: U=305.5, z=-4.732, p<0.001; FI: (U=711, z=-2.067, p<0.04). Furthermore, no significant differences were observed between FD and FI users in regards with memorability ratings in text-based passwords. On the other hand, a significant higher number

of FI users rated the graphical authentication as more memorable than FD users (U=421.5, z=-4.006, p<0.001).



Mann-Whitney U test statistics

Group 1	Group 2	U	z	p
FD-Textual	***FD-Graphical***	***305.5***	***-4.732***	***<0.001***
FI-Textual	***FI-Graphical***	***711***	***-2.067***	***0.039***
FD-Textual	FI-Textual	751.5	-0.944	0.354
FD-Graphical	***FI-Graphical***	***421.5***	***-4.006***	***<0.001***

Figure 53. Users' responses on the statement: *"The user authentication key is memorable"*

7.5.6 Main Findings

Results have shown several main effects between users' field dependence-independence, user authentication type and device type. **Regarding task completion time, FI users performed significantly different in graphical authentication than FD users**, whereas in the case of text-based passwords no significant differences were observed**. Furthermore, FD users performed significantly worse on graphical authentication that took place on desktop computers than text-based authentication**, whereas for FI users no significant differences were observed. **In the same line, FD users perform worse in text-based authentication when this takes place on touch-based devices, however, FI users perform similarly well on both types of devices. Finally, in general, users performed significantly better in text-based authentication when these were deployed on desktop computers**, but in the case of graphical authentication no significant differences were recorded. Next, we report the main findings and interpretations based on the analysis of results.

- Task completion time and failure rate in graphical authentication significantly differs between FD and FI users. Results have shown a main effect of field dependence-independence on graphical authentication. In particular, FI users needed significantly less time and less attempts to complete the graphical authentication task compared to FD

users across device type. An interpretation of these results could be based on the particular stimuli and interaction design of the graphical authentication mechanism, i.e., in the case of graphical authentication, homogeneous objects and structure/organization are illustrated to the users, in which the surrounding framework might dominate the perception of the aiming items within. Accordingly, when FD users interact with these types of stimuli, they might find it difficult to locate the information they are seeking because other information might mask what they are looking for. On the other hand, FI users find it easier to recognize and select the important information from its surrounding field due to their improved dis-embedding skills and visual search task abilities (Angeli et al. 2009). Furthermore, when information is presented in an ambiguous, unstructured format, FI users impose their own structure on the information, while FD users attempt to first understand and learn that information as it is presented and without restructuring it, which might explain the added difficulty and time in completing the graphical authentication task compared to FI users. This finding is also in accordance with previous research, which has shown that FI users have a tendency to use their own internal references whereas FD users rely more on external frames of reference (Chen and Liu 2008). Finally, given that FI users have an improved visual working memory in contrast to FD users (Miyake et al. 2001; Rittschof 2010), FI users might have been positively affected compared to FD users in graphical authentication tasks since the recognition and recall of images are primarily processed through the visual working memory sub-system (Baddeley 1992; 2012).

- Desktop-based graphical authentication is less usable than text-based authentication for FD users, but not for FI users. In line with the aforementioned finding, results revealed that in desktop-based interactions, FD users needed significantly more time and attempts to complete the graphical authentication task compared to the text-based task. A possible interpretation could be based on the familiarity users had in text-based authentication over graphical authentication. On the other hand, FI users did not have significant differences in task completion time and failure rate between the two user authentication mechanisms. In this respect, since the familiarity factor did not affect the graphical authentication mechanism, FI users had better performance than FD users in graphical authentication, and recorded similar performance with text-based password authentication which might be accredited to their dis-embedding skills, improved visual working memory and visual search task abilities (Angeli et al. 2009).
- Time to complete text-based authentication significantly differs between desktop computers and touch-based devices, but not for graphical authentication. Results revealed that the device affects text-based password interactions. In particular, analyses of touch-based user interactions revealed that in general, the time to complete text-based password tasks was significantly larger than desktop-based user interactions. Such a result

increases the external validity of prior research results which revealed that entering text-based passwords on mobile touch-based devices is more time consuming and considered a more demanding task compared to standard desktop computers (von Zezschwitz et al. 2014; Findlater et al. 2011). In regards with graphical authentication mechanisms, no significant differences were observed between desktop-based and touch-based interactions. Such a result might be explained by the fact that selecting images through the computer mouse or through touch on the screen is fairly the same task execution process (i.e., selecting the images through computer mouse clicks vs. finger touch on the screen).

- The interaction device in text-based authentication significantly affects FD users' task completion time, but not FI users. Analysis of results has shown that the task performance of FD and FI users has been affected by specific combinations of user authentication and device types, given the users' different cognitive processing abilities, and adaptation skills within contextual shifts (desktop vs. touch-based). Results revealed that FD users had a significant increase of time to complete the text-based password task on touch-based devices compared to desktop computers, whereas FI users did not have significant differences in task completion time between the two interaction device types. Furthermore, the analysis of desktop-based interactions revealed no significant differences between FD and FI users in text-based passwords, which might be explained by their familiarity with text-based passwords. However, in touch-based interactions, FI users were significantly faster in completing the textual password task compared to FD users due to their positive adaptation and independence in regards with contextual and field changes (desktop vs. touch-based). These results suggest that the device, and eventually the field change, towards touch-based interactions (context-wise and interaction-wise) was adopted more efficiently and effectively by FI users compared to FD users. This finding strengthens the claim of previous research, which state that FD users depend on their surrounding field whereas FI users are not significantly influenced by their surrounding field and context of use (Davis 1991; Messick 1993; Goodenough and Karp 1961; Reardon and Moore 1988).

7.6 Investigate the Effect of Cognitive Processing Abilities on User Performance of User Authentication Type

In this section we describe 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. 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.

The study was conducted 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.

7.6.1 User Groups

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 12.

Table 12. 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

7.6.2 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 54 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).

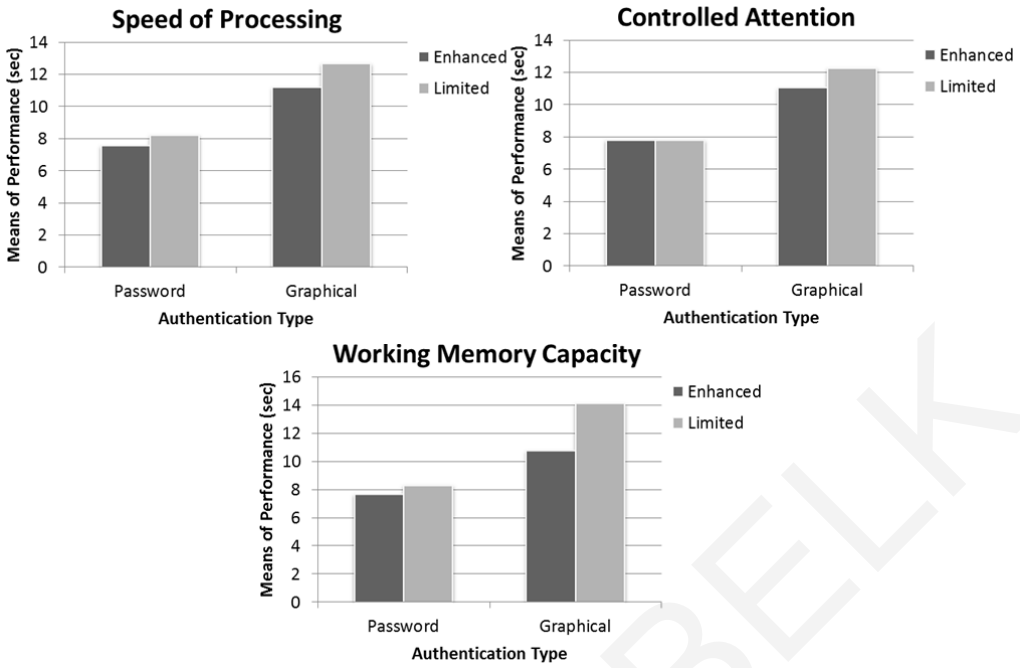


Figure 54. Means of performance for speed of processing (top left), controlled attention (top right) and working memory capacity (bottom) user groups

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.

7.6.3 User Authentication Effectiveness

For each user authentication session the total number of tries made for successfully authenticating in each type was recorded. Table 13 summarizes 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 13. 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 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.

7.6.4 Main Findings

For the context of this research 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. **Users with enhanced cognitive processing abilities performed significantly faster than users with limited cognitive processing abilities in graphical authentication**, where in text-based authentication no significant differences were observed. **Regarding effectiveness, graphical authentication keys are easier to be retained in memory than text-based password for users with limited cognitive processing abilities as they needed less attempts to complete the task.** The main findings are listed below:

- 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.
- 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. 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 us-

ers' cognitive processing abilities could improve authentication task efficiency and effectiveness, and minimize users' cognitive loads and erroneous interactions.

7.7 Investigate the Effect of Cognitive Styles and Cognitive Processing Abilities on Performance of User Authentication Type and Policy

In this section we present and discuss our observations and experiences of applying a 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.

A total of 137 individuals participated in the study (54 males, 83 females, age 17-22), 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 in 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; and (ii) 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 modeling and adaptation process.

In order to compare 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 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 get 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 characteristics so that the conditions were balanced across all user groups. Participants were not aware whether they were receiving a personalized or non-personalized authentication mechanism.

7.7.1 Adaptation Rules

In this section, we describe the applied adaptation rules that recommend a specific type of authentication and policy. The adaptation rules are based on the aforementioned studies which revealed an

effect of users' cognitive styles and cognitive processing abilities on preference and performance of text-based and graphical user authentication mechanisms.

During the first step of adaptation, 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.

7.7.2 User Groups

The cluster analysis of the user modeling mechanism separated users into clusters based on their cognitive style ratios and cognitive processing *z*-values (Table **14**). 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 that clusters from the ones of the other cluster.

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=216). In this respect a Welch t-test was conducted for unequal variances of data.

Table 14. 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

Results indicated that there were significant differences among 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 modeling procedure grouped effectively the users into different clusters, and could be thus safely used in the main data analysis.

7.7.3 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.

No significant outliers were used in the analysis, as assessed by inspection of a boxplot. 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 55 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.

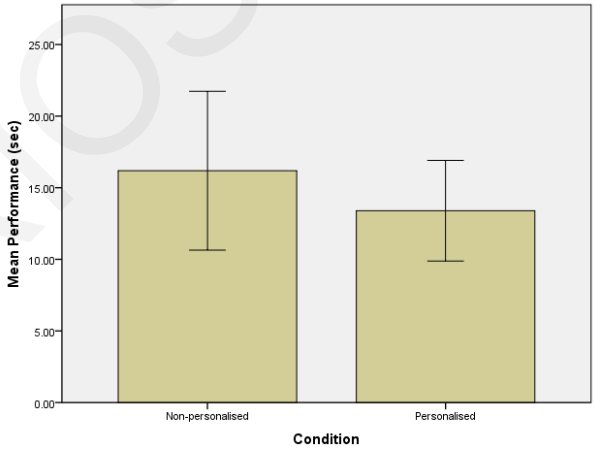


Figure 55. Means of performances per condition

7.7.4 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 at-

tempts were not similar, as assessed by visual inspection (Figure 56). 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. These results were statistically significantly different (U=517699, z=-14.898, p=0.01).

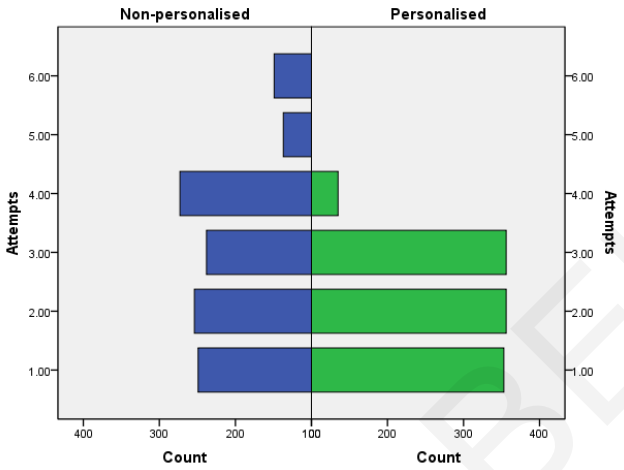


Figure 56. Total attempts to successfully authenticate in each condition

7.7.5 Main Findings

This study proposed a preliminary personalization approach for supporting the design and deployment of usable and secure user authentication tasks. The proposed approach was realized in an initial prototype Web-based system that provided personalized user authentication mechanisms based on individual differences in cognitive styles and cognitive processing abilities. This study was one of the early studies that guided the final development and evaluation of the PAC system.

The study revealed that matching 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 the theories of cognitive factors 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.

7.8 Investigate the Effect of Verbal/ Imager Cognitive Styles on Preference and Performance of CAPTCHA Mechanisms

In this section we describe the sampling and procedure of a user study that aimed to investigate the effects of users' cognitive styles (Verbal/ Imager), on preference and task performance related to different designs of CAPTCHA. The method and results of the study have also been described in Belk et al. (2015a; 2012a).

This user study embraced a between-subject design, aiming to examine whether cognitive styles of users affect preference and performance (task efficiency and effectiveness) on two different types of CAPTCHA challenges; text-recognition and image-recognition. An invitation was announced on the Web-sites of various undergraduate Computer Science courses in order to recruit the participants. The aim of this selection process was to recruit a representative sample of participants that were already familiarized with CAPTCHA challenges based on the fact that Computer Science students are faced daily with CAPTCHA challenges in online courses, forums, blogs, social networking Web-sites, etc.

The participants were asked to visit a Web-page in order to take part in the study. The Web-page provided information and guidelines regarding the study as well as the two CAPTCHA challenges (text and image). The users first provided basic demographic information (age, gender). After, the users were required to choose between the two variations of CAPTCHA (i.e., text- vs. image-recognition) and then solve the preferred CAPTCHA challenge. For the purpose of the study, the complexity level of each CAPTCHA challenge was the same (i.e., 8 characters with the same percentage of noise and distortion was used in the text-recognition challenge, whereas 12 colored images were used in the image-recognition challenge). After solving the CAPTCHA challenge, the users were redirected to an online psychometric test aiming to elicit the users' cognitive styles.

A total of 131 undergraduate Computer Science students participated (76 male, 55 female, age 20-25, mean 23) having recorded the same number of CAPTCHA sessions.

7.8.1 User Groups

For our analysis, we separated users in three categories based on cognitive styles (Verbal/Imager/Intermediate) and in two categories based on cognitive processing abilities (limited/enhanced). Table 15 summarizes the number of users in each group.

Table 15. Number of users per cognitive styles' group

Verbals	Imagers	Intermediates	Total
65	43	23	131

7.8.2 User Preference related to CAPTCHA Challenges

Participants were asked to choose between two variations of CAPTCHA (i.e., text- vs. image-based). In Table 16 we summarize the CAPTCHA preferences according to the users' cognitive styles.

Table 16. Users' cognitive styles vs. CAPTCHA preference

Cognitive Styles	CAPTCHA Type	
	Text-recognition	**Image-recognition**
Verbals	42	23
Imagers	24	19
Intermediates	14	9
Total	80	51

A binomial statistical test was conducted to examine whether there is a general preference relating text- or image-recognition CAPTCHA challenges (H_0: p(text-recognition)=0.5 and p(image-recognition)=0.5). The results revealed that there is significant preference towards text-recognition CAPTCHA challenges (p<0.01). Furthermore, a Pearson's chi-square test was conducted to examine whether there is a relationship between users' cognitive styles and their preference towards a specific type of CAPTCHA challenge (i.e., text- or image-recognition). The results revealed that there is no significant relationship between these two variables (*Chi square value*=0.791, *df*=2, p=0.673). As a consequence, no safe conclusion can be drawn at this stage whether cognitive styles of users influence their preference towards a specific type of CAPTCHA challenge.

However, examining each cognitive styles' group individually with respect to preference towards a particular CAPTCHA type, it has been identified that users of the Verbal class have significant positive preference towards text-recognition CAPTCHA (*Chi square value*=5.554, *df*=1, p<0.02). In contrast, users belonging to the Imager class (*Chi square value*=0.581, *df*=1, p=0.446) and Intermediate class (*Chi square value*=1.087, *df*=1, p=0.297) have not shown a clear preference towards one or the other direction (i.e., text- vs. image-recognition CAPTCHA challenge).

7.8.3 Task Completion Efficiency

For task completion efficiency, two separate analyses were performed: i) comparison of solving times between all CAPTCHA sessions that also included more than one attempts to solve the challenge; and ii) comparison of solving times between CAPTCHA sessions that were solved at first attempt. Complementary data measures such as number of CAPTCHA refreshes are also reported.

Task Completion Efficiency of all CAPTCHA Sessions. A three by two way factorial analysis of variance (ANOVA) was conducted aiming to examine main effects and interactions between the users' cognitive styles (i.e., Verbal, Imager and Intermediate) and CAPTCHA preference (i.e., text- vs. image-recognition) over the time needed to solve a CAPTCHA challenge. We illustrate the results in Figure 57.

As assessed by inspection of boxplots, there were five outliers in the data that were caused by sessions that included more than four attempts to solve the challenge (increasing thus significantly

the total time to solve the challenge), and were removed from the current analysis. The analysis revealed that, the main effect of users' cognitive styles on time needed to solve a CAPTCHA challenge is not significant ($F(2,125)=2.345$, $p=0.1$, *partial* $\eta^2=0.038$). In contrast, a significant main effect of the CAPTCHA challenge type (i.e., text- vs. image-recognition) with regards to the time needed to solve a challenge has been identified ($F(1,125)=34.402$, $p<0.001$, *partial* $\eta^2=0.224$), as users solved text-recognition CAPTCHA significantly more efficient than image-recognition CAPTCHA.

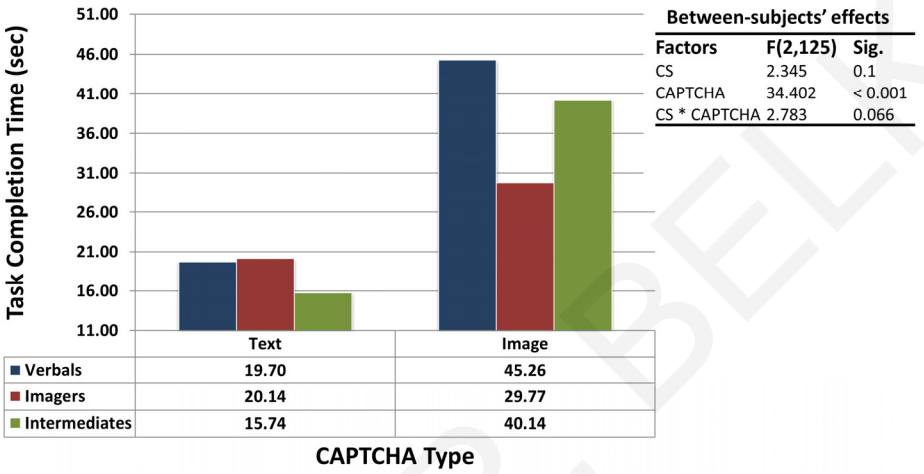


Figure 57. Means of task efficiency per cognitive styles' group (CS) and CAPTCHA preference for all sessions

Furthermore, a pairwise comparison between CAPTCHA types for each cognitive styles' group (Table 17) revealed that users of the Verbal and Intermediate class performed significantly faster in text- than in image-recognition CAPTCHA challenges (Verbals: $MD=-25.560$, $SE=4.528$; $F(1,119)=31.866$, $p<0.001$, Intermediates: $MD=-24.400$, $SE=7.323$; $F(1,119)=11.103$, $p=0.001$). However, users belonging to the Imager class had no significant effect on task efficiency between text- and image-recognition CAPTCHA challenges ($MD=-9.629$, $SE=5.394$; $F(1,119)=3.187$, $p=0.077$), as they performed faster in the image-recognition CAPTCHA challenge compared to the other two groups. An interpretation of this result can be based on the fact that all users were more familiar and experienced interacting with text-recognition CAPTCHA, hence the majority of users (mostly Verbals and Intermediates) were more efficient at solving the text-recognition challenge. On the other hand, since the familiarity factor did not affect the image-recognition CAPTCHA, we have observed that the visual approach of processing and organizing information of the Imagers has positively affected their task completion efficiency compared to the Verbals. This is further supported based on a pairwise comparison between cognitive styles' groups, revealing that Imagers were significantly faster at solving image-recognition CAPTCHA compared to Verbals ($MD=-15.489$, $SE=5.394$; $F(1,119)=4.158$, $p=0.018$).

Table 17. Pairwise comparisons of CAPTCHA types per cognitive styles' group regarding task efficiency

Cognitive Styles	(I) CAPTCHA	(J) CAPTCHA	Mean Diff. (I-J)	Sig.
Verbals	Text	Image	-25.560	<0.001
Imagers	Text	Image	-9.629	=0.077
Intermediates	Text	Image	-24.400	=0.001

Task Completion Efficiency of CAPTCHA Sessions solved at First Attempt. The same analysis was conducted as the previous one, for cases that CAPTCHA sessions were solved at first attempt without any errors. Main aim was to analyze the users' actual cognitive processing time required to solve the challenge, since a failed attempt or refresh loads a new challenge, requiring the users to restart the cognitive process. Figure 58 illustrates the means of task efficiency per cognitive styles' group and preference towards CAPTCHA.

The new analysis revealed that the main effect of users' cognitive styles on time needed to solve a CAPTCHA challenge is significant ($F(2,102)=5.276$, $p=0.007$, *partial* $\eta^2=0.099$). Similar to the previous analysis, the effect of the CAPTCHA challenge type (i.e., text- vs. image-recognition) on the time needed to solve a CAPTCHA challenge was significant ($F(1,102)=27.450$, $p<0.001$, *partial* $\eta^2=0.222$), as users solved the text-recognition challenge more efficiently than the image-recognition challenge. Furthermore, there was an interaction effect between users' cognitive styles and CAPTCHA type on the time needed to solve the challenge ($F(1,102)=5.358$, $p=0.006$, *partial* $\eta^2=0.1$).

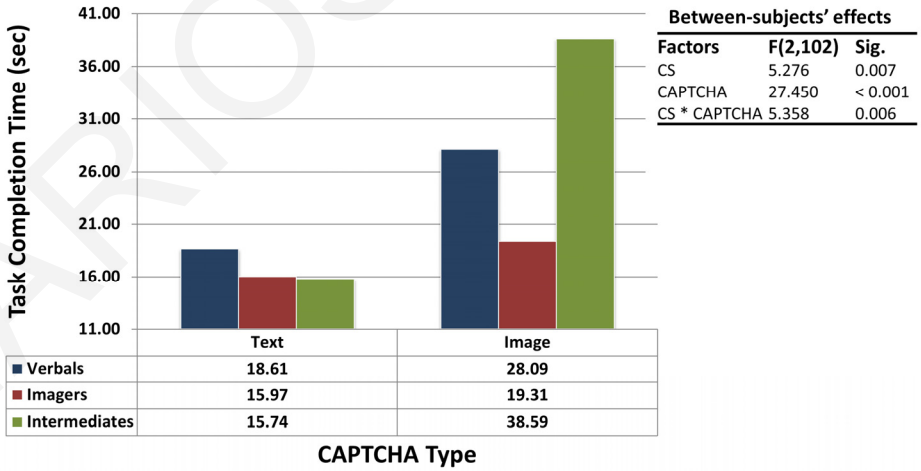


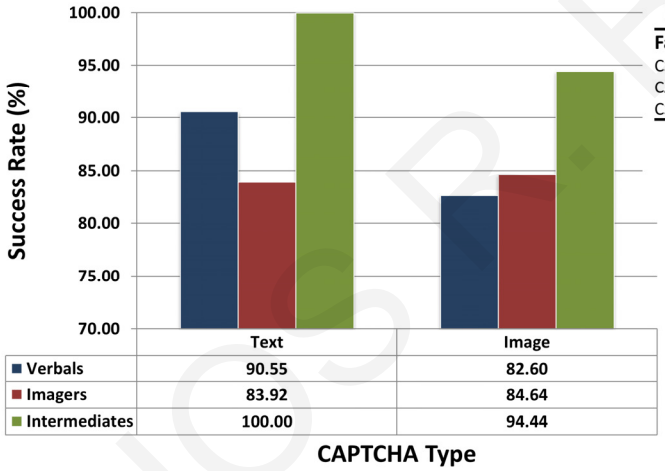
Figure 58. Means of task efficiency per cognitive styles' group (CS) and CAPTCHA preference for sessions solved at first attempt

To this end, the results provide initial indications that cognitive styles play an important role on CAPTCHA solving time and that image-recognition CAPTCHA could be provided as an alternative CAPTCHA mechanism to Imager users since no significant differences were observed with the text-recognition CAPTCHA (which had an additional advantage of the familiarity factor since us-

ers were more experienced with text-recognition challenges). In addition, Imagers were significantly faster than Verbals in solving image-recognition challenges.

7.8.4 Task Completion Effectiveness

Task completion effectiveness was measured as the success rate of the CAPTCHA session; for example, when a user solved the CAPTCHA at first attempt, the success rate value is 100%, whereas for a user that solved the challenge at third attempt, the success rate value is 33%. A three by two way factorial analysis of variance (ANOVA) was conducted using cognitive styles (Verbal/ Imager/ Intermediate) and CAPTCHA preference (text and image) as independent variables and CAPTCHA success rate as the dependent variable. Figure 59 illustrates the success rate per cognitive styles' group and CAPTCHA type. Table 18 also summarizes the total number of attempts per cognitive styles' group and CAPTCHA type.



Between-subjects' effects

Factors	F(2,131)	Sig.
CS	0.796	0.374
CAPTCHA	2.143	0.122
CS * CAPTCHA	0.396	0.674

Figure 59. Means of success rate per cognitive styles' group (CS) and CAPTCHA preference

The analysis revealed that, the main effect of users' cognitive styles on success rate to solve a CAPTCHA challenge is not significant ($F(2,131)=0.796$, $p=0.374$, *partial* $\eta^2=0.006$). In addition, there was no main effect of the CAPTCHA challenge type (i.e., text- vs. image-recognition) on the CAPTCHA success rate ($F(1,131)=2.143$, $p=0.122$, *partial* $\eta^2=0.033$).

The results might be explained by the fact that the majority of sessions were successfully completed at first attempt. Nevertheless, based on the descriptive statistics, we observe that Verbals and Intermediates have better success rates in the case of text-recognition challenges compared to the image-recognition. In the case of Imagers, minimal differences in success rate exist between the two CAPTCHA types. Also worth mentioning is the fact that Intermediates had the highest success rates in both CAPTCHA types compared to the other user groups, with a 100% success rate of all Intermediate users in the case of text-recognition CAPTCHA.

Table 18. Number of attempts per cognitive styles' group and CAPTCHA type.

Cognitive Styles	Attempts	CAPTCHA Type		
		Text-recognition	Image-recognition	Total
Verbals	1	36	16	52
	2	2	4	6
	3	1	3	4
	>4	3	0	3
Imagers	1	18	14	32
	2	2	3	5
	3	3	1	4
	>4	1	1	2
Intermediates	1	14	8	22
	2	0	1	1

Complementary Data Measures. The number of refreshes was recorded as complementary data measures. Table 19 summarizes the number of refreshes per cognitive styles' group and CAPTCHA type.

Table 19. Number of refreshes per cognitive styles' group and CAPTCHA type

	Verbals	Imagers	Intermediates	Total
Text	1	0	6	7
Image	3	0	0	3

Imagers did not refresh any challenge in both CAPTCHA types, whereas 3 sessions of Verbals (1 user with 2 refreshes, 1 user with 1 refresh) initiated a refresh in an image-recognition CAPTCHA, while 1 refresh was initiated in a text-recognition CAPTCHA. In the case of Intermediates, 6 refreshes were recorded in the case of text-recognition, among them, 1 user initiated 2 consecutive refreshes in the same session. The Kruskal-Wallis H and the Mann-Whitney U test respectively did not reveal significant differences between the 3 cognitive styles' groups and the 2 CAPTCHA types on the number of refreshes.

7.8.5 Main Findings

Analysis of results demonstrated several main effects of cognitive processing characteristics of users on preference and task performance of different visual designs of CAPTCHA challenges. **Regarding user preference, a significant positive tendency of users preferring text- than image-recognition CAPTCHA challenges has been observed. Furthermore, Verbal users significantly preferred text- than image-recognition challenges whereas a growing trend for Imager**

users has shown to prefer image-recognition challenges. Regarding task completion efficiency, Verbals and Intermediates were significantly more efficient in text-recognition CAPTCHA, whereas Imagers did not perform significantly different in either CAPTCHA design as they solved image-recognition CAPTCHA challenges much faster than the other user groups.

Figure 60 provides a visual illustration of the main effects of users' cognitive styles (Verbal/ Imager/ Intermediate) on CAPTCHA preference and performance. The vertical lines show the effect's strength of the particular cognitive characteristic (i.e., Verbal/ Imager/ Intermediate) on the usability metrics investigated (i.e., user preference, task completion, success rate) with respect to the different CAPTCHA designs (i.e., text vs. image, and baseline vs. higher complexity).

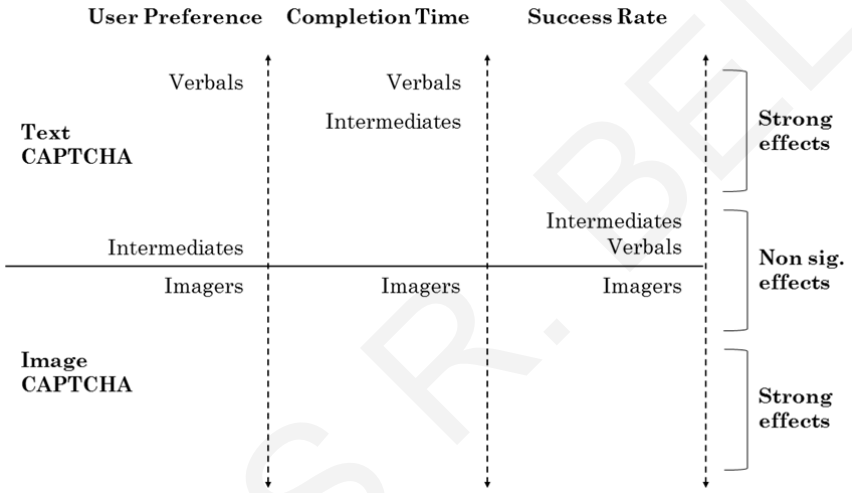


Figure 60. Main effects of users' cognitive styles on CAPTCHA preference and performance

We list the main findings below:

- Regarding user preference, participants in general preferred significantly text- than image-recognition CAPTCHA challenges. This finding can be explained by taking into consideration that the majority of Web application providers utilize text-recognition CAPTCHA (Bursztein et al. 2010), and thus, users are more familiar in solving text- than image-recognition CAPTCHA challenges.
- Results also revealed a significant preference for users belonging to the Verbal class to choose text- than image-recognition challenges and, as the sample increases there is a growing trend for users belonging to the Imager class to prefer image-recognition challenges.
- Results of task efficiency revealed that Verbals and Intermediates were significantly more efficient when interacting with text-recognition CAPTCHA, whereas in the case of Imagers, no significant differences in performance were observed between the two variations of CAPTCHA since they solved image-recognition CAPTCHA challenges much faster than the other two cognitive style groups. This result indicates that Imagers were positively affected by their cognitive style of processing more efficiently graphical than

text-based information, underpinning that cognitive styles are important to be considered in the design of CAPTCHA challenges. Accordingly, we suggest that image-recognition CAPTCHA challenges could be a viable alternative to current text-recognition challenges for Imager users. On the other hand, it is suggested to provide text-recognition CAPTCHA challenges to Verbals and Intermediates.

7.9 Investigate the Effect of Verbal/ Imager and Wholist/ Analyst Cognitive Styles on Preference and Performance of CAPTCHA Mechanisms and Device Type

This section presents a four-month between-subject user study in which 192 participants interacted with personalized and non-personalized CAPTCHA mechanisms in an ecological valid context based on their cognitive styles (Verbal/ Imager and Wholist/ Analyst) and the device used for interaction (standard desktop or mobile touch-based). The participants were required to solve personalized CAPTCHA challenges, primarily before posting comments on an online blog, when accessing specific material of the course or before viewing their course grades. From the beginning of the study we encouraged the participants to use their touch-based mobile devices for interacting with the system.

The participants were accessing the course's Web-site and solving CAPTCHA through standard IO devices (keyboard and mouse) on desktop computers, and touch-based mobile devices. During each CAPTCHA session, the system illustrated a specific type of CAPTCHA (text-recognition or image-recognition) based on the cognitive styles of each user, combined with the interaction device used.

In order to investigate the added value of personalizing the CAPTCHA task based on the users' cognitive styles and the interaction device, a matched and a mismatched condition was randomly assigned to specific adaptation rules so that half of the participants would interact with a personalized CAPTCHA mechanism (matched condition), and half of the participants would interact with a non-personalized CAPTCHA mechanism (mismatched condition). For example, in case of a matched condition, the user received the CAPTCHA challenge as recommended by the adaptation rule, whereas a mismatched condition provided the opposite type of CAPTCHA to the one suggested by the mechanism. The allocation was based on the users' cognitive styles so that the conditions were balanced across all cognitive style groups. The participants were not aware whether they were receiving a personalized or a non-personalized CAPTCHA challenge.

The users' interactions were recorded for a period of three months. After this period, aiming to engage all participants with both types of CAPTCHA mechanisms (textual and graphical), during the last month of the study, the service provided the opposite type of CAPTCHA to all users (users that initially interacted with a text-recognition CAPTCHA, then interacted with an image-recognition CAPTCHA, and vice versa). The interactions during the last month were intended only

to provide experience to users regarding the opposite type of CAPTCHA, and further elicit their preference towards a particular CAPTCHA type at the end of the study.

7.9.1 Adaptation Rules

The CAPTCHA type (text-recognition or image-recognition) was provided to the users based on a rule-based algorithm (see chapter 6). In particular, in case the CAPTCHA tasks are performed on standard IO devices, the mechanism recommends a text-recognition CAPTCHA to Verbals, and an image-recognition CAPTCHA to Imagers since each type of CAPTCHA is best matched to the habitual approach of the users' Verbal/ Imager cognitive style (section 7.8). On the other hand, when a touch-based device is used, based on cognitive styles' theory (Riding and Cheema 1991), given that Wholist users view the standard keyboard as a whole and are dependent on their contextual surroundings, changing the standard keyboard to a virtual keyboard might negatively affect their interactions, and therefore the mechanism recommends an image-recognition CAPTCHA. In contrast, given that Analysts might not be significantly affected by their surroundings' change, the Verbal/ Imager cognitive style is utilized as the primary factor for deciding the CAPTCHA type. Thus, the same rule is applied as in the case of interacting with a standard IO device, i.e., provide a text-recognition CAPTCHA to Verbals and an image-recognition CAPTCHA to Imagers. In case no information about the users' cognitive styles exists, the mechanism decides the CAPTCHA type by only considering the users' interaction device type. In particular, an image-recognition CAPTCHA is provided to users that interact with touch-based mobile devices, since recent research has shown that entering text on a virtual keyboard is in general a more demanding task compared to text input on a standard keyboard (Findlater et al. 2011). Finally, given that the usability of both types of CAPTCHA are considered similar when interaction takes place on standard IO devices, a random CAPTCHA type is provided to the users in this case.

7.9.2 User Groups

A total of 192 individuals participated in the study (42% male, 58% female, age 17-25) and were undergraduate university students. A total of 3157 successful CAPTCHA sessions were recorded during the study, with 1862 sessions of users utilizing a standard IO device, and 1295 sessions of users utilizing a touch-based mobile device. The initial five CAPTCHA sessions for each participant were excluded from the analysis and served as learning sessions for the users to get familiar and understand the task of each CAPTCHA. Furthermore, as touch-based devices of users where different, we considered for our analysis a sub-sample of interactions with touch-based tablet devices with a minimum of seven and maximum of ten inches, since prior research has shown that mobile screen sizes larger than 4.3 inches are more efficient during information seeking tasks

(Raptis et al. 2013), and screen sizes between 5.7 and 9.7 inches have a main effect on enjoyment (Kim et al. 2011).

Based on the cognitive style elicitation phase, we separated our sample in 4 groups (Verbal-Wholist, Verbal-Analyst, Imager-Wholist, Imager-Analyst) according to their interactions with the cognitive styles elicitation tool (Table 20).

Table 20. Cognitive styles' classes based on the user modeling process

	Verbals	**Imagers**	**Total**
Wholists	57	48	105
Analysts	51	36	87
Total	108	84	192

We next present the analysis of interaction results and provide interpretations of our observations based on the user study conducted.

7.9.3 CAPTCHA Efficiency

Various statistical analyses were performed regarding CAPTCHA solving efficiency with the aim to investigate the following: (i) Compare solving time between personalized and non-personalized CAPTCHA interactions; and (ii) investigate interaction effects between cognitive styles, device type and CAPTCHA type on the time to solve a CAPTCHA challenge.

Efficiency of Personalized vs. Non-personalized CAPTCHA Interactions

An independent-samples t-test was performed to determine mean differences on the time needed to solve the personalized and non-personalized CAPTCHA challenge. Figure 61 illustrates the means of performance for each condition.

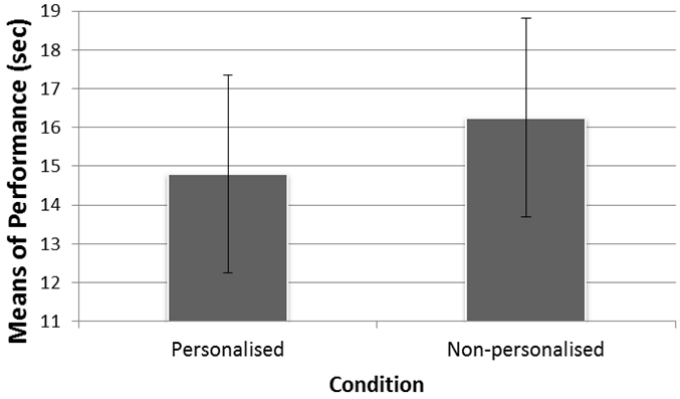


Figure 61. Means of performance per condition

The analysis revealed that interactions with personalized CAPTCHA and non-personalized CAPTCHA were significantly different ($t(344.612)=6.365$, $p<0.01$). Accordingly, the results indicate a main effect of personalizing CAPTCHA on task efficiency since the personalized CAPTCHA-based interactions were more efficient ($M=14.80$, $SD=1.86$) than non-personalized CAPTCHA ($M=16.25$, $SD=2.56$).

Efficiency Interaction Effects between Cognitive Styles, Device and CAPTCHA

A 4x2x2 factorial analysis of variance (ANOVA) was conducted using cognitive styles (Verbal/Imager and Wholist/ Analyst), device type (standard IO and touch-based), and CAPTCHA type (textual and graphical) as independent variables, and the time to successfully solve the CAPTCHA as the dependent variable. The analysis revealed that there was a statistically significant interaction between device and CAPTCHA type on the time to successfully solve a CAPTCHA ($F(1,384)=21.516$, $p<0.001$). Figure 62 illustrates the means of performance per device and CAPTCHA type. In this context, a pairwise comparison of CAPTCHA types revealed that text-based and image-based CAPTCHA interactions on standard IO devices did not have significant differences in solving time ($MD=0.192$, $SE=0.298$; $F(1,380)=0.416$, $p=0.520$), whereas in the case of touch-based interactions, image-recognition CAPTCHA were more efficient than text-recognition CAPTCHA ($MD=2.230$, $SE=0.3$; $F(1,380)=55.886$, $p<0.001$) due to the significant increase of time for solving a text-recognition CAPTCHA in touch-based devices.

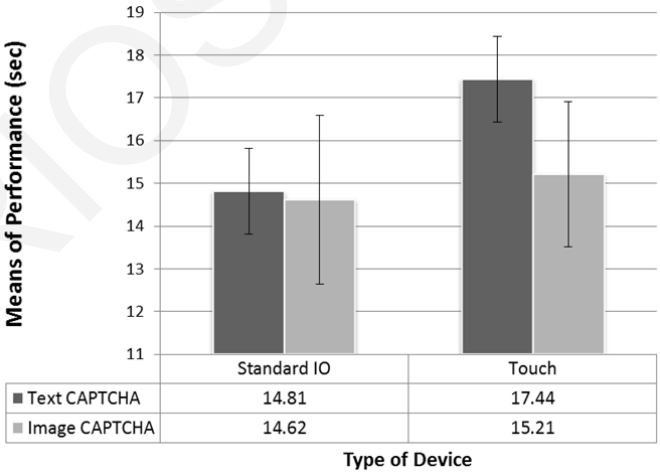


Figure 62. Means of performance for device and CAPTCHA types

Furthermore, a pairwise comparison of device type showed that text-recognition CAPTCHA were solved significantly faster on standard IO devices compared to touch-based devices ($MD=2.628$, $SE=0.298$; $F(1,380)=78.019$, $p<0.001$). Similarly, image-recognition CAPTCHA were solved significantly faster on standard IO devices compared to touch-based devices ($MD=0.590$, $SE=0.255$; $F(1,380)=3.896$, $p=0.049$), however, the mean difference compared to text-recognition CAPTCHA was considerably less, suggesting that image-recognition CAPTCHA could be utilized

as a valid alternative to text-recognition CAPTCHA when deployed on mobile touch-based devices.

The aforementioned results could be interpreted considering that solving a text-recognition CAPTCHA on a touch-based device is a more demanding task than on a standard IO device since text entry on virtual keyboards is less efficient compared to standard desktop keyboards (Findlater et al. 2011). Nevertheless, the analysis also revealed a statistically significant interaction between cognitive styles, device and CAPTCHA type on the time to successfully solve a CAPTCHA ($F(3,384)=2.821$, $p=0.039$). Such a result indicates that cognitive styles have also a main effect on CAPTCHA solving time and should be considered in combination with the device and CAPTCHA type. Figure 63 illustrates the means of performance of cognitive styles groups and CAPTCHA type when interacting with standard IO and touch-based devices.

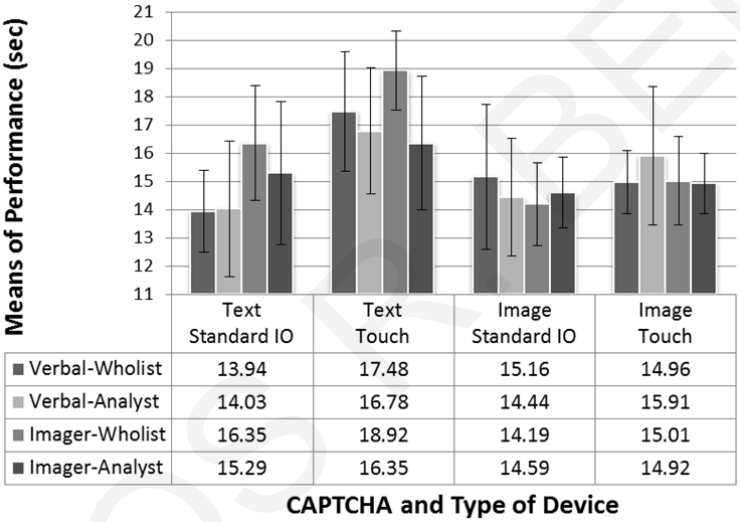


Figure 63. Means of performance for cognitive styles, device and CAPTCHA type

Pairwise comparisons (Table 21) between CAPTCHA types revealed the following: in standard IO interactions, Verbal-Wholists were significantly faster in solving text-recognition CAPTCHA compared to image-recognition CAPTCHA ($MD=1.219$, $SE=0.519$; $F(1,368)=5.530$, $p=0.019$), whereas in touch-based interactions the same group was significantly faster in image-recognition CAPTCHA ($MD=2.521$, $SE=0.519$; $F(1,368)=23.640$, $p<0.01$). Such a result supports the theoretical assumption of this work, suggesting that Verbals are significantly faster when interacting with text-recognition CAPTCHA on standard IO devices (Belk et al. 2012a), however, when the device type/ context is changed, Wholist users are negatively affected when interacting with virtual keyboards, which explains the fact that Wholists were significantly faster in image-recognition than text-recognition CAPTCHA when interacting on touch-based devices. On the other hand, interactions of Imager-Wholists revealed significant differences in both device types as they were significantly faster when interacting with image-recognition compared to text-recognition CAPTCHA on both standard IO and touch-based devices. In the same line, Imager-Analysts were significantly faster when interacting with an image-recognition CAPTCHA on touch-based devices indicating that Imagers significantly perform faster with image-recognition CAPTCHA.

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 and being affected differently in various contexts of use (Riding and Cheema 1991), the results indicate that these cognitive processing characteristics could be a determinant factor on the personalization of CAPTCHA mechanisms as they improve task completion efficiency of CAPTCHA.

Table 21. Pairwise comparisons of CAPTCHA types per cognitive style and device type

Cognitive Styles	Device	(I) CAPTCHA	(J) CAPTCHA	Mean Diff. (I-J)	Sig.
Verbal Wholist	Standard IO	Text	Image	-1.219	0.019
		Image	Text	1.219	0.019
	Touch	Text	Image	2.521	0.001
		Image	Text	-2.521	0.001
Verbal Analyst	Standard IO	Text	Image	-0.411	0.454
		Image	Text	0.411	0.454
	Touch	Text	Image	0.874	0.112
		Image	Text	-0.874	0.112
Imager Wholist	Standard IO	Text	Image	2.154	0.001
		Image	Text	-2.154	0.001
	Touch	Text	Image	3.920	0.001
		Image	Text	-3.920	0.001
Imager Analyst	Standard IO	Text	Image	0.702	0.283
		Image	Text	-0.702	0.283
	Touch	Text	Image	1.431	0.029
		Image	Text	-1.431	0.029

7.9.4 CAPTCHA Effectiveness

CAPTCHA effectiveness was measured in terms of success rate. The following were investigated based on each user's calculated CAPTCHA success rate value: (i) Comparison of the success rate between personalized and non-personalized CAPTCHA interactions; and (ii) investigation of interaction effects between cognitive styles, device and CAPTCHA.

Effectiveness of Personalized vs. Non-personalized CAPTCHA Interactions

The analysis compared the effectiveness between the personalized and non-personalized CAPTCHA interactions (Figure 64). An independent samples t-test showed that there is a statistically significant difference between the two conditions ($t(324.944)=-8.526$, $p<0.01$) which indi-

cates that the proposed personalization method significantly affects the success rate of CAPTCHA. In particular, personalized CAPTCHA interactions had a mean success rate of 83.26% (*SD*=5.06), whereas non-personalized CAPTCHA had a mean success rate of 77.55% (*SD*=7.73). The results suggest that personalized CAPTCHA tasks have an improved success rate compared to non-personalized CAPTCHA tasks.

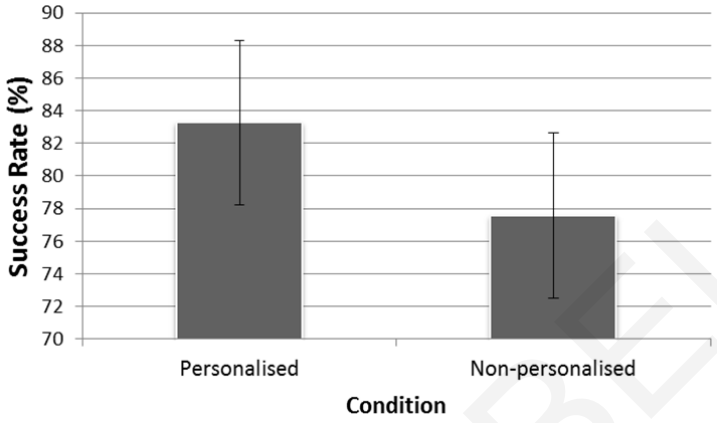


Figure 64. Success rate between personalized and non-personalized CAPTCHA interactions

Effectiveness Interaction Effects between Cognitive Styles, CAPTCHA and Device

A 4x2x2 factorial analysis of variance (ANOVA) was conducted using cognitive styles (Verbal/Imager and Wholist/ Analyst), device type (standard IO and touch-based), and CAPTCHA type (textual and graphical) as independent variables and CAPTCHA success rate as the dependent variable. Figure 65 illustrates the success rate per device and CAPTCHA type. The analysis revealed that there is a statistically significant interaction between device and CAPTCHA type on the success rate of solving CAPTCHA ($F(1,384)=46.576$, $p<0.001$). A pairwise comparison of CAPTCHA types showed that text-based and image-based CAPTCHA interactions have significant differences in success rate on both standard IO and touch-based interactions (standard IO: *MD*=4.264, *SE*=0.721; $F(1,368)=35.014$, $p<0.001$; touch-based: *MD*=11.220, *SE*=0.721; $F(1,368)=242.387$, $p<0.001$). Especially in the case of touch-based interactions a high value of mean difference of success rate (11.22%) has been observed between text-recognition and image-recognition CAPTCHA suggesting that image-recognition CAPTCHA are more effective when deployed on touch-based devices. This might be due to the fact that the success rate of text-recognition CAPTCHA was significantly decreased when deployed on touch-based devices compared to standard IO devices (*MD*=6.542, *SE*=0.719; $F(1,368)=82.764$, $p<0.001$). Regarding image-recognition CAPTCHA, a pairwise comparison of standard IO and touch-based interactions revealed that success rate of standard IO devices was not significantly different compared to touch-based devices (*MD*=0.414, *SE*=0.722; $F(1,368)=0.329$, $p=0.567$).

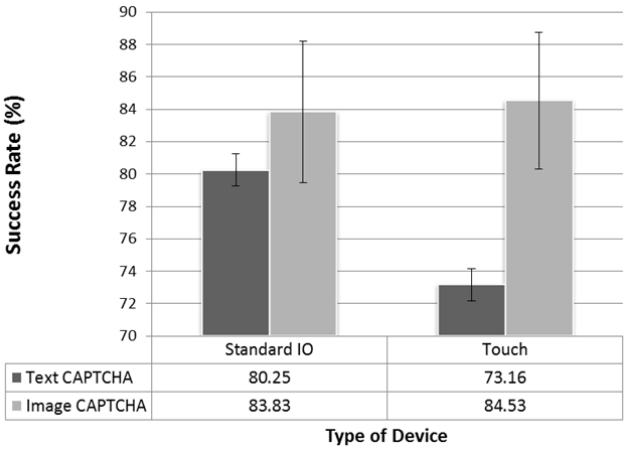


Figure 65. Success rate for different CAPTCHA and device types

The analysis also revealed interaction effects between cognitive styles, device and CAPTCHA type. Figure 66 illustrates the means of success rate of cognitive styles groups and CAPTCHA type when interacting with standard IO and touch-based devices. Results showed that image-recognition CAPTCHA had a significant higher success rate for all user types on both device types.

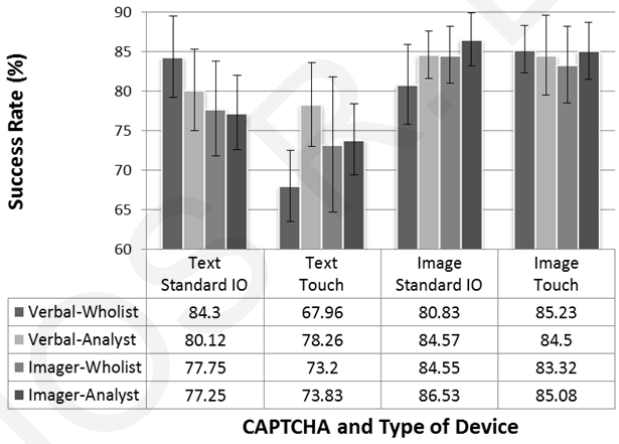


Figure 66. Success rate for cognitive styles, device and CAPTCHA type

Furthermore, pairwise comparisons (Table 22) between standard IO and touch-based devices revealed that Verbal-Wholists were negatively affected by touch-based devices when interacting with text-recognition CAPTCHA. In particular, touch-based interactions with text-recognition CAPTCHA for Verbal-Wholists were significantly slower than with standard IO interactions (MD=16.343, SE=1.304; F(1,368)=157.095, p<0.001). On the other hand, Verbal-Analysts were not significantly affected by the device change of text-recognition CAPTCHA since no significant differences were observed in success rate for this cognitive style group (MD=1.856, SE=1.365; F(1,368)=1.848, p=0.175). Such a result further supports theory on cognitive styles that Analyst users are context independent and more active to accept contextual changes; hence the change of text input from standard keyboard to touch-based virtual keyboard did not significantly affect their performance in terms of errors.

Table 22. Pairwise comparisons of device types per cognitive style and CAPTCHA type

CAPTCHA	CS	(I) Device	(J) Device	Mean Diff. (I-J)	Sig.
Text	Verbal-Wholist	Standard IO	Touch	16.343	0.001
		Touch	Standard IO	-16.343	0.001
	Verbal-Analyst	Standard IO	Touch	1.856	0.175
		Touch	Standard IO	-1.856	0.175
	Imager-Wholist	Standard IO	Touch	4.551	0.001
		Touch	Standard IO	-4.551	0.001
	Imager-Analyst	Standard IO	Touch	3.417	0.038
		Touch	Standard IO	-3.417	0.038
Image	Verbal-Wholist	Standard IO	Touch	-4.401	0.001
		Touch	Standard IO	4.401	0.001
	Verbal-Analyst	Standard IO	Touch	.071	0.959
		Touch	Standard IO	-.071	0.959
	Imager-Wholist	Standard IO	Touch	1.226	0.389
		Touch	Standard IO	-1.226	0.389
	Imager-Analyst	Standard IO	Touch	1.448	0.378
		Touch	Standard IO	-1.448	0.378

Regarding image-recognition CAPTCHA, Verbal-Wholists were significantly more effective when interacting with touch-based devices ($F(1,368)=11.394$, $p=0.001$), whereas in the case of all the rest cognitive style groups, no significant differences were observed between standard IO and touch-based interactions.

Finally, the results may be utilized as complementary data for further supporting the interaction effects observed in the previous analysis of task efficiency and providing additional indications that cognitive styles could be considered as personalization factors for designing more usable CAPTCHA mechanisms. In particular, based on the analyses, results suggest that individual differences in cognitive styles should be utilized for deciding different visual and interaction designs of CAPTCHA challenges since significant differences were observed among users with different cognitive styles in both task efficiency and effectiveness based on their interactions with various types of devices and CAPTCHA.

7.9.5 User Preference and Perceived Usability

With the aim to engage all participants with both types of CAPTCHA (textual and graphical) and both types of devices (standard IO and touch-based), during the last month of the study, the system provided the opposite type of CAPTCHA to all users. The interactions during the last month were

not utilized in the previous analysis and were intended only to provide experience to users regarding the opposite type of CAPTCHA, and further elicit their preference and perceived usability regarding a particular CAPTCHA type.

Aiming to validate findings of the quantitative analysis and to enrich our understanding about users perceptions and perceived usability we conducted a survey which investigated the following factors: (i) Which type of CAPTCHA the users prefer; (ii) which type of CAPTCHA the users believe is more efficient to solve; (iii) which type of CAPTCHA the users believe is more effective to solve. The survey consisted of 6 questions that were divided in two groups. The first group of questions asked the participants to rank the two CAPTCHA types (text or image) when interaction takes place on standard IO devices, and the second group asked the same questions focusing on interactions that take place on touch-based devices. An example question of the first group was *"Which CAPTCHA type would you prefer to solve when interaction takes place on standard IO devices?"* and an example question of the second group of questions was *"Which CAPTCHA type do you solve faster when interaction takes place on touch-based devices?"*. For each question, participants ranked the two CAPTCHA methods with 1 and 2 to represent their first and second choice. Table 23, Table 24 and Table 25 list the number of participants who chose a specific type as their first choice, respectively for ranking the CAPTCHA type regarding preference, perceived efficiency and perceived effectiveness.

Chi-square tests were conducted to examine whether there is a relationship between users' cognitive styles (Verbal/ Imager and Wholist/ Analyst) and their preference, perceived efficiency and perceived effectiveness toward a specific CAPTCHA type, given a specific type of interaction device.

Table 23. Users' preference

	Verbal-Wholist	**Verbal-Analyst**	**Imager-Wholist**	**Imager-Analyst**
When interaction takes place on a standard IO device				
Text-recognition	40	32	20	22
Image-recognition	17	19	28	14
When interaction takes place on a touch-based device				
Text-recognition	11	12	10	6
Image-recognition	46	39	38	30

Factor 1 - CAPTCHA Preference

In the case of standard IO interactions, results revealed that there is a significant relationship between cognitive styles and CAPTCHA (*Chi square value*=9.282, *df*=3, *p*=0.026). The majority of users (Verbal-Wholists, Verbal-Analysts and Imager-Analysts) preferred text-recognition CAPTCHA when interacting on standard IO devices, in contrast to Imager-Wholists who preferred image-recognition CAPTCHA. This finding can be explained by taking into consideration that a

high number of service providers utilize text-recognition CAPTCHA (Bursztein et al. 2010), and thus, users are more familiar in solving text-recognition than image-recognition CAPTCHA challenges on standard IO devices. Nevertheless, Imager users (especially Imager-Wholists) significantly preferred image-recognition CAPTCHA instead of text-recognition CAPTCHA which is closer to their cognitive styles of processing and organizing information.

In the case of touch-based devices, users across all types of cognitive style dimensions (Verbal/ Imager and Wholist/ Analyst) preferred interacting with image-recognition CAPTCHA. In this respect, no strong relationship exists between users' cognitive styles and their preference toward a specific type of CAPTCHA when interaction takes place on a touch-based device (*Chi square value*=0.667, *df*=3, *p*=0.881). As a consequence, this result suggests that the type of device has a strong effect across all types of users when interacting with image-recognition CAPTCHA on touch-based devices. This might be due to the added difficulty of text input in touch-based devices (Findlater et al. 2011) which in this case has a stronger influence on CAPTCHA preference than cognitive styles.

Table 24. Users' perceived efficiency

	Verbal-Wholist	**Verbal-Analyst**	**Imager-Wholist**	**Imager-Analyst**
When interaction takes place on a standard IO device				
Text-recognition	37	29	17	13
Image-recognition	20	22	31	23
When interaction takes place on a touch-based device				
Text-recognition	15	19	11	7
Image-recognition	42	32	37	29

Factor 2 - CAPTCHA Perceived Efficiency

Regarding standard IO interactions, there is a statistical significant association between cognitive styles and perceived efficiency (*Chi square value*=12.892, *df*=3, *p*=0.005). The majority of Verbal-Wholists and Verbal-Analysts thought that text-recognition CAPTCHA were more efficient than image-recognition CAPTCHA, whereas Imager-Wholists and Imager-Analysts thought that image-recognition CAPTCHA were more efficient. The results support the quantitative measures obtained throughout the study which revealed that cognitive styles have a main effect on efficiency of different CAPTCHA types. On the other hand, in questions related to touch-based interactions no significant association between cognitive styles and perceived efficiency was observed (*Chi square value*=4.175, *df*=3, *p*=0.243). The majority of users across all cognitive style groups thought that image-recognition CAPTCHA were more efficient than text-recognition CAPTCHA when interaction takes place on touch-based devices.

Table 25. Users' perceived effectiveness

	Verbal-Wholist	**Verbal-Analyst**	**Imager-Wholist**	**Imager-Analyst**
When interaction takes place on a standard IO device				
Text-recognition	27	23	13	9
Image-recognition	30	28	35	27
When interaction takes place on a touch-based device				
Text-recognition	17	20	11	12
Image-recognition	40	31	37	24

Factor 3 - CAPTCHA Perceived Effectiveness

Responses of the participants that were related to standard IO interactions revealed a statistical significant association between cognitive styles and perceived effectiveness (*Chi square value*=8.247, *df*=3, *p*=0.041). Although the majority of user rankings showed that image-recognition CAPTCHA were more effective than text-recognition CAPTCHA, a high number of Verbal-Wholists and Verbal-Analysts ranked text-recognition CAPTCHA as their first choice. Regarding touch-based interactions, there was no significant association between cognitive styles and perceived effectiveness (*Chi square value*=3.184, *df*=3, *p*=0.364). This might be based on the added difficulty of entering text on touch-based devices that increases erroneous interactions (Findlater et al. 2011).

7.9.6 Main Findings

Results indicate that the proposed personalization method was at some extend successful since **user interactions with personalized CAPTCHA were significantly more efficient and effective than non-personalized CAPTCHA**, suggesting that cognitive styles and device type could be considered as personalization factors for improving the usability and user experience of CAPTCHA tasks. Furthermore, results also yielded several interaction effects between cognitive styles, device and CAPTCHA types on both user performance in terms of task efficiency and effectiveness and user preference. In particular, **users of a particular cognitive style (Verbal or Imager) solve more efficiently and effectively the matched type of CAPTCHA (respectively text-recognition and image-recognition CAPTCHA on standard IO devices.** Furthermore, **Wholist users perform significantly worse when text-recognition CAPTCHA are deployed on touch-based devices compared to standard IO devices**, whereas Analyst users are not negatively affected by the device change as no significant differences exist between standard IO and touch-based interactions. **Regarding preference, users in general preferred text-recognition than image-recognition CAPTCHA challenges on standard IO devices.** Finally, results revealed that **the type of device**

has an overarching effect over cognitive styles since the majority of users in all user groups preferred image-recognition CAPTCHA when deployed on touch-based devices. We list below the main findings of this study:

- Users belonging to the Verbal class solve more efficiently and effectively text-recognition than image-recognition CAPTCHA challenges when these are deployed on standard IO device, whereas users belonging to the Imager class the opposite. Such a result supports the validity of similar research attempts which showed a main effect of cognitive styles on CAPTCHA efficiency (Belk et al. 2015a; 2012a).
- The incorporation of the Wholist/ Analyst dimension in the analysis revealed that Wholist users are negatively affected, in terms of task efficiency and effectiveness, when text-recognition CAPTCHA are deployed on touch-based devices with virtual keyboards, whereas in the case of Analyst users no significant differences were observed between standard IO and touch-based interactions. The result could be interpreted based on cognitive styles' theory (Riding and Cheema 1991), suggesting that Analyst users are more active and positive to adapt to contextual surroundings and changes, in contrast to Wholist users that are more passive and dependent on their surroundings.
- Participants in general preferred significantly text-recognition than image-recognition CAPTCHA challenges when these are deployed on standard IO devices, except of Imager-Wholist users that preferred image-recognition CAPTCHA.
- Regarding touch-based devices, the analysis showed that the type of device has an overarching effect over cognitive styles since the majority of users in all user groups preferred image-recognition CAPTCHA, which might be explained by the fact that entering text on visual touch-based keyboards is considered a more demanding task (Findlater et al. 2011).

7.10 Investigate the Effect of Cognitive Processing Abilities on Performance of CAPTCHA Mechanisms

In this section we describe the method and design of a user study that aimed to investigate whether individual differences in cognitive processing abilities affect task completion time and task completion success rate of two different levels of CAPTCHA challenge complexity (baseline and higher) of both text-recognition and image-recognition CAPTCHA. The method and results of the study have also been described in Belk et al. (2015a). In addition, the method and results of a similar user study were described in Belk et al. (2013a). In this study, the users' cognitive styles were used as control factors; based on the cognitive styles of each user (Verbal/ Imager/ Intermediate), the system provided a text-recognition CAPTCHA to Verbal and Intermediate users, and an image-

recognition CAPTCHA to Imager users since an observable main effect of cognitive styles of users on CAPTCHA task completion efficiency had been observed.

The user study was applied in the frame of a registration process of a university Computer Science course as part of students' enrolment in the course's Web-site. Main aim of this process was to increase the ecological validity of the users' interactions with CAPTCHA challenges since the Web-site would be used by the students to view and download material of their course throughout the semester. The user study embraced a between-subject design, aiming to investigate whether cognitive processing abilities of users affect task completion efficiency and effectiveness of different levels of CAPTCHA complexity (i.e., baseline or higher level of complexity for both text- and image-recognition CAPTCHA).

The user study was conducted in a controlled lab setting and was split in two phases at two different time stamps: Phase A for eliciting the users' cognitive processing characteristics (cognitive styles and cognitive processing abilities), and Phase B for enrolling the users in the online course and record their interactions with the CAPTCHA challenges.

In Phase A, users initially interacted with the developed psychometric tests by providing their unique student identity, with the aim to elicit their cognitive processing characteristics. The results of each psychometric test were bound with each user's unique student identity in order to map a particular CAPTCHA type (text or image) to the user and relate his/her interactions with the CAPTCHA challenge in Phase B. For the purpose of the study, in order to proceed with Phase B, all participants interacted first with all the psychometric tests in order to perform the cluster analysis for classifying the users into cognitive factor groups based on the cognitive styles' ratios and cognitive processing abilities' *z*-values (see chapter 6).

In Phase B, users enrolled in the course through a registration form by creating a username (using their student identity) and a password, and providing their age, gender and email. The registration form also included the developed CAPTCHA mechanism which required users to solve either a text-recognition or an image-recognition CAPTCHA challenge that was decided based on their cognitive styles (these were retrieved from the database according to the provided student identity). With the aim to investigate the effects of cognitive processing abilities of users on the complexity level of CAPTCHA challenges, the system randomly provided different levels of CAPTCHA complexity so that half of the users would interact with a baseline complexity CAPTCHA and the other half with a higher complex CAPTCHA. The allocation was based on the users' cognitive processing abilities so that the complexity levels were balanced across all user groups (limited and enhanced cognitive processing abilities).

A total of 125 undergraduate Electrical Engineering students participated (48 male, 77 female, age 18-28, mean 20). A total of 125 CAPTCHA sessions have been recorded.

7.10.1 User Groups

For our analysis, we separated users in three categories based on cognitive styles (Verbal/Imager/Intermediate) and in two categories based on cognitive processing abilities (limited/enhanced). Table 26 summarizes the number of users in each group.

Table 26. Number of users per cognitive styles' and cognitive processing abilities' group

Cognitive Processing Abilities	**Cognitive Styles**			
	Verbals	**Imagers**	**Intermediates**	**Total**
Limited	21	15	11	47
Enhanced	38	28	12	78
Total	59	43	23	125

In this study we aimed to investigate whether cognitive processing abilities of users affect task efficiency and effectiveness of both text- and image-recognition CAPTCHA. Two separate analyses were performed for text-recognition and image-recognition CAPTCHA interactions since the allocation of CAPTCHA type (text or image) was based on the Verbal/ Imager cognitive styles' dimension. Given the between-subject study design (the allocation of CAPTCHA complexity was split randomly to users based on their cognitive processing abilities), we conducted the analysis of variance (ANOVA) test. Additional data measures such as number of CAPTCHA refreshes are also reported.

7.10.2 Task Completion Efficiency and Effectiveness of Text-recognition CAPTCHA

A two by two way factorial analysis of variance (ANOVA) was conducted aiming to examine main effects and interactions between the users' cognitive processing abilities (i.e., limited, enhanced) and CAPTCHA complexity level (i.e., baseline, higher) over the time needed to solve a text-recognition CAPTCHA challenge. We summarize the results in Figure 67.

Results indicate that complexity level (baseline/ higher) has a main effect on task completion time ($F(1,82)=5.735$, $p=0.019$, *partial* $\eta^2=0.068$). Such a result was rather expected given the increased number and added complexity of the characters. In addition, there was a main effect of cognitive processing abilities on time to complete ($F(1,82)=4.434$, $p=0.038$, *partial* $\eta^2=0.054$) since users with enhanced cognitive processing abilities were significantly faster in solving both types of CAPTCHA complexity designs compared to users with limited cognitive processing abilities. Furthermore, there was no interaction effect between cognitive processing abilities and complexity level on the time to complete ($F(1,82)=2.028$, $p=0.158$, *partial* $\eta 2=0.025$). Pairwise comparisons between baseline and high complexity levels (Table 27) revealed that users with limited cognitive processing abilities completed the baseline level CAPTCHA significantly faster compared to the high complex CAPTCHA ($MD=-6.006$, $SE=2.355$; $F(1,78)=6.504$, $p=0.013$, *partial* $\eta 2=0.077$). In

contrast, no significant differences were observed between baseline and higher levels of CAPTCHA complexity for users with enhanced cognitive processing abilities (*MD*=-1.526, *SE*=2.085; $F(1,78)=0.536$, $p=0.466$, *partial* $\eta^2=0.007$).

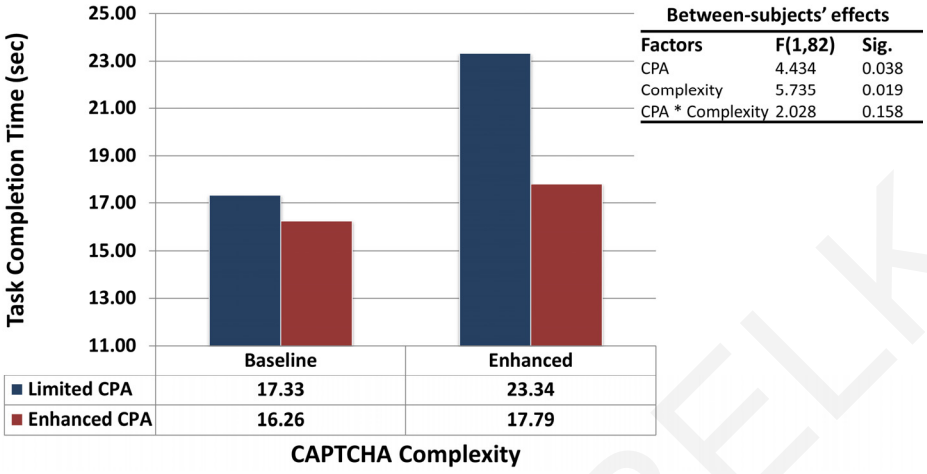


Figure 67. Users' cognitive processing abilities (CPA) and text-recognition CAPTCHA task efficiency

Such a result suggests that CAPTCHA with higher complexity could be provided to users with enhanced cognitive processing abilities given that the usability in terms of task efficiency is not significantly decreased. In the context of a personalization system, increasing the CAPTCHA complexity to users with enhanced cognitive processing abilities could increase the security level of the CAPTCHA at a rather small cost to usability. In contrast, it is suggested not to provide highly complex CAPTCHA (but rather a baseline complexity level) to users with limited cognitive processing abilities since this would increase significantly the CAPTCHA task completion time.

Table 27. Pairwise comparisons of CAPTCHA complexity per cognitive processing abilities' group regarding task efficiency

Cognitive Processing Abilities	**(I) CAPTCHA**	**(J) CAPTCHA**	**Mean Diff. (I-J)**	**Sig.**
Limited	Baseline	Higher	-6.006	=0.013
Enhanced	Baseline	Higher	-1.526	=0.466

For task effectiveness, a two by two way factorial analysis of variance (ANOVA) was conducted to investigate whether cognitive processing abilities of users have an effect on success rate (Figure 68). Results revealed a main effect of complexity on success rate ($F(1,82)=4.050$, $p=0.048$, *partial* $\eta^2=0.049$) since the success rate of baseline complexity CAPTCHA was overall higher compared to the higher complex CAPTCHA. There was also a main effect of cognitive processing abilities on the success rate of text-recognition CAPTCHA ($F(1,82)=4.109$, $p=0.046$, *partial* $\eta^2=0.05$) since users with enhanced cognitive processing abilities had a higher success rate in both types of complexity levels.

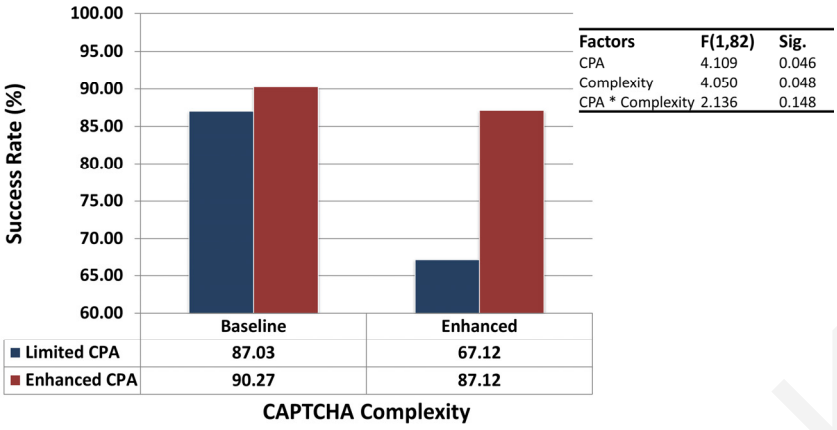


Figure 68. Users' cognitive processing abilities (CPA) and text-recognition CAPTCHA task success rate

Results suggest that highly complex text-recognition CAPTCHA hinder the usability in terms of task effectiveness for users with limited cognitive processing abilities since they were significantly less effective in solving the highly complex CAPTCHA compared to the baseline complexity CAPTCHA (Baseline-Higher CAPTCHA: *MD*=19.908, *SE*=8.580; *F*(1,78)=5.383, *p*=0.023, *partial* η^2=0.065). In addition, pairwise comparisons between limited and enhanced user groups revealed that in the case of baseline level CAPTCHA, no significant differences were observed between the two user groups (Limited-Enhanced: *MD*=-3.241, *SE*=8.026; *F*(1,78)=0.163, *p*=0.687, *partial* η^2=0.002), whereas in the case of high level CAPTCHA, users with enhanced cognitive processing abilities had significant higher success rates than those with limited abilities (Limited-Enhanced: *MD*=-19.992, *SE*=8.181; *F*(1,78)=5.972, *p*=0.017, *partial* η^2=0.071).

7.10.3 Task Completion Efficiency and Effectiveness of Image-recognition CAPTCHA

The same ANOVA analysis was conducted for image-based interactions as the one conducted for text-based interactions. We summarize the results in Figure 69.

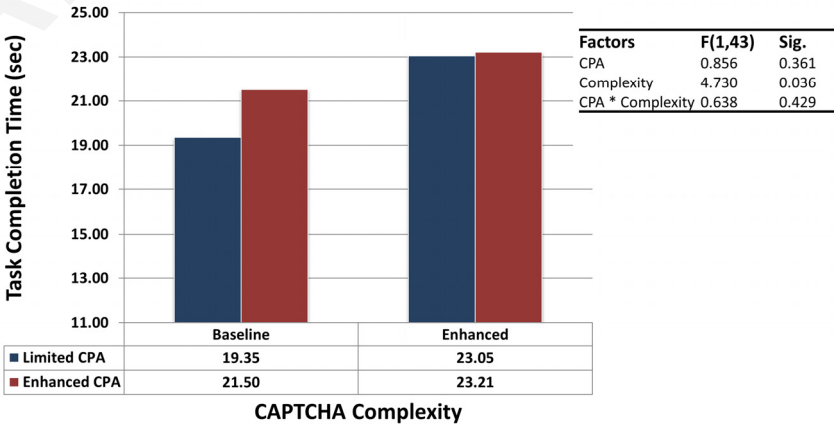


Figure 69. Users' cognitive processing abilities (CPA) and image-recognition CAPTCHA task efficiency

Similarly to the text-recognition CAPTCHA analysis, complexity level (baseline/higher) has a main effect on task completion time ($F(1,43)=4.730$, $p=0.036$, *partial* $\eta^2=0.108$) since users across all groups performed faster in the baseline complexity image-recognition CAPTCHA. Furthermore, cognitive processing abilities did not have a main effect on task completion efficiency ($F(1,43)=0.856$, $p=0.361$, *partial* $\eta^2=0.021$). Also, there was no interaction effect between cognitive processing abilities and CAPTCHA complexity on time to complete the image challenge ($F(1,43)=0.638$, $p=0.429$, *partial* $\eta^2=0.016$). Based on the results we suggest providing the same baseline ASIRRA version (12 colored images) to both users with limited and enhanced cognitive processing abilities. More images and additional security measures could be provided for increasing the security of ASIRRA that would however decrease considerably its task completion efficiency for both user types.

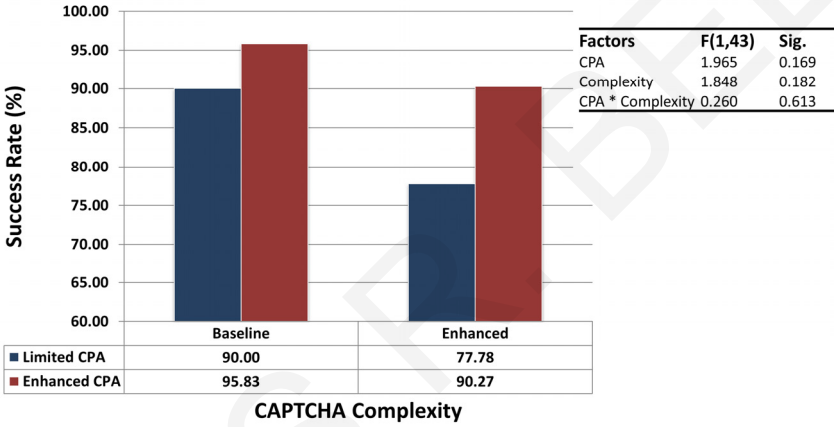


Figure 70. Users' cognitive processing abilities (CPA) and image-recognition CAPTCHA task success rate

Finally, regarding task effectiveness (Figure 70), based on descriptive statistics we observe that the success rate is decreased from baseline to higher complexity image-based CAPTCHA (especially for users with limited cognitive processing abilities). However, based on the ANOVA test analyses, results did not reveal a main effect of complexity on success rate ($F(1,43)=1.848$, $p=0.182$, *partial* $\eta^2=0.045$). Also, there was no main effect of cognitive processing abilities on the success rate of image-recognition CAPTCHA ($F(1,43)=1.965$, $p=0.169$, *partial* $\eta^2=0.048$).

7.10.4 Complementary Data Measures

The number of refreshes was recorded as complementary data measures.

Table **28** summarizes the number of refreshes per user group, CAPTCHA type and complexity level. The Mann-Whitney U test did not reveal significant differences between the user groups and CAPTCHA complexity levels on the number of refreshes.

Table 28. Number of refreshes per cognitive processing abilities' (CPA) group (limited/ enhanced), CAPTCHA type (text/ image) and complexity level (baseline/ higher)

CAPTCHA (complexity)	Limited CPA	Enhanced CPA	Total
Text (Baseline)	1	2	3
Text (Higher)	3	4	7
Image (Baseline)	2	2	4
Image (Higher)	1	0	1

7.10.5 Main Findings

Analysis of results demonstrated several main effects of cognitive processing characteristics of users on preference and task performance of different visual designs of CAPTCHA challenges. **Regarding task efficiency and effectiveness, users with limited cognitive processing abilities performed significantly worse in high complex CAPTCHA designs than in baseline designs.** On the other hand, users with enhanced cognitive processing abilities performed similarly well in high complex designs as no significant differences where observed between interactions that took place with baseline and high complex designs. In the case of image-recognition CAPTCHA, users of both groups performed worse in the high complex design than in the baseline design.

Figure 71 provides a visual illustration of the main effects of users' cognitive processing abilities (limited/enhanced) on CAPTCHA performance. The vertical lines show the effect's strength of the particular cognitive characteristic (i.e., limited/ enhanced cognitive processing abilities (CPA)) on the usability metrics investigated (i.e., user preference, task completion, success rate) with respect to the different CAPTCHA designs (i.e., text vs. image, and baseline vs. higher complexity). The horizontal dark line distinguishes the CAPTCHA designs (text vs. image, baseline vs. higher complexity).

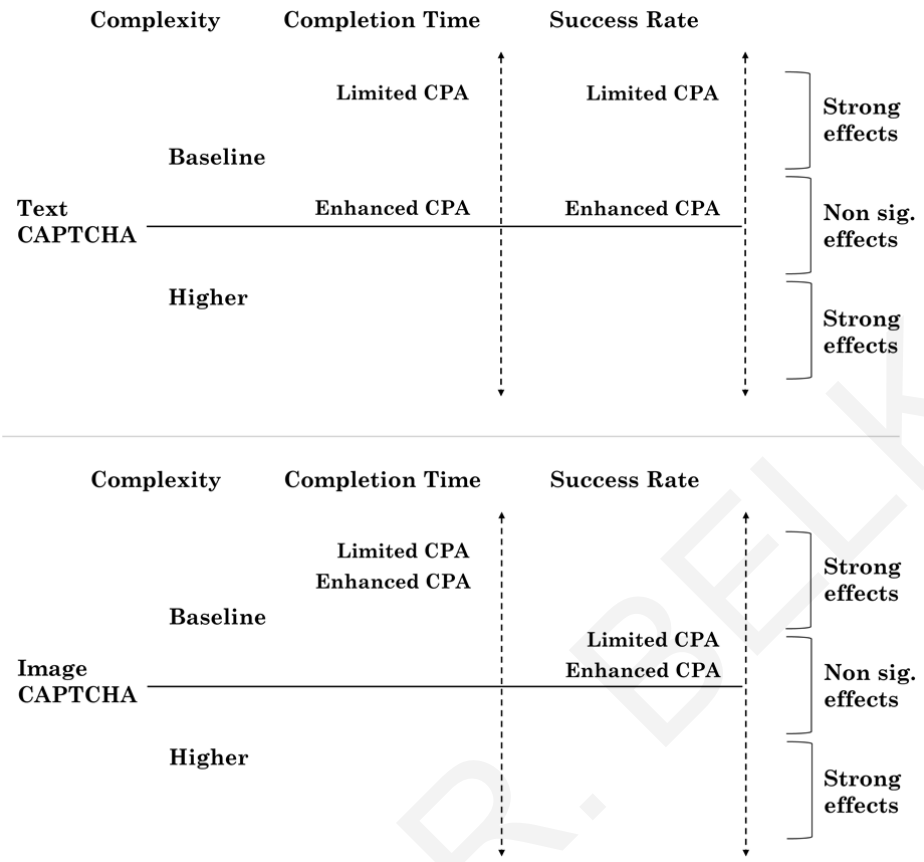


Figure 71. Main effects of users' cognitive processing abilities (CPA) on CAPTCHA performance

We list the main findings below:

- With regards to task performance (efficiency and effectiveness), this research work suggests providing a baseline complexity level of text-based CAPTCHA to users with limited cognitive processing abilities since they were negatively affected by the increase of character distortion and noise in the challenge.
- A highly complex text-based CAPTCHA could be provided to users with enhanced cognitive processing abilities in order to increase CAPTCHA security at a rather non-significant negative cost to usability.
- Regarding image-recognition CAPTCHA, results suggest that service providers should bear in mind that increasing the complexity level of image-recognition CAPTCHA (e.g., increase the number of images), affects negatively the task completion efficiency and effectiveness for both types of users (especially user with limited cognitive processing abilities).

7.11 Summary

This chapter reported a number of user studies that aimed to increase our understanding and knowledge on supporting usable security interaction design through user modeling, and adaptivity

in user interface designs in order to assist users to accomplish efficiently and effectively comprehensive and usable authentication and CAPTCHA tasks. In particular, the purpose of the studies was to investigate human cognitive differences in information processing and their effects on user preference and task performance of different user authentication and CAPTCHA designs. All the presented studies entailed a psychometric-based survey for eliciting the users' cognitive processing characteristics, and ecological valid interaction scenarios with two complementary types of user authentication and CAPTCHA (text and image). Furthermore, the user authentication and CAPTCHA mechanisms embraced different levels of complexity in terms of number and type of characters/ images and added distortion. Results of this research provide evidence that specific human cognitive factors have a main impact on users' preference and task efficiency and effectiveness of user authentication and CAPTCHA mechanisms.

The contributions of these studies entail two important aspects: theory and application. Regarding theory, the presented studies provide evidence that socio-cognitive theories, like the reported human cognitive theories, can be considered as applicable analysis frameworks in understanding deeper user authentication- and CAPTCHA-related tasks. Such frameworks are necessary given the heterogeneity of users and the globalization of today's services and applications. In particular, results of the studies can be interpreted under the light of cognitive processing styles and abilities as they demonstrate a main effect of human cognitive differences on user preference and task performance of different user authentication and CAPTCHA designs. Individuals with varying cognitive styles and cognitive processing abilities are affected, prefer and perform differently when interacting with different user authentication and CAPTCHA mechanisms. Thus, it is necessary that designers of such security mechanisms should consider human cognitive styles and abilities of users while interacting with the system.

Regarding application, the analysis and discussion of results underpinned the necessity for versatility in the design and development of user authentication and CAPTCHA mechanisms and suggest several recommendation rules (presented in chapter 8) for delivering personalized security mechanisms driven by the observed main effects of the studies.

In conclusion, results suggest, that enhancing current user authentication and CAPTCHA mechanisms aiming to embrace both text-based and image-based designs, with adjusted and personalized levels of complexity, could be to the users' benefit. In this context, in chapter 8 we defined and evaluated the impact of adaptation rules based on the observed main effects of human cognitive differences on user authentication- and CAPTCHA-related interactions. In particular, based on the observed main effects, a personalization mechanism was developed (reported in chapter 6) that delivers a specific user authentication and CAPTCHA type bootstrapped on the users' cognitive styles and the complexity level based on the users' cognitive processing abilities, e.g., provide low/ baseline complexity CAPTCHA challenges to users with limited cognitive processing abilities.

We envision that such a personalization approach would have many positive implications from the users' point of view since, providing security mechanisms, personalized to the users' cognitive

styles and cognitive processing abilities would support the users' efficiency of processing information cognitively as well as decrease cognitive load, and eventually improve the user experience and user acceptance of the mechanism. Overarching goal of the reported studies was to drive this research towards the design and development of a personalization framework, specializing on recommending "best-fit" security mechanism, with the aim to provide a viable alternative to the current state of "one-size-fits-all" paradigm.

CHAPTER 8: Definition and Evaluation of Adaptivity Rules and Design Guidelines

Prior targeted and stand-alone research attempts (reported in chapter 7) have shown several interaction effects between several cognitive factors and design characteristics of user authentication and CAPTCHA mechanisms. According to the main findings and effects of these studies, we have chosen to map specific human factors with design characteristics of user authentication and CAPTCHA mechanisms as follows: (i) Map human cognitive style differences (Verbal/ Imager and Wholist/ Analyst) with the type of the security mechanism (textual and graphical) since cognitive styles have shown to correlate with the type of information presented and processed in these mechanisms (Belk et al. 2012a; 2013c; 2014a; 2014b; 2015a; 2015b); and (ii) map human cognitive processing abilities (limited/enhanced) with the complexity of the mechanism (number of characters/images) since results have shown that specific elementary cognitive processes have an effect on task performance, problem solving and overall efficiency of processing and controlling information cognitively in such tasks (Belk et al. 2013a; 2013d; 2014b; 2015a).

Figure 72 illustrates the proposed mapping between the main factors of the user model. Accordingly, the mapping between the factors is performed on a two-level concept; in the first level, the high-level cognitive processes (cognitive styles) are used to decide the type of the security mechanism (textual or graphical), and in the second level, the elementary cognitive processes (i.e., speed and control of processing and working memory) decide the complexity level of the security mechanism (e.g., number and type of characters/images). Furthermore, given that our previous studies have shown that working memory capacity affects the task performance of different user authentication types (i.e., users with limited working memory capacity did not perform efficiently with graphical authentication mechanisms), a secondary mapping between elementary cognitive processes is additionally performed with the security type.

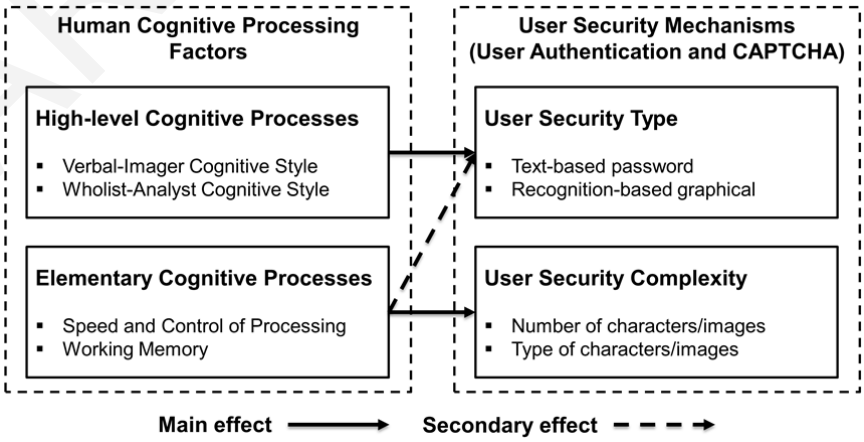


Figure 72. Mapping between human factors and design factors of user security mechanisms

In this section we will present a set of human-centered design guidelines for personalizing user authentication and CAPTCHA mechanisms. Table 29 summarizes the main criteria in order to ana-

lyze and document the usefulness of adopting a personalized approach in user authentication and CAPTCHA mechanisms. Accordingly, given existing usability, user experience and user acceptance issues in user authentication and CAPTCHA mechanisms, we propose to adapt and personalize the type and complexity level (How) of user authentication and CAPTCHA tasks (Where) based on a set of human cognitive factors (What), with the aim to assist the users during information processing and prevent cognitive load and eventually improve task completion efficiency, effectiveness and provide a positive user experience (Why).

Table 29. Guidelines for personalizing security-related tasks according to human cognitive factors

Where	Why	What	How	Guideline
User Authentication	- Assist information processing - Prevent cognitive load - Improve task completion time - Improve task effectiveness - Improve user experience	- Verbal - Wholist - Limited CPE - Limited WMC	- Textual - Standard complexity	1A (Figure 75)
		- Imager - Analyst - Limited WMC	- Textual - Standard complexity	1B (Figure 76)
		- Verbal - Wholist - Enhanced CPE - Enhanced WMC	- Textual - Higher complexity	2 (Figure 77)
		- Imager - Analyst - Enhanced WMC	- Graphical - Standard complexity	3 (Figure 78)
		- Imager - Analyst - Enhanced CPE - Enhanced WMC	- Graphical - Higher complexity	4 (Figure 79)
CAPTCHA		- Verbal - Wholist - Limited CPE - Limited WMC	- Text-recognition - Standard complexity	5 (Figure 82)
		- Verbal - Wholist - Enhanced CPE - Enhanced WMC	- Text-recognition - Higher complexity	6 (Figure 83)
		- Imager - Analyst - Limited CPE	- Image-recognition - Standard com-	7 (Figure 84)

		- Limited WMC	plexity	
		- Imager - Analyst - Enhanced CPE - Enhanced WMC	- Image-recognition - Higher com-plexity	8 (Figure 85)

In the following sections we describe in detail each guideline and their corresponding adaptation effects and human cognitive factors. For each guideline we also provide a visual illustration of the respective security mechanism and the triggered mapping of human cognitive factors and design characteristics for both user authentication and CAPTCHA mechanisms. In cases of a logical disjunction (*OR*) of two or more human factors (i.e., in case that the decision for a design factor is dependent either on the one or the other factor, e.g., a user being Verbal *OR* Wholist), we do not explicitly provide multiple guidelines, but rather we present one mutual guideline indicating the logical disjunction between the factors and the design factor decision on the figure.

8.1 Design Guidelines for User Authentication Mechanisms

The user authentication mechanism communicates to the users the personalized authentication task. Two types of user authentication are used: a text-based password mechanism (Figure 73) and a recognition-based graphical authentication mechanism (Figure 74). The text-based password mechanism requires from users to recall and enter alphanumeric characters (including numbers, a mixture of lower- and upper-case letters) and special keyboard characters in a specific sequence. The graphical authentication mechanism requires from users to recall and enter single-object images in a specific sequence (e.g., tennis ball, teddy bear, etc.). The design and development of the graphical authentication mechanism is based on well reputed recognition-based graphical authentication mechanisms; such as DejaVu (Dhamija and Perrig, 2000), PassFaces (2009) and ImagePass (Mihajlov and Jerman-Blazic, 2011). In case users forget their authentication key, an option for resetting the key is available in which a hyperlink is sent to the users' email that redirects to a form for resetting their authentication key.

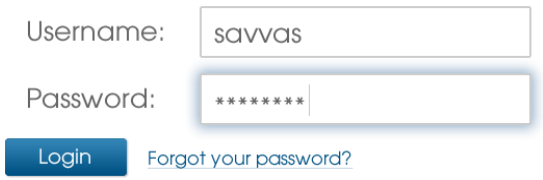


Figure 73. Text-based password mechanism

Following existing research works on design and security issues in user authentication (Renaud et al. 2013; Biddle et al. 2012; Komanduri et al. 2011), we suggest two different user authentication policies for each user authentication type; a standard and a higher complex user authentication pol-

icy. In the case of text-based passwords, a standard policy requires the creation of a password key that consists of eight alphanumeric characters with no further restrictions applied, whereas an enhanced policy requires similarly eight alphanumeric characters, entailing one upper-case letter and lower-case letters and special characters. In the case of graphical authentication mechanisms, a standard and a higher complex policy respectively requires users to enter five and eight user-selected images that are shuffled within twenty-five stable, system-assigned decoy images. Although the theoretical key space is smaller compared to traditional text-based passwords, the particular design choice is typical for recognition-based graphical authentication (Biddle et al. 2012; Renaud et al. 2013; Ma et al. 2013).

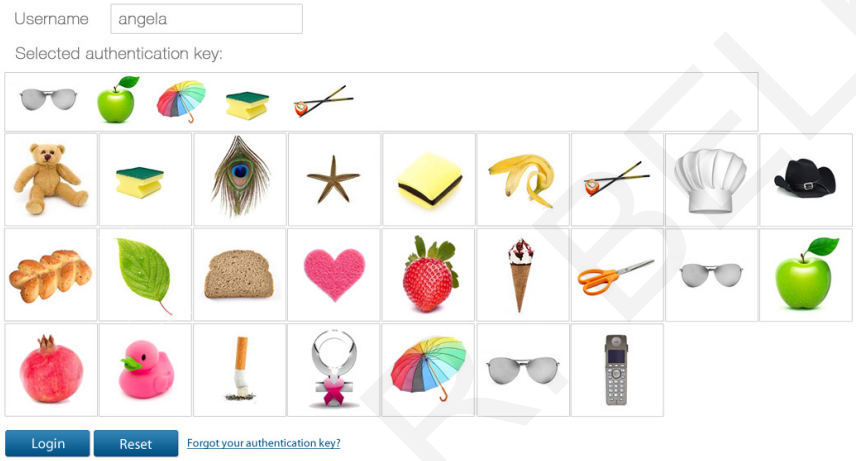


Figure 74. Recognition-based graphical authentication mechanism

8.1.1 Guideline #1: Text-based Password with Standard Complexity

Guideline #1 entails communicating a text-based password with standard complexity. This guideline is split in two sub-guidelines; Guideline #1A (Figure 75) and Guideline #1B (Figure 76). Both guidelines follow a two-step adaptation process. In Guideline #1A, at a first level, in case users have a Verbal or Wholist cognitive style we suggest to provide a text-based password mechanism since this particular type of authentication is best matched to the habitual approach of users' cognitive processing styles. The reasoning behind this choice is based on existing theory on cognitive styles and prior studies that have shown that Verbals and Wholists are more efficient in completing text-based password tasks than graphical authentication tasks (Belk et al. 2014a; 2015b). On the one hand, Verbals are more efficient in processing textual information since they process and represent information in words, whereas prior studies have shown that Wholists are not efficient and effective in visual search tasks in picture-based grids, such as recognition-based graphical authentication. At a second level, in case users have limited cognitive processing efficiency (CPE) or limited working memory capacity a standard complexity policy will be provided to them, which requires the creation of a password key of a minimum of 8 alphanumeric characters with no further restrictions applied. Given the logical disjunction between the cognitive styles and cognitive pro-

cessing factors (Verbal *OR* Wholist, Limited CPE *OR* Limited WMC), for alternative cases such as a user being Verbal *AND* Analyst, the same authentication type is applied as Guideline #1A since the decision for the text-based authentication type depends on users being Verbals or Wholists.

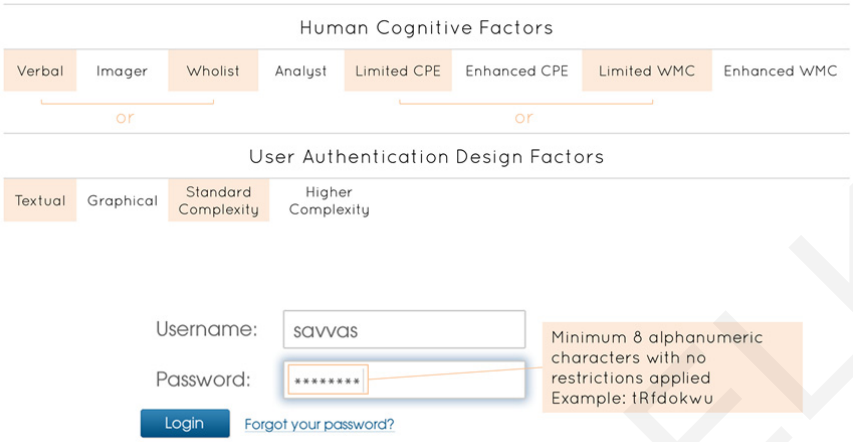


Figure 75. Guideline #1A: Text-based password with standard complexity

In Guideline #1B, users have Imager and Analyst cognitive styles. As we will see in Guideline #2, given their preferred and habitual approach in processing and representing information in mental pictures, users being Imagers and Analysts, with enhanced working memory capacity should be provided with a graphical authentication mechanism. Nevertheless, given that recognition-based graphical authentication is a more demanding process in terms of memory information retrieval than text-based authentication (text vs. pictures), in case users have limited working memory capacity, we suggest providing a text-based password mechanism with a standard complexity authentication key policy.

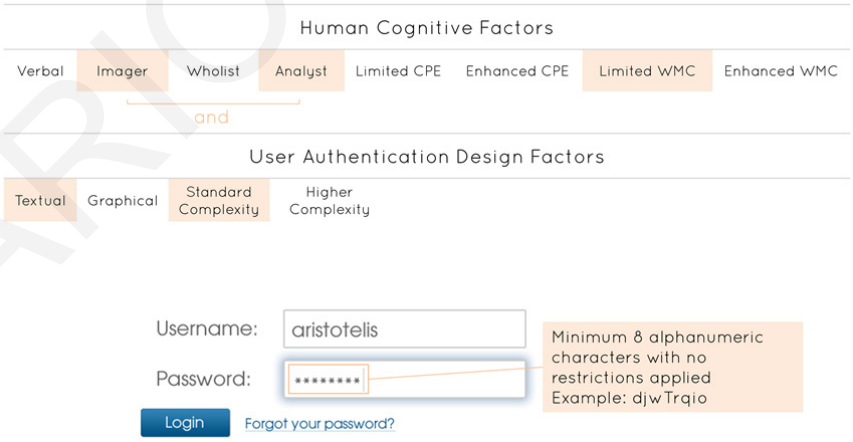


Figure 76. Guideline #1B: Text-based password with standard complexity

8.1.2 Guideline #2: Text-based Password with Higher Complexity

Guideline #2 suggests providing a text-based password with higher complexity (Figure 77). Similar to Guideline #1, Verbal or Wholist users are provided with a text-based password mechanism given

their cognitive styles' characteristics. On the other hand, in case these users have enhanced cognitive processing efficiency and enhanced working memory capacity, it is suggested to provide a higher complexity policy. Although a higher complex policy might demand more cognitive processing and eventually more time to complete the task, studies have shown that users with enhanced cognitive processing abilities are as efficient and effective in completing high complex and less complex user authentication tasks (Belk et al. 2014b). This way, depending on custom requirements of service providers, a higher complex policy can be provided to these types of users, increasing the security of the authentication key, at a rather minimum cost to usability.

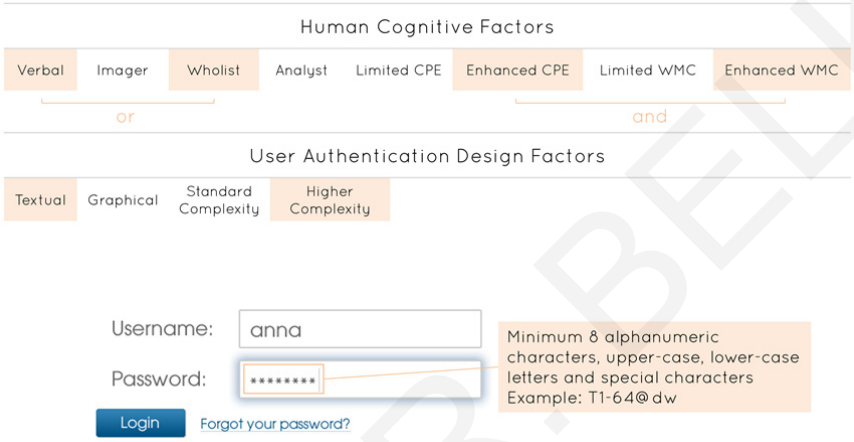


Figure 77. Guideline #2: Text-based password with higher complexity

8.1.3 Guideline #3: Recognition-based Graphical Authentication with Standard Complexity

Guideline #3 entails communicating a recognition-based graphical authentication with standard complexity (Figure 78). In this case, users are Imagers and Analysts, and have enhanced working memory capacity. The reasoning behind this guideline is based on the following hypotheses which have been validated in prior studies (see chapter 7). Imagers process and represent information in mental pictures and thus are efficient in recalling and processing graphical information, while Analysts perform efficiently on visual search tasks (Davis 1991; Messick, 1993; Goodenough and Karp 1961; Reardon and Moore 1988). In the context of recognition-based graphical user authentication, Analysts perform efficiently since recognition-based graphical authentication mechanisms entail primarily a visual search task (i.e., users are required to search for and recognize their graphical authentication key). Furthermore, Analysts have an improved visual working memory and are thus positively affected in graphical authentication tasks since the recognition and recall of images are primarily processed by utilizing the visual working memory sub-system. Furthermore, given that recognition-based graphical authentication is a more demanding process in terms memory information retrieval than text-based authentication (text vs. pictures), a prerequisite for providing a graphical authentication mechanism is that users should have enhanced working memory capacity

in order to better handle and process information during the recall process. Finally, a standard complexity policy is provided in which users are required to create an authentication key entailing a minimum of 5 images, which is typical for recognition-based graphical authentication mechanisms.

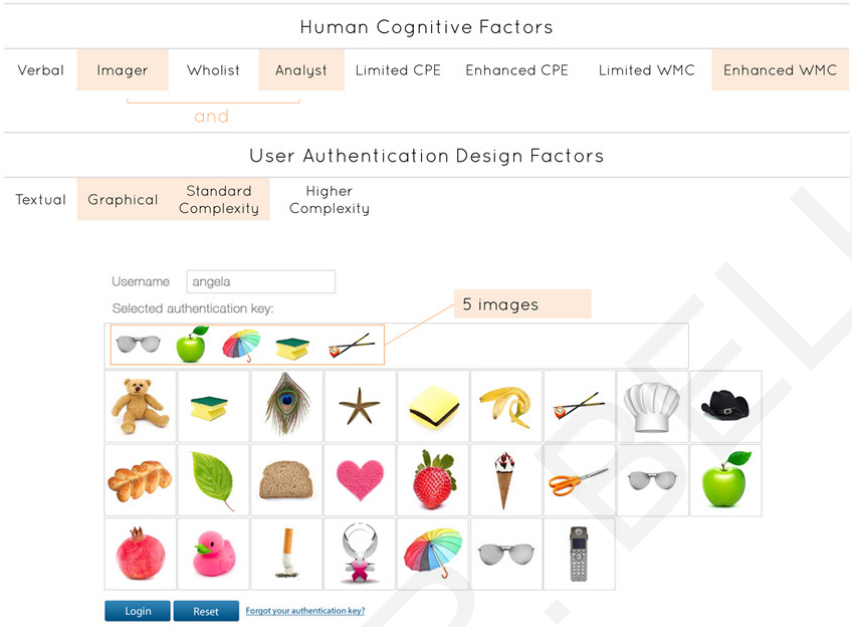


Figure 78. Guideline #3: Recognition-based graphical authentication with standard complexity

8.1.4 Guideline #4: Recognition-based Graphical Authentication with Higher Complexity

Guideline #4 suggests providing a recognition-based graphical authentication mechanism with higher complexity (Figure 79). The same principle and reasoning is followed as in Guideline #3, however in this case a higher complex policy is provided to users, requiring the creation of a graphical authentication with a minimum of 8 images. The same rules apply as in Guideline #3, with an additional prerequisite of the user having both an enhanced cognitive processing efficiency and enhanced working memory capacity.

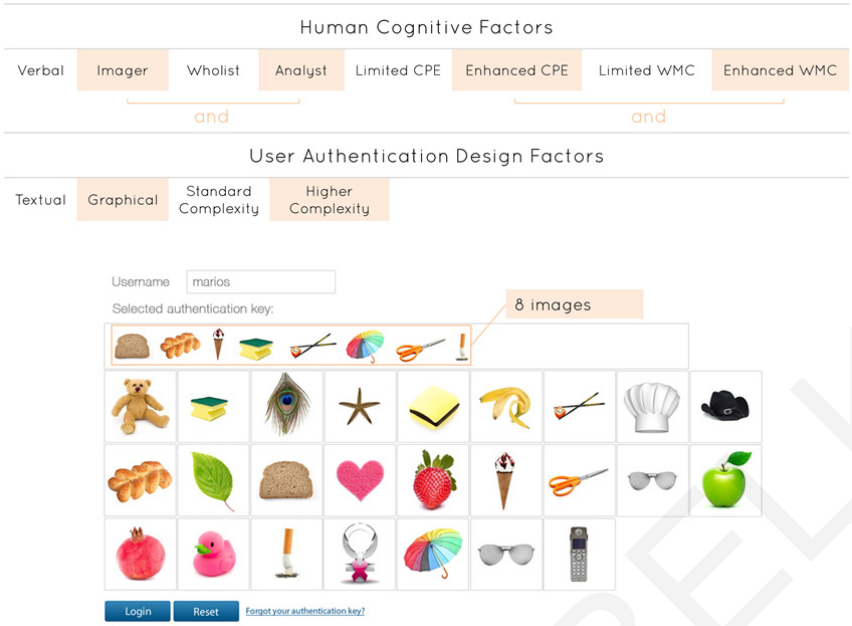


Figure 79. Guideline #4: Recognition-based graphical Authentication with higher complexity

8.2 Design Guidelines for CAPTCHA Mechanisms

The CAPTCHA mechanism communicates to the users the personalized CAPTCHA challenge. Two types of CAPTCHA mechanisms are used: A text-recognition CAPTCHA that requires from users to recognize and enter distorted alphanumeric characters, and an image-recognition CAPTCHA that requires from users to recognize and select specific images of a particular theme. The design and development of the text-recognition CAPTCHA mechanism is based on a similar technical approach followed by reCAPTCHA (von Ahn et al. 2008) as well as freely available open-source software (Securimage 2014). The image-recognition CAPTCHA mechanism is based on Microsoft ASIRRA which presents to the users images illustrating cats and dogs requiring from them to recognize and select the images that display cats (Elson et al. 2007). Both CAPTCHA mechanisms include a refresh button that initialize a challenge by reloading a new set of characters/images.

Following the design and security guidelines proposed in Bursztein et al. (2011), Zhu et al. (2010) and Golle (2008) we have designed two different complexity levels for each CAPTCHA type; a design with standard complexity and a higher complex design. In the case of text-recognition CAPTCHA, the criteria for developing the different levels of complexity are based on the number of characters presented, and the percentage of text distortion and noise illustrated in each CAPTCHA challenge. The standard complexity CAPTCHA entails a random number of 5-7 characters and 40% character rotation, collapsing and lines, while the higher complex CAPTCHA entails 8-10 characters, and 60% character rotation, collapsing and lines, as illustrated in Figure 80.

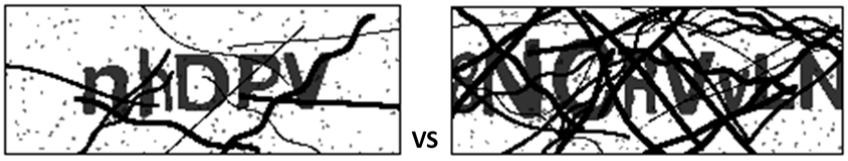


Figure 80. Standard vs. higher complexity text-recognition CAPTCHA

In the case of image-recognition CAPTCHA, the criteria for developing the different levels of complexity is based on the number of images illustrated in each challenge and the type of image color used (greyscale or color). The standard complexity CAPTCHA illustrates a 12-image challenge with colored images while the higher complexity CAPTCHA illustrates a 14-image challenge with greyscale images, as illustrated in Figure 81. The rationale behind the color change is based on the research work reported in Golle (2008), that suggests illustrating greyscale images for decreasing the attach success rate for the ASIRRA challenge. Given that a greyscale image removes important information for the efficient and effective recognition of the image, we suggest providing this type of image to users with enhanced cognitive processing abilities, since providing this to users with more limited cognitive abilities would probably hinder the efficiency and effectiveness of processing information and eventually decrease the usability of the task.

Figure 81. Standard (colored) vs. higher (greyscale) complexity image-recognition CAPTCHA

Furthermore, based on the analysis of the CAPTCHA study reported in sections 7.8 and 7.10, although Imagers had significant improved task completion efficiency in image-recognition CAPTCHA compared to Verbals and Intermediates, results have shown that in general, users were solving the original image-recognition CAPTCHA challenge (Microsoft ASIRRA) less efficiently compared to the text-recognition CAPTCHA. Based on our observations and experiences while conducting the studies, this might be caused due to the interaction design of the Microsoft ASIRRA implementation. In particular, the current version of Microsoft ASIRRA illustrates 12 small (40 pixels X 40 pixels) colored images and users are required to hover the mouse pointer on each image in order to view the larger version of the image, which is rather time consuming. Accordingly, we suggest not using the mouse hover technique but instead illustrating larger (120 pixels X 120 pixels) and responsive images by leveraging current CSS3 features (W3C 2015) for adapting the size of the images according to the device's screen size dimensions (mobile touch-based vs. monitor of desktop computer). Accordingly, based on the usability evaluation study of ASIRRA (Elson et al. 2007), the typical response time for recognizing a 14,400 pixels image (120 pixels X 120 pixels) is estimated to be 10.2 seconds for solving a 12-image CAPTCHA challenge, with a 98.5% per image accuracy and an overall success rate of 83.4%. Given the reported main effects of cognitive styles (Verbal/ Imager/ Intermediate) on task efficiency of text- and image-recognition CAPTCHA, in addition with the suggested visual and interaction design enhancements of the

ASIRRA challenge, we expect that personalized CAPTCHA types (e.g., image-recognition for Imagers) would significantly improve task completion efficiency.

8.2.1 Guideline #5: Text-recognition CAPTCHA with Standard Complexity

Guideline #5 suggests providing a text-recognition CAPTCHA mechanism with standard complexity (Figure 82). In this case users can have a verbal cognitive processing style or holistic cognitive processing style. The primary reason behind this suggestion is based on the fact that users are Verbals and thus have improved abilities in processing textual information. In addition, given that Wholist users do not have improved visual search abilities, which is required in image-recognition CAPTCHA, these types of users are provided with a text-recognition CAPTCHA. Furthermore, a text-based challenge with standard complexity is provided due to the fact that users have both limited cognitive processing efficiency and working memory capacity. Thus, providing a higher complex challenge which requires improved cognitive processing abilities might decrease the usability of the task.

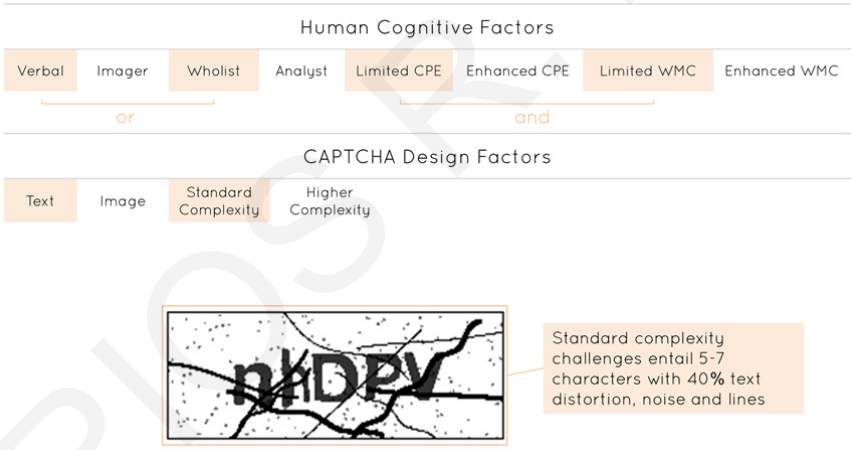


Figure 82. Guideline #5: Text-recognition CAPTCHA with standard complexity

8.2.2 Guideline #6: Text-recognition CAPTCHA with Higher Complexity

Guideline #6 involves a text-recognition CAPTCHA with higher complexity. Figure 83 illustrates an example text-based CAPTCHA challenge with high levels of text distortion, noise and lines. The same reasoning is followed for the CAPTCHA type recommendation (Verbal or Wholist), however in this case, given that users have either enhanced cognitive processing efficiency or enhanced working memory capacity, a higher complex challenge can be provided. The rationale behind this suggestion is based on prior studies that have shown that users with enhanced cognitive processing abilities perform equally well in higher and less complex CAPTCHA challenges (see chapter 7). This way, higher complex CAPTCHA challenges can be provided to users, increasing

the security of the mechanisms at a minimum cost to usability. Nevertheless, given this unequal treatment between users with limited and enhanced cognitive processing abilities (since users with enhanced abilities are provided with a more demanding CAPTCHA challenge), we suggest enhancing the CAPTCHA challenge with a user feedback mechanism for eliciting the user's preference and perceived usability of the challenge. This way, users with enhanced cognitive processing abilities, that are required to solve more demanding and highly complex CAPTCHA challenges can explicitly adapt the complexity level. Apparently, such a feedback mechanism is also dependent on the custom security requirements of the service provider, since different requirements apply in different domains and contexts of use. Given the logical disjunction between the cognitive styles and cognitive processing factors (Verbal *OR* Wholist, Enhanced CPE *OR* Enhanced WMC), for alternative cases such as a user having enhanced CPE *AND* limited WMC, the same guideline is applied as Guideline #6 since the decision for the higher complex text-based challenge depends on the prerequisite that the user should have either enhanced CPE or enhanced WMC.

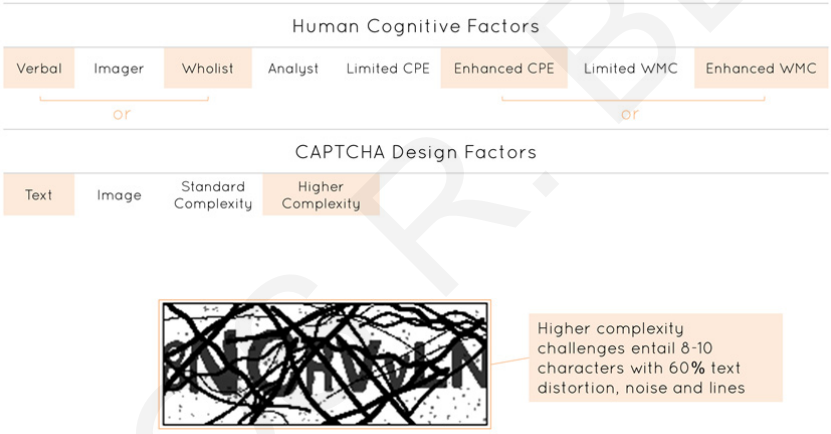


Figure 83. Guideline #6: Text-recognition CAPTCHA with higher complexity

8.2.3 Guideline #7: Image-recognition CAPTCHA with Standard Complexity

Guideline #7 suggests an image-recognition CAPTCHA mechanism with standard complexity levels (Figure 84). In this case, users have imager and analytic cognitive processing styles, providing thus an advantage in processing visual and pictorial information as well as in visual search tasks. In particular, given that image-recognition CAPTCHA entail a visual search task for distinguishing cats among dogs, Analysts have an advantage since they have improved visual search task abilities and dis-embedding skills. In addition, given that the image-recognition challenge primarily entails information processing of pictures, the Imagers' habitual and preferred approach in processing graphical information provides a cognitive processing advantage during that task. Furthermore, a standard complexity CAPTCHA challenge entailing 12 colored images is based on the fact that users have limited cognitive processing abilities or limited working memory capacity, and might be thus overwhelmed when solving more images and with greyscale color illustrations.

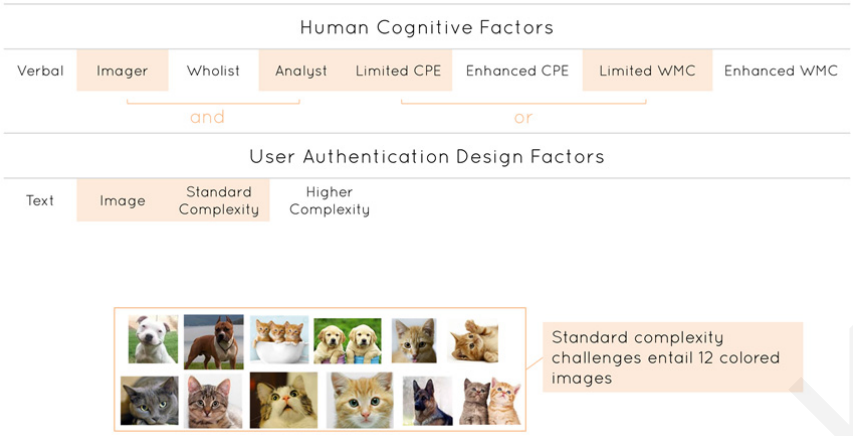


Figure 84. Guideline #7: Image-recognition CAPTCHA with standard complexity

8.2.4 Guideline #8: Image-recognition CAPTCHA with Higher Complexity

Guideline #8 suggests an image-recognition CAPTCHA challenge with higher complexity (Figure 85). Similarly to Guideline #7, an image-recognition CAPTCHA is provided due to the fact that users have an imager and analytic cognitive style providing thus an advantage in cognitive processing over text-based information. Furthermore, in this case a higher complex challenge is provided since users have enhanced cognitive processing abilities and enhanced working memory capacity.

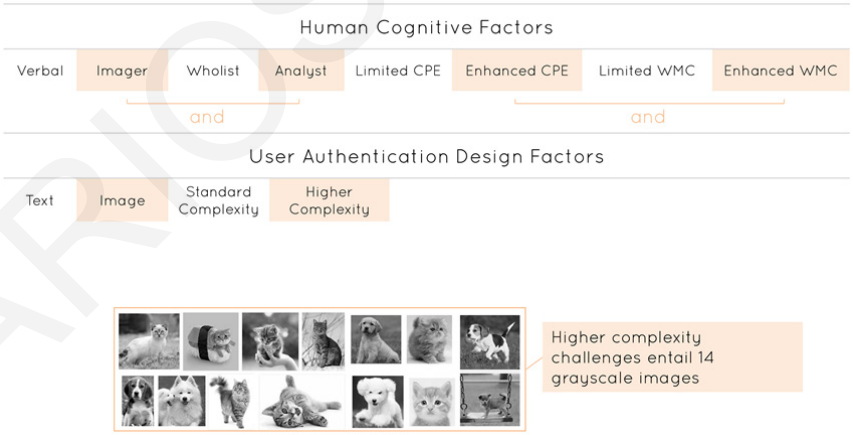


Figure 85. Guideline #8: Image-recognition CAPTCHA with higher complexity

8.3 Adaptation Paradigm in PAC based on Guidelines

Based on the aforementioned guidelines and using as an example Guideline #2, we further provide in Figure 86 an adaptation paradigm at an implementation level. Main aim is to illustrate and make more clear to the reader how the guidelines and adaptation effects (from a user interface design level) can be realized and applied to a more technical perspective using the respective algorithms

and formalizations in the PAC framework (see chapter 6). The adaptation paradigm follows a three step process: (1) the user's model characteristics are initially retrieved from the database; (2) depending on the pool of available adaptation rules, specific rules are applied and adaptation decisions are taken (e.g., whether a textual or graphical authentication mechanism should be used); and (3) based on the generated set of adaptation decisions, a rule-based mechanism is run in which the personalized security type and complexity is communicated to the user interface.

According to Figure 86, in Step 1 a client-side script calls the Web server for retrieving the user model characteristics of the user. In this particular example the user is 25 years old, has Verbal and Wholist cognitive styles and has enhanced cognitive processing abilities and working memory capacity. In Step 2, the system calls the adaptation engine *r* which is responsible to generate a set of recommendations (*R'*) for a user u_i using the user model um(u_i) and a set of adaptation rules (*AR*) which are based on the abovementioned design guidelines. According to the set of all available recommendations *R* in the system, a subset *R'* is retrieved for that particular user. In this case, Guideline #2 is chosen and applied which entails communicating a text-based password mechanism with a higher complexity policy level. Finally, in Step 3, the generated recommendation *R'* are sent to a server-side script in order to generate the personalized user authentication mechanism based on the suggested recommendations.

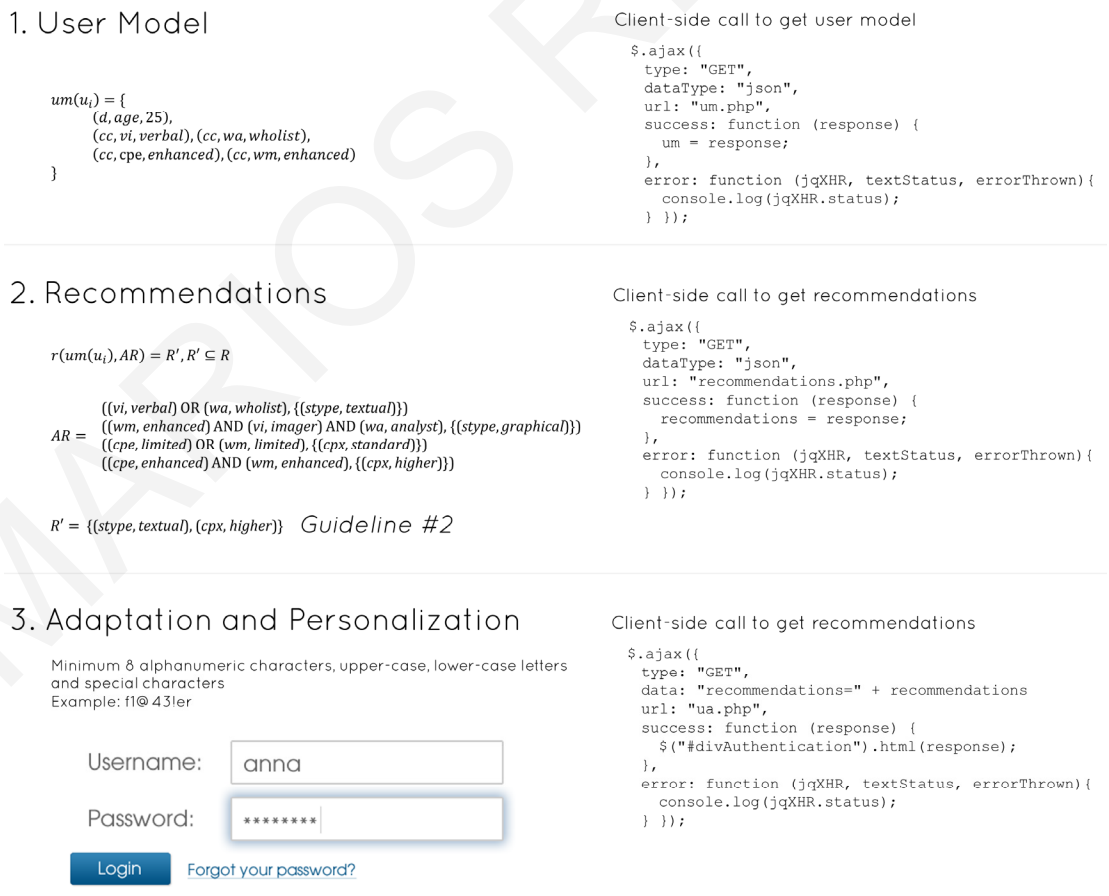


Figure 86. An adaptation paradigm based on Guideline #2

8.4 Evaluation

In further support of the abovementioned guidelines we next present a related user study. Main aim is to practically recognize the added value of aligning these mechanisms to the unique intrinsic characteristics of users based on the suggested design conditions and adaptation effects. In this respect, a within-subjects study based on a match-mismatch approach was followed, evaluating the users' task completion efficiency and effectiveness when interacting with the personalized and non-personalized security task. We further present the method and developed hypotheses of the study.

8.4.1 Study Design Methodology

The user study was applied in a number of laboratory sessions for a specific computer science module for a period of three months. Both user authentication and CAPTCHA mechanisms were embedded in the laboratory's Web-site in which students were required to interact for viewing and downloading their material related to their daily course. Main aim of this process was to increase the ecological validity of the users' interactions with the two security mechanisms since the Web-site would be used by the students in a real-life scenario. Thus, their interactions with the security mechanisms would be performed as usual without the intervention of any experimental equipment or person. The user study lasted for three months and was split in four phases based on a within-subjects design as follows.

Phase A – User Modeling

The first month of the study was dedicated to classify the participants into different groups based on their performance scores on a series of specially designed cognitive factor elicitation tools which were part of the user modeling module of the PAC framework (see chapter 6). Controlled laboratory sessions with a maximum of 10 participants were conducted with the aim to apply the psychometric tests in a scientific right manner. Participants were first guided through an online consent form and agreed to participate in the study. Then they enrolled in the study by initially choosing a unique username and then providing demographic information (i.e., age, gender, department of studies and major). Then the participants interacted with the developed online psychometric tests to elicit their cognitive processing characteristics. For the purpose of the study, in order to proceed with Phase B, all participants had to interact first with the user modeling module in order to elicit their scores for all cognitive factors and further process the data and perform a cluster analysis for mapping each security type and complexity level to users based on the generated clusters.

Phase B – Initial User Interactions

In Phase B participants created their authentication key. In this stage, the adaptation component mapped a specific type (text-based or graphical) and complexity level (standard or higher) to each user account based on the cluster each user was assigned according to his responses to the psychometric test in Phase A. We followed a match-mismatch mapping condition aiming to evaluate the formulated adaptation rules. Within each formed user group, the conditions were randomly applied on the adaptation rules so that half of the participants would first interact with a personalized mechanism (matched condition), and half of the participants would first interact with a non-personalized mechanism (mismatched condition).

The mapped condition was constant throughout Phase B. Participants interacted with the assigned user authentication and CAPTCHA mechanisms as follows: (i) During user login in the course's laboratory course, participants were required to interact with the user authentication mechanism; and (ii) during a user action (e.g., uploading their daily lab exercise), participants were required to interact with the CAPTCHA mechanism by solving a challenge. Specific IP address monitoring techniques were applied in the course's Web-site so that it would be accessible only from the computers located at the laboratory room. The main aim of this process was to control the frequency of user interactions with the security mechanisms (the laboratory course was held twice a week). The users' interactions with the security mechanisms were recorded for one month (two sessions per week; a maximum of eight sessions for each user).

Phase C – Swapping the Security Mechanism

After Phase B, the system swapped the participants' security mechanism. In particular, participants that interacted with a matched (personalized) security mechanism in Phase B were prompted to create a new authentication key based on the mismatched condition, and vice versa. The new authentication key would be used for the same period as in Phase B (one month; two sessions per week; a maximum of eight sessions for each user). In the case of CAPTCHA mechanisms, similarly, the condition was swapped for all users and kept constant throughout Phase C. The main aim of Phase C was to engage the whole sample in both conditions for the same period of time.

Phase D – Post-study Survey

At the end of the study, a post-study questionnaire was provided to all participants aiming to elicit their perceived usability regarding their interactions with both conditions of the user authentication and CAPTCHA mechanisms. Main aim was to increase our understanding about the users' interactions with the security mechanisms and triangulate the quantitative results with qualitative measures.

8.4.2 Participants

A total of 135 students of social sciences participated in the study (62 males, 73 females, mean age 20.14). All participants had prior experience with text-based password and text-recognition CAPTCHA mechanisms. No participant had prior experience with recognition-based graphical authentication mechanisms and image-recognition CAPTCHA mechanisms.

8.4.3 User Interaction Metrics

Client-side and server-side scripts were developed to monitor the users' behavior during interaction with the user authentication and CAPTCHA mechanisms. 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). Similarly, in the case of CAPTCHA mechanisms, task efficiency and effectiveness was respectively measured based on the total time and number of attempts required to solve the CAPTCHA challenge.

8.4.4 Hypotheses

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

H_1. The time needed (efficiency) to solve a personalized security mechanism is reduced compared to a non-personalized mechanism.

H_2. The total number of attempts (effectiveness) to solve a personalized security mechanism is reduced compared to a non-personalized mechanism.

H_3. Users' perceived task usability is improved when interacting with the personalized condition compared to the non-personalized condition.

8.4.5 Analysis of User Interactions

The main aim of the study is to assess the added value of applying the suggested guidelines and adaptation rules in terms of users' task completion efficiency and effectiveness. Based on the within-subjects study design, several paired samples *t*-test analyses were run to determine differences in terms of time to complete and required attempts between user interactions with the matched (personalized) and mismatched (non-personalized) condition.

User Modeling

A total of 135 user accounts have been created during Phase A in which controlled laboratory sessions were conducted aiming to elicit the participants' cognitive characteristics. The participants' scores on each psychometric test were processed as described in chapter 6 and further fed to the user grouping engine of PAC in order to generate groups of users for each cognitive factor. The cluster analysis of the user modeling module separated users into clusters based on their processed scores of the psychometric tests. Figure 87 illustrates the participants' user model characteristics.

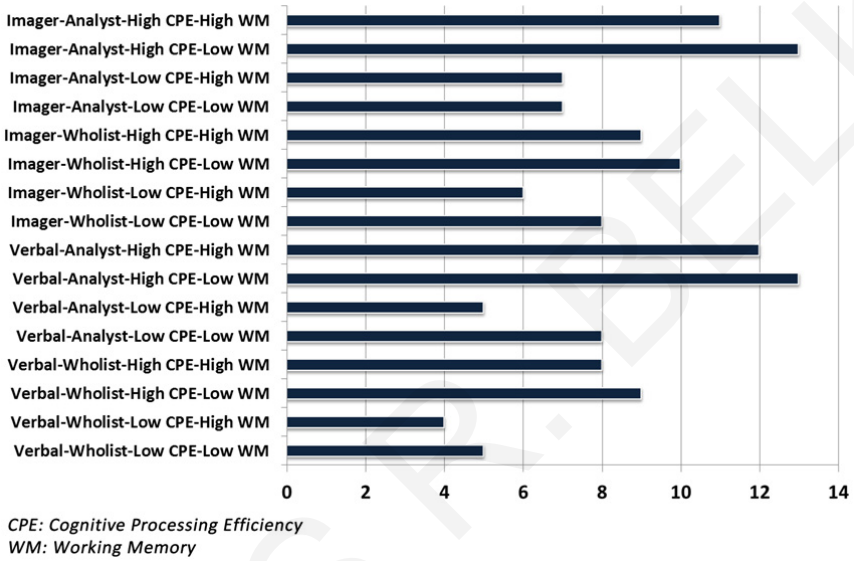


Figure 87. Distribution of participants' user models

Several independent-samples *t*-tests were conducted to determine mean differences on the processed values (e.g., cognitive style ratios) between the generated cluster groups (e.g., Verbal and Imager group). Homogeneity of variances was not violated in all cases, as assessed by Levene's test for equality of variances. Results indicate that there were significant differences among the processed values between all the clusters, indicating that the user modeling module grouped effectively the users into different clusters, and could be thus safely used in the main data analysis.

Personalized vs. Non-personalized User Authentication

Task Completion Time Comparisons. A paired-samples *t*-test was conducted to determine whether there are significant differences between the time needed to authenticate through 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.

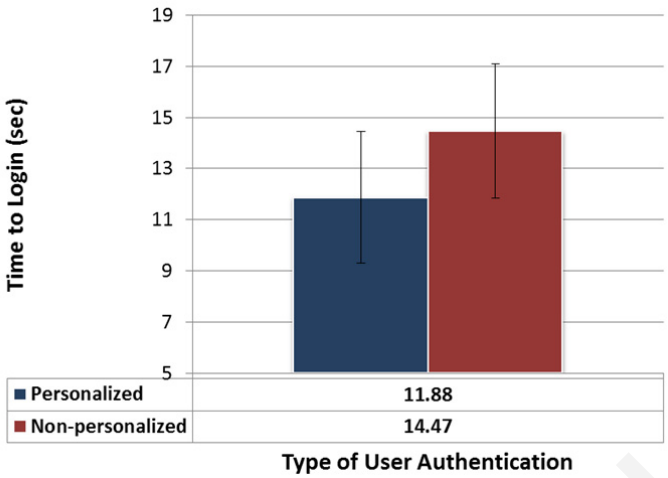


Figure 88. Means of task completion time (sec) per user authentication condition

The analysis revealed that interactions with personalized user authentication mechanisms were more efficient (M=11.88, SD=2.59) than non-personalized user authentication mechanisms (M=14.47, SD=2.64). These results were statistically significant different ($t(134)$=-7.816, p<0.001). Figure 88 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 thus support Hypothesis #1.

Furthermore, Figure 89 illustrates the time to login per session for users that interacted first with the matched condition in Phase B and then with the mismatched condition in Phase C (Match-Mismatch group, Figure 89 left) and vice versa (Mismatch-Match group, Figure 89 right). Descriptive statistics reveal that users of the mismatched condition recorded consistently the highest times to authenticate over all sessions, compared to the matched condition. Such a result indicates the increased difficulty of users in interacting with the mismatched condition further supporting Hypothesis #1.

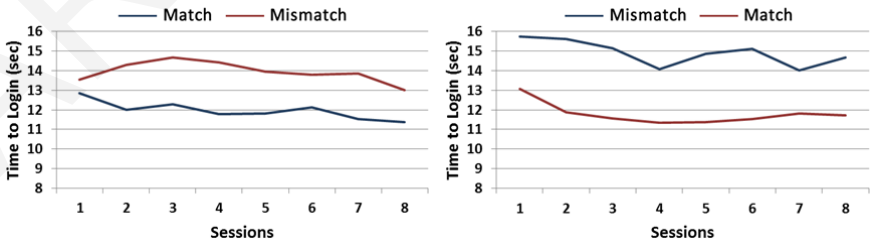


Figure 89. Means of task completion time per session for the match-mismatch group and mismatch-match group

Failure Rate. Based on the number of attempts required to login, the number of sessions with failed attempts was counted. Sessions are considered as failed when more than one attempt is required by the participant to successfully authenticate. In contrast, successful sessions are the ones in which participants authenticate successfully at first attempt. The failure rate of each user was calculated as the number of failed sessions divided by all sessions of the user. Among 2016 user

authentication sessions, 172 attempts failed (11.72% overall failure rate). A paired-samples *t*-test was conducted to determine whether there are significant differences between the failure rate through the personalized and non-personalized user authentication mechanism. The analysis revealed that the mean failure rate for personalized conditions was 8.04% (*SD*=13.04%) and for non-personalized conditions 9.43% (*SD*=15.20%). Descriptive statistics indicate an increase of failure rate in the non-personalized condition, however inferential statistics revealed that these differences were not significantly different ($t(134)=-.825$, $p=0.416$). In this respect, no safe conclusions can be drawn for supporting Hypothesis #2 since no significant differences in failure rate have been observed.

Authentication Key Resets. The total number of authentication key resets was counted along the study. Table 30 summarizes the total number of authentication key requests per condition and authentication type. In total, 19 authentication key requests were initiated throughout the study, among those requests, 2 users requested the authentication key reset three times, and the rest users requested the key reset one time. Results reveal a higher number of authentication key resets in graphical authentication across conditions compared to text-based password.

Table 30. Number of authentication key resets

	Textual	**Graphical**
Matched	2	5
Mismatched	4	8
Total	6	13

Personalized vs. Non-personalized CAPTCHA

Task Completion Time Comparisons. A paired-samples *t*-test was conducted to determine whether there are significant differences between the time needed to solve a CAPTCHA challenge through the personalized and non-personalized mechanism. The analysis revealed that users needed significant less time to solve the personalized CAPTCHA challenge (*M*=14.6, *SD*=3.07) than the non-personalized CAPTCHA challenge (*M*=16.74, *SD*=3.03). These differences were statistically different ($t(134)=-5.526$, $p=0.01$). Figure 90 illustrates the means of performances of each condition. Accordingly, the results indicate that individual differences in cognitive processing improve task completion efficiency of personalized CAPTCHA challenges and further support Hypothesis #1.

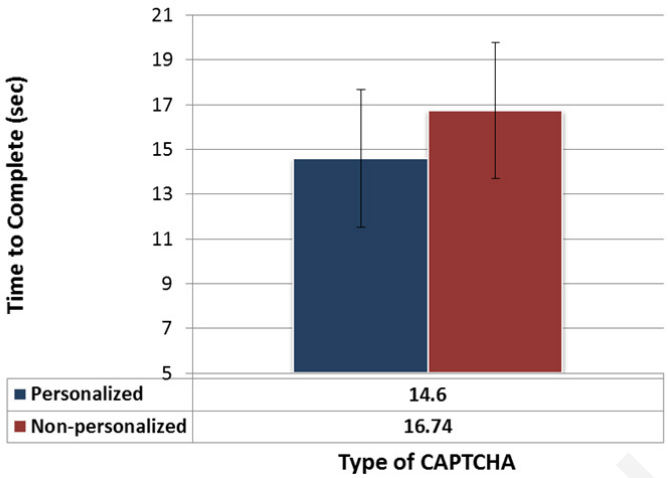


Figure 90. Means of task completion time (sec) per CAPTCHA condition

Furthermore, Figure 91 illustrates the time to solve the CAPTCHA challenge per session for users that interacted first with the matched condition for one month and then with the mismatched condition (Match-Mismatch group, Figure 91 left) and vice versa (Mismatch-Match group, Figure 91 right). Accordingly, no significant differences were observed for users that started interacting for one month with the matched condition and then with the mismatched condition. On the other hand, higher differences were observed for users that started interacting with the mismatched condition and then with the matched condition. A possible interpretation might be based on the experience factor that could have positively affected users' interactions with the mismatched condition since users first interacted with the matched condition and then with the mismatched condition. Nonetheless, descriptive statistics indicate that across groups, users were solving the personalized CAPTCHA challenge faster than the non-personalized challenge.

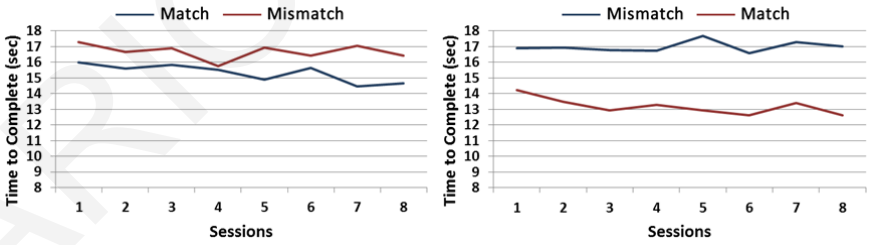


Figure 91. Means of task completion time per session for the match-mismatch group and mismatch-match group

Failure Rate. Similarly to the user authentication analysis, the number of sessions with failed attempts was counted. Among 1916 CAPTCHA sessions, 97 attempts failed (5% overall failure rate). A paired-samples *t*-test was conducted to determine whether there are significant differences between the failure rate through the personalized and non-personalized CAPTCHA mechanism. The analysis revealed that the mean failure rate for personalized conditions was 3.98% (*SD*=9.13%) and for non-personalized conditions 6.33% (*SD*=10.94%). Inferential statistics revealed that these differences were significantly different ($t(134)=-1.975$, $p=0.05$). Such a result supports Hypothesis #2

suggesting that the personalized CAPTCHA mechanism improves task effectiveness (less failure rate) compared to the non-personalized CAPTCHA mechanism.

Post-study Survey

At the end of the study, we conducted a survey aiming to validate findings of the quantitative analysis as well as to enrich our understanding about the users' perceptions and perceived usability based on their interactions with the security mechanisms. All participants were asked to rank the two conditions of both security mechanisms (user authentication and CAPTCHA) based on the following aspects: (i) The condition that the users prefer; (ii) the condition that was more efficient; and (iii) the condition that was more effective. Example questions were *"Which CAPTCHA type do you prefer?"*, *"In which authentication type did you need less time to complete the task?"*, and *"In which authentication type did you need less attempts to complete the task?"*. For each question, participants ranked the two methods with 1 and 2 to represent their first and second choice. Table 31 and Table 32 respectively list the number of participants who chose a specific user authentication and CAPTCHA condition as their first choice for each factor.

Factors related to User Authentication. A binomial statistical test was conducted to examine whether there is a preference relating personalized and non-personalized authentication mechanisms (H_0: p(personalized)=0.5 and p(non-personalized)=0.5). The result revealed that there is significant preference towards personalized mechanisms (p<0.001). In particular, the majority of users (72.5%) preferred the matched user authentication mechanism. In combination with the quantitative analysis that revealed significant better performance in the matched condition, such a result is promising for the applicability of the design guidelines and adaptation rules since the suggested recommendations have positively affected the users' preference. Regarding perceived usability, there was also a statistical significant choice towards the personalized condition (p<0.001). A total of 92 participants thought that the personalized condition was the most efficient while 43 chose the mismatched condition. Such a result further supports the quantitative results which revealed that task efficiency was improved in the personalized condition. Finally, users found the personalized condition more effective to use (p=0.025), although the quantitative analysis did not reveal significant differences in failure rates between the two conditions. To this end, results partially support Hypothesis #3 since users perceived the usability (in terms of efficiency) and preferred the personalized user authentication mechanism.

Table 31. Participants that chose a specific authentication condition as their first choice for each evaluation factor

	Matched	Mismatched
User Authentication Preference	98	37
User Authentication Efficiency	92	43
User Authentication Effectiveness	81	54

Factors related to CAPTCHA. The results revealed a high number of participants (106 participants) preferring the personalized CAPTCHA mechanism. The differences between the users' choices were significant (p<0.001). Similarly to the user authentication mechanism, such a result is promising for the applicability of the suggested approach since the recommendation based on the design guidelines and the adaptation rules has positively affected the users' preference. Regarding perceived usability, there was also a statistical significant choice towards the personalized condition (p=0.001). A total of 88 participants thought that the personalized condition was the most efficient while 47 chose the mismatched condition. Such a result further supports the quantitative results which revealed that task efficiency was improved in the personalized condition. Finally, there was no clear choice towards a condition in regards with perceived effectiveness (p=0.863). This might be based on the fact that the majority of users solved the CAPTCHA challenge at first attempt, making it difficult to compare the effectiveness of one of the two conditions. In this context, results partially support Hypothesis #3 since users perceived the usability (in terms of task completion efficiency) and preferred the personalized CAPTCHA mechanism.

Table 32. Participants that chose a specific CAPTCHA condition as their first choice for each evaluation factor

	Matched	Mismatched
CAPTCHA Preference	106	29
CAPTCHA Efficiency	88	47
CAPTCHA Effectiveness	66	69

8.4.6 Security Analysis

The analysis of results in the previous section revealed the impact and added value of personalization on usability aspects of user authentication and CAPTCHA tasks. In this section we present a security analysis of the mechanisms aiming to investigate whether this improvement in usability does not negatively affect the security of the mechanisms. Accordingly, we present an analysis on the security strength of the generated authentication keys. Regarding CAPTCHA mechanisms, we have used existing state-of-the-art mechanisms (i.e., ASIRRA) which refer to predefined design guidelines and security metrics that have been evaluated in previous works showing the security

strength of each mechanism (Bursztein et al. 2010; 2011; Elson et al. 2007; Golle 2008; Zhu et al. 2010). In addition, justifications for the choice behind the selected user authentication and CAPTCHA mechanisms, and respective policies, design guidelines and security metrics are presented in section 7.2.1 and section 7.2.2.

In this context, we focus the security analysis on the strength of the generated authentication keys (textual and graphical keys). Specifically, we compute the theoretical key space and entropy (theoretical and practical) since these are important and highly researched metrics for evaluating the security of authentication mechanisms (Komanduri et al. 2011; Shay et al. 2010; Bonneau 2012; Biddle et al. 2012). An evaluation of other types of attacks (e.g., online guessing attacks, shoulder surfing, phishing, etc.) is out of the scope of this analysis since these types of attacks are already bound to the core design of each mechanism and are not highly affected by the user study's dynamics itself. For example, online guessing attacks can be prevented in both authentication mechanisms through Human Interaction Proof mechanisms (e.g., CAPTCHA) that can be enabled after multiple unsuccessful user logins. The interested reader may find an analysis and theoretical comparison of such attacks between text-based passwords and graphical authentication mechanisms in Biddle et al. (2012).

For the security analysis of both user authentication mechanisms, and based on each provided policy, we calculated the theoretical key space, the theoretical entropy and the practical entropy of the generated authentication keys. Key space (k_p) is defined as the range of different possible values of a key. Entropy is a measure on how difficult it is to guess a password (Burr et al. 2006). In particular, entropy is measured as the expected value (in bits) of the information contained in a string (Shannon 1949), and can be related to authentication key strength by providing a lower bound on the expected number of guesses to find a text (Massey 1994). The primary difference between key space and entropy is that key space is an absolute measure of maximum combinations, whereas entropy is related to how users select from the key space. The password key space (k_p) can be related directly to the maximum entropy as follows (O'Gorman 2003):

$$H_{max} = log_2 k_p \text{ [bits]}$$

Furthermore, a true measure of Shannon's theoretical entropy cannot be computed in cases of user-chosen authentication keys since users tend to choose more memorable than random keys. Thus, in the analysis we also consider practical entropy of the generated keys following a variation of Shannon's entropy calculation described and used in Komanduri et al. (2011) and Shay et al. (2010). Since Shannon's formula allows to calculate in an additive manner, the adjusted calculation formula measures the practical entropy based on the various facets of the generated authentication keys by considering the placement of each character class (lower-case, upper-case, numbers, symbols) and image, and the content of each character and image. The final entropy is the summation of the entropy calculation of each facet.

Results

Two different text-based policies were provided; a standard policy and a higher complex policy. In the standard policy, users were required to create a text-based password with a minimum of 8 characters with no restrictions applied. In the higher complex policy, users were required to create an 8-character long password that includes lower-case characters (26 choices), upper-case characters (26 choices), numbers (10 choices), and special characters (32 choices). The key space of all possible combinations for the baseline and higher complex policies is respectively calculated as follows:

$$\textit{Standard}\ (26+26+10+32)^8 = 6.09569\text{E+}15$$

$$\textit{Higher}\ 94^8 - (68^8 + 62^8 + 84^8 - (36^8 + 58^8 + 52^8 + 26^8)) = 3.12598\text{E+}15$$

The maximum theoretical entropy for text-based keys based on the standard and higher complex policy is:

$$\textit{Standard}\ H_{max} = 52.43 \text{ bits}$$

$$\textit{Higher}\ H_{max} = 51.47 \text{ bits}$$

The key strength of the studied graphical authentication mechanism is significantly smaller than the text-based password due to the substantially smaller theoretical key space, a common issue in recognition-based graphical authentication mechanisms (Biddle et al. 2012; Ma et al. 2013). In particular, based on the provided policies, that required the selection of 5 (standard policy) and 8 (higher policy) unique images (the same image could not be selected twice in a single authentication key), the possible authentication key space of selecting these 5 or 8 images in a specific order from a set of 25 images is respectively calculated as follows:

$$\textit{Standard}\ 25 \cdot 24 \cdot 23 \cdot 22 \cdot 21 = 6.3\text{x}106$$

$$\textit{Higher}\ 28 \cdot 27 \cdot 26 \cdot 25 \cdot 24 \cdot 23 \cdot 22 \cdot 21 = 1.25319\text{E+}11$$

The maximum theoretical entropy for graphical keys based on the standard and higher complex policy is respectively as follows:

$$\textit{Standard}\ H_{max} = 22.58 \text{ bits}$$

$$\textit{Higher}\ H_{max} = 36.86 \text{ bits}$$

Furthermore, we calculated the practical entropy by following the method followed in Komanduri et al. (2011) and Shay et al. (2010). In particular, the additive nature of Shannon's formula for entropy enables us to calculate entropy for a distribution of authentication keys as a whole which results by adding the entropy based on each facet of the authentication (e.g., we separately estimate the entropy based on character/ image placement and the content of each character/ image). Accordingly, text-based password entropy was calculated by adding the entropy of each facet of the authentication keys (e.g., character content and character placement). For graphical authentication, we also calculated the practical entropy based on image content and placement, following a similar additive method.

Figure 92 and Figure 93 respectively illustrate the frequency of characters in all generated password keys, and the character class placement in each of the positions of the password. Figure 94

and Figure 95 respectively illustrate the frequency of images in all generated graphical authentication keys, and the related images utilized in the authentication mechanism. Accordingly, we have calculated the practical entropy of each authentication key facet. Table 33 summarizes the theoretical entropy and total practical entropy estimates based on each facet for each user authentication mechanism. Accordingly, the total practical entropy estimates in both mechanisms are lower than the maximum theoretical entropy. Also, some entropy values are known deterministically once the other facets are known (e.g., where lower-case characters are placed).

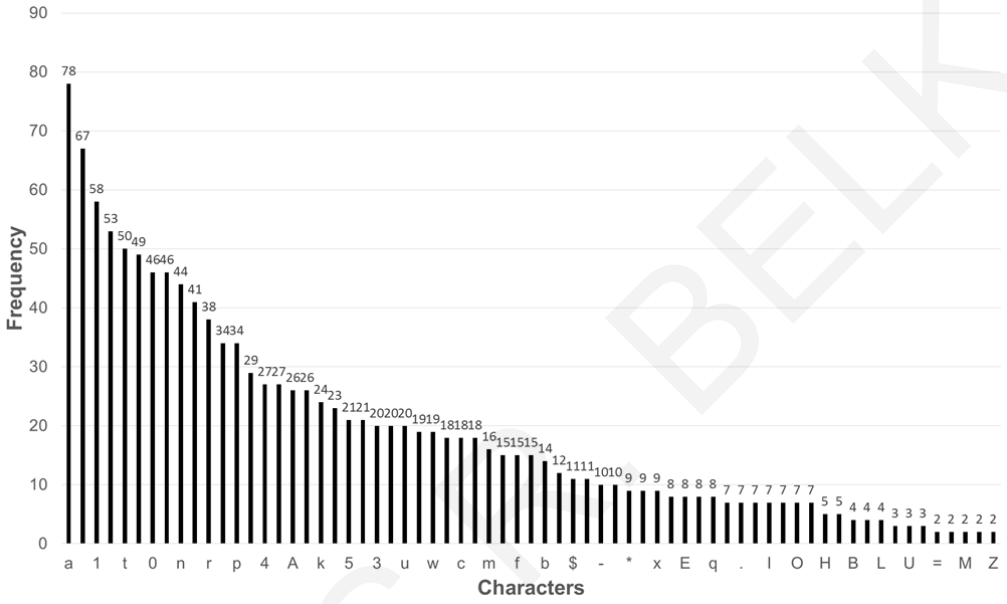
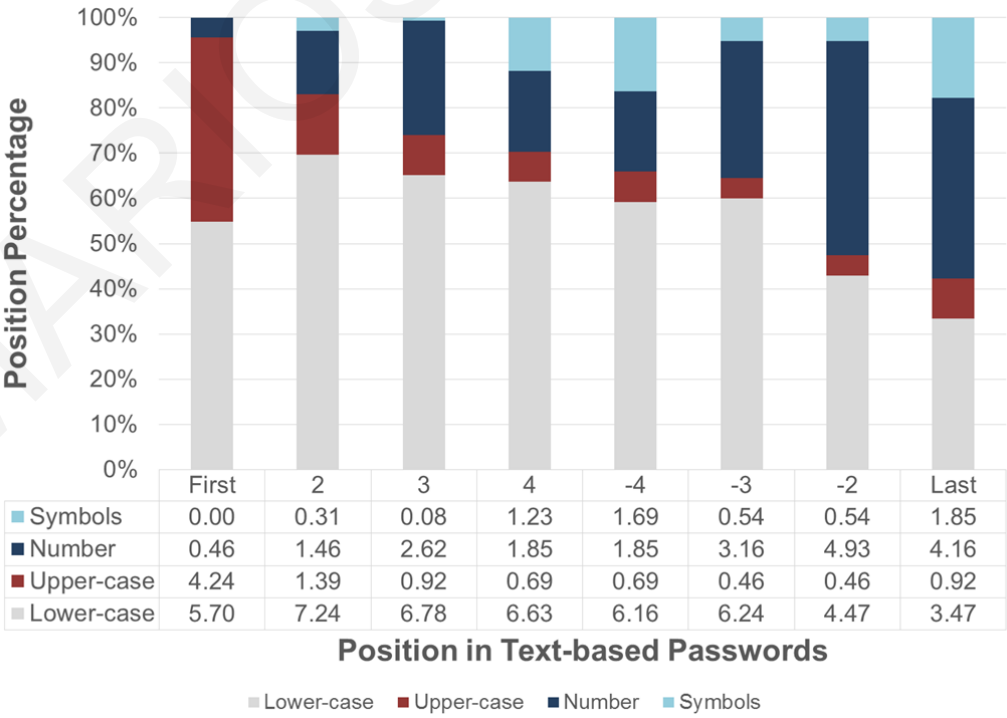


Figure 92. Frequency of characters in the generated text-based passwords



	First	2	3	4	-4	-3	-2	Last
Symbols	0.00	0.31	0.08	1.23	1.69	0.54	0.54	1.85
Number	0.46	1.46	2.62	1.85	1.85	3.16	4.93	4.16
Upper-case	4.24	1.39	0.92	0.69	0.69	0.46	0.46	0.92
Lower-case	5.70	7.24	6.78	6.63	6.16	6.24	4.47	3.47

Figure 93. Character placement among the positions in the text-based password key

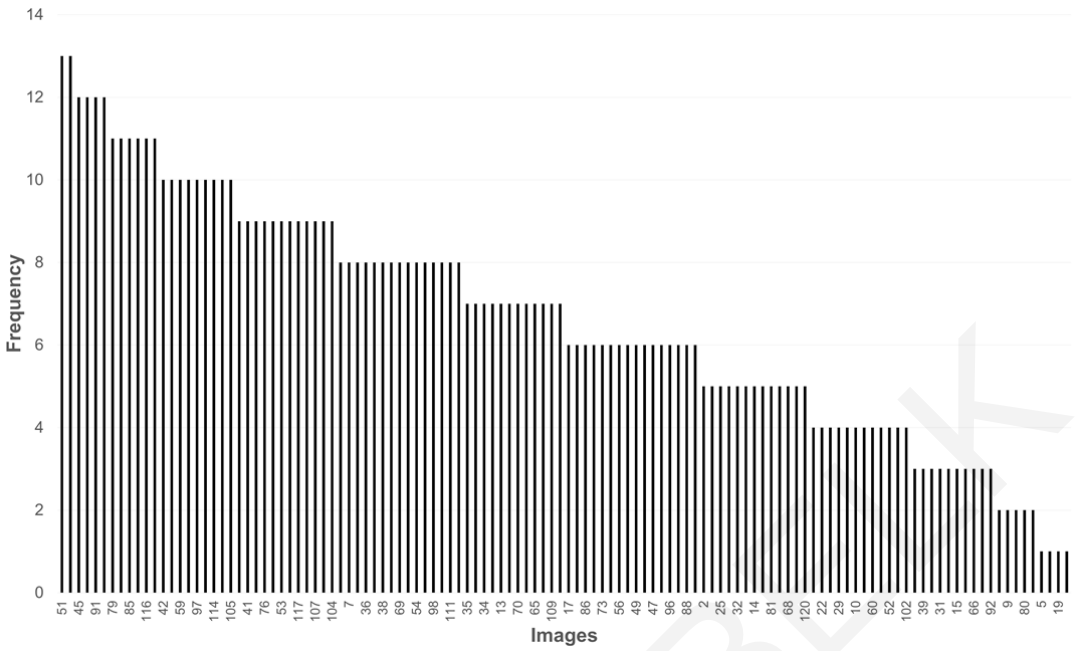


Figure 94. Frequency of images in the generated graphical authentication keys (Figure 95 illustrates the actual images and the corresponding frequency of use in the same order as the x-axis of the current figure)

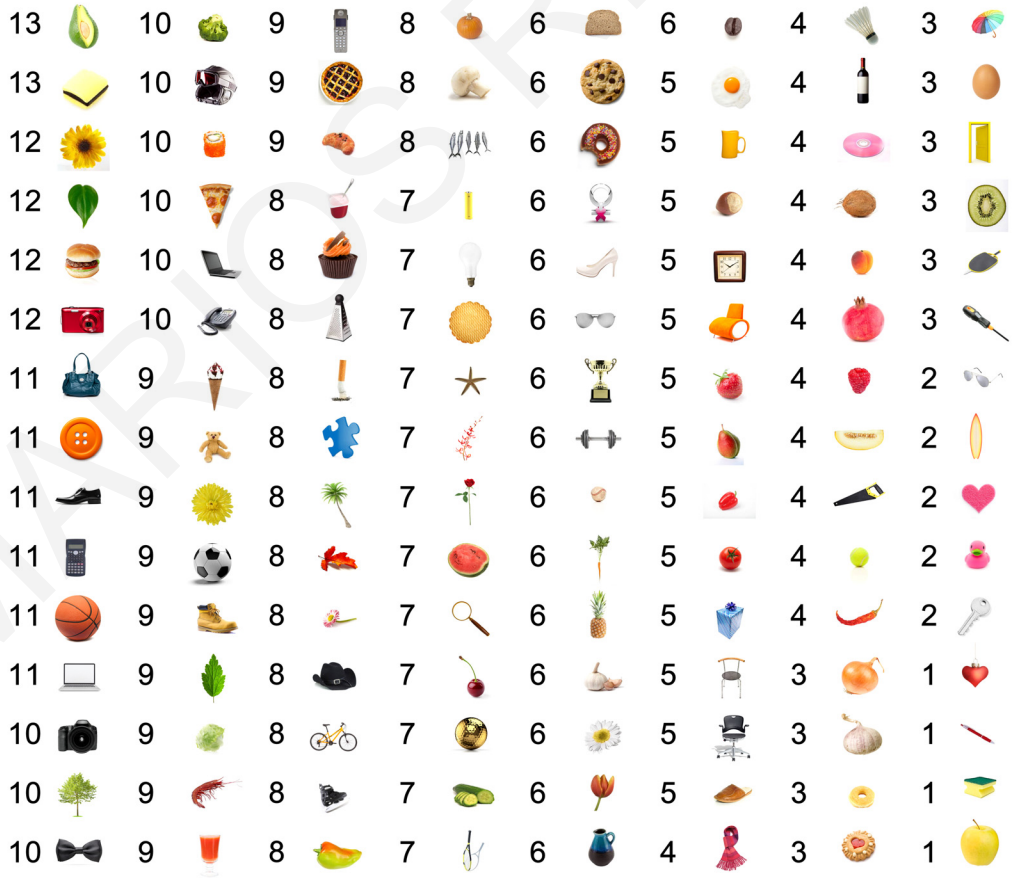


Figure 95. Actual images used and their frequency of use throughout all the generated keys

Table 33. Entropy estimates (in bits) of each authentication key facet (following the approach reported in Komanduri et al. (2011) and Shay et al. (2010))

	Matched	**Mismatched**
		Text-based Password Entropy
Entropy in Length	*2.34*	*1.55*
Entropy in Symbols		
How many symbols	0.24	0.09
Where they are	2.41	2.23
What they are	3.16	2.41
Total	*5.81*	*4.73*
Entropy in Numbers		
How many numbers	0.48	0.29
Where they are	2.65	2.96
What they are	3.20	3.11
Total	*6.33*	*6.36*
Entropy in Upper-case		
How many upper-case	0.35	0.11
Where they are	2.44	2.70
What they are	4.13	3.26
Total	*6.92*	*6.07*
Entropy in Lower-case		
How many lower-case	-	-
Where they are	-	-
What they are	4.39	4.52
Total	*4.39*	*4.52*
Practical Text Entropy	**25.79**	**23.23**
Theoretical Max Text Entropy	**52.43 (standard) / 51.47 (higher)**	
		Graphical Entropy
Entropy in Images		
How many images	1.25	1.42
Where they are	6.07	6.55
What they are	5.97	6.73
Practical Graphical Entropy	**13.29**	**14.70**
Theoretical Max Graphical Entropy	**22.58 (standard) / 36.86 (higher)**	

Main Findings

The theoretical entropy is higher than the practical entropy in both user authentication types. Furthermore, the practical entropy is higher in the text-based password mechanism than the graphical authentication mechanism. Such results were expected since research has shown that users react differently to policy rules (e.g., placing the number in the same location in the password) (Shay et al. 2010), and thus calculating theoretical entropy as a measure for security strength might not be highly accurate given the dynamic nature in such contexts of use. It is worthwhile mentioning that in both authentication types, text-based and image-based, the practical entropy is about half of the theoretical entropy. These entropy results indicate acceptable randomness in the selection of authentication keys which suggests that participants' selections were not influenced by any particular biased factors which could decrease the ecological validity of the study. Finally, we note that the practical entropy is almost equal among matched and mismatched users for a given authentication type. These results further indicate that users across different groups chose fairly random authentication keys with respect to the supported security policies.

8.5 Summary

The purpose of this chapter is to propose and evaluate a set of guidelines and adaptation effects that take into consideration a set of human cognitive processing factors and design characteristics for personalizing user authentication and CAPTCHA tasks. Our intention is to provide the most optimized condition, in terms of design type and complexity level, based on specific cognitive factors. The reader can further realize the adaptation effects and added value of this approach through a user study that investigated user interactions on given security tasks in which 135 users interacted with the personalized and the non-personalized version of user authentication and CAPTCHA mechanisms. Results revealed that matching the user security type (textual or graphical) and the complexity to users' cognitive styles and cognitive processing abilities improves task performance, primarily in terms of task completion efficiency. These findings are consistent with the theories of cognitive factors that are referred in our approach, and it seems that the challenging task of interpreting and applying these theories into adaptation rules for personalizing user authentication and CAPTCHA tasks has been at some extent successful and promising for the future.

CHAPTER 9: Conclusions and Future Work

The thesis proposed and investigated the feasibility of an alternative approach to current state-of-the-art practices of user authentication and CAPTCHA; personalizing security-related tasks to the user's cognitive processing styles and abilities. Such an endeavor is considered valuable for the design and the deployment of more usable human-computer interaction processes with the aim to offer personalized and adaptive security mechanisms aiming to assist users to accomplish efficiently and effectively comprehensive and usable security tasks.

The problem was approached through a three-phase methodological approach that aimed to gradually build a personalization framework specializing on communicating the "best-fit" security type and complexity level based on the users' cognitive processing styles and abilities. In the first phase, we investigated whether particular human cognitive factors, derived from validated theories in cognitive psychology, have a main effect of users' preference and task performance related to different designs of user authentication and CAPTCHA tasks. For the purpose of this phase we have designed multiple experimental studies which entailed credible psychometric-based tests for eliciting the users' cognitive characteristics, and ecological-valid interaction scenarios of users interacting with user authentication and/or CAPTCHA mechanisms as part of real-life tasks. The results of the studies can be interpreted under the light of the cognitive theories used in this work as they demonstrate a main effect of particular cognitive factors on both task performance and user preference related to various types of user authentication and CAPTCHA mechanisms. In the second phase of this thesis, we gradually built a personalization framework, namely PAC, whose design was driven by the observed main effects of the studies. The PAC framework is an extensible personalization framework that maps the most appropriate design factors of user authentication and CAPTCHA mechanisms to specific human cognitive factors, aiming to assist the users during information processing, prevent cognitive load and eventually provide a positive user experience. In particular, the PAC framework is conceptually composed of a user modeling module that incorporates the human factors that were identified during the analysis of state-of-the-art research works of this thesis, and a personalization module that realizes a set of adaptation effects and design guidelines that were identified based on the main effects of the studies in the first phase of the thesis. Finally, in the third phase we experimentally validated the PAC framework by realizing the user model and adaptation effects in a real-life Web-based system, in which users interacted with personalized and non-personalized user authentication and CAPTCHA tasks. Final results revealed that matching the user security type (textual or graphical) and the complexity level to users' cognitive styles and cognitive processing abilities improves task performance, primarily in terms of task completion efficiency.

9.1 Summary of Contributions

The contributions of this thesis are multi-fold which are framed by the overarching vision of supporting security-related tasks through personalization and adaptivity based on human cognitive differences in information processing. Such an endeavor is by definition interdisciplinary since it embraces the combination of principles applied to human sciences with technologies provided by information science. We summarize below the main contributions of this thesis:

1. We attempted to re-approach the area of Human-Computer Interaction and Security underlying the new user requirements that reinforce the design and development of user-centered security systems. Consequently, we underpinned the importance of adaptation and personalization in the delivery of personalized information and multi-purpose user interactions in the context of user authentication and CAPTCHA;
2. We presented a thorough analysis of state-of-the-art research works in the area of user authentication and CAPTCHA that focus on usability issues in such security mechanisms. Furthermore, we identified and summarized the most important design and security factors of each area that can be used as a reference by the reader to consider usability and security issues in the design of user authentication and CAPTCHA mechanisms;
3. We identified the importance of human factors in Web adaptation and personalization, pinpointing their dynamicity and how they can influence the design of multi-purpose interactions and interfaces. We thoroughly reviewed and presented a number of theories and models with respect to human cognition, attention, learning and how these can be extracted, modeled and interpreted in a way that could add value to systems and services by enhancing their content presentation and navigation;
4. We attempted to inclusively elaborate on the process of adaptation and personalization of hypermedia environments. We presented an extensive investigation of the adaptation and personalization fields (based on existing state-of-the-art research and reviews), on the importance of user modelling and methods of extraction; and on systems, technologies and methodologies assigned to a number of application areas trying to approach the topic from a more global perspective;
5. Based on the literature analysis we designed a high-level adaptation and personalization framework that realizes the mapping of specific theoretical human factors and dimensions with the more deterministic nature of technologies, algorithms, and functions;
6. We proposed a formalization of a human factor-based user model for personalizing security-related tasks;
7. We proposed a formalization of an adaptation engine for recommending a particular user authentication and CAPTCHA type and complexity level based on the combination of the user modeling factors;

8. We proposed an open and interoperable adaptation and personalization framework, namely PAC, by emphasizing on its modules, components and technologies used. The outcome of PAC could serve as a guide of how a number of interdisciplinary elements, attributes and functionalities can co-exist and enhance usability, satisfaction, and user experience delivered via its intelligent user interface in the context of user authentication and CAPTCHA;
9. We studied the impact of a number of human cognitive factors on user preference and task performance of different user authentication and CAPTCHA mechanisms. Based on the presented results which embrace objective quantitative data (captured data during experimentations) as well as subjective qualitative self-reporting data (focus group studies and surveys), we suggest that following a user-centered design methodology, it is necessary that designers of authentication and CAPTCHA mechanisms should clearly bear in mind individual differences of users while interacting with the system. Currently, there is a strong underlying design assumption that text-based passwords and text-recognition CAPTCHA mechanisms are the most popular and comprehensive way for user authentication and human interaction proofing (Herley and van Oorschot 2012; Bursztein et al. 2014). The results of the reported studies suggest enhancing current mechanisms aiming to embrace both text-based and graphical-based mechanisms, with adjusted levels of complexity. As the results suggest, such an approach would have many positive implications from a usability and user experience point of view since, recommending security mechanisms, personalized to the users' cognitive processing styles and abilities would increase the users' information processing efficiency, and thus improve task completion efficiency and effectiveness, and user satisfaction;
10. We proposed a set of adaptation effects and design guidelines for personalizing user authentication and CAPTCHA tasks based on human cognitive differences. These guidelines can be used by researchers and practitioners to design and develop more usable authentication and CAPTCHA mechanisms.

In this context, the outcome of this thesis has shown positive indications that the suggested cognitive-based personalization approach could provide a viable alternative direction to current "one-size-fits-all" user authentication and CAPTCHA practices, for supporting the users during information processing, improve usability of tasks and eventually provide a positive user experience. As seen through the user studies conducted, the suggested and studied cognitive factors have shown to be elements of paramount importance for the concept of personalization and the development of human-centered security mechanisms, since they have a main effect on particular design factors of user authentication and CAPTCHA mechanisms. By personalizing the security type and complexity level to the users' cognitive characteristics, it has been shown that users complete their task faster and more accurate, as well as that users with particular cognitive processing styles have a preference towards particular designs of security mechanisms. More specifically, we list below the main findings extracted throughout the user studies.

Finding A – Task completion time in text-based authentication is in general faster across users, compared to graphical authentication. Users across groups were completing that text-based password task faster than graphical tasks which might be explained by the familiarity factor.

Finding B – Verbals completed the text-based authentication task faster than Imagers. Several studies were analyzed comparing task completion differences in text-based passwords between Verbals and Imagers showing that Verbals are completing the task faster than Imagers. However, in several cases the differences were not significantly different, with Verbals being slightly faster than Imagers. An interpretation of this result can be based on the fact that all users were more familiar and experienced interacting with text-based passwords, hence no significant differences were observed in some cases between the Verbal and the Imager.

Finding C – Participants in general preferred graphical authentication mechanisms, with a significant preference of Imager users. The preference might be affected by the novelty effect of graphical authentication, however, in several studies Verbal users did not have a clear preference towards either of the two mechanisms.

Finding D – Task completion time and success rate in graphical authentication significantly differs between Verbal/ Wholist and Imager/ Analyst users. Results have shown a main effect of cognitive styles on graphical authentication. In particular, Imager/ Analyst users needed significantly less time and less attempts to complete the graphical authentication task compared to Verbal/ Wholist users.

Finding E – Desktop-based graphical authentication is less usable than text-based authentication for Wholist users, but not for Analyst users. Results revealed that in desktop-based interactions, Wholist users needed significantly more time and attempts to complete the graphical authentication task compared to the text-based task. In contrast, Analyst users performed similarly in both text-based and graphical-based authentication.

Finding F – Time to complete text-based authentication significantly differs between desktop computers and touch-based devices, but not for graphical authentication. Results revealed that the device affects text-based password interactions. In particular, analyses of touch-based user interactions revealed that in general, the time to complete text-based password tasks was significantly larger than desktop-based user interactions. In the case of graphical authentication, no significant differences were observed between desktop-based and touch-based interactions. Such a result can be based on the fact that user interactions of graphical authentication does not significantly differ in both scenarios (selecting images through mouse clicks vs. through finger touch).

Finding G – The interaction device in text-based authentication significantly affects Wholist users' task completion time, but not Analyst users. Results revealed that Wholist users had a significant increase of time to complete the text-based password task on touch-based devices compared to desktop computers, whereas Analyst users did not have significant differences in task completion time between the two interaction device types. Furthermore, the analysis of desktop-based interactions revealed no significant differences between Wholist and Analyst users in text-

based passwords, which might be explained by their familiarity with text-based passwords. However, in touch-based interactions, Analyst users were significantly faster in completing the textual password task compared to Wholist users due to their positive adaptation and independence in regards with contextual and field changes (desktop vs. touch-based).

Finding H – Cognitive processing abilities affect task completion performance of graphical authentication mechanisms. Results have shown that in graphical authentication, users with enhanced working memory and cognitive processing speed perform significantly faster than users with more limited cognitive processing abilities.

Finding I – Cognitive styles have a significant main effect on user preference and task performance of CAPTCHA challenges. Analysis of results has shown that Verbals prefer and solve significantly faster text CAPTCHA. Furthermore, there is a growing trend of Imagers preferring and solving faster image CAPTCHA.

Finding J – The interaction device affects Wholist/ Analyst users in completing the CAPTCHA task differently. Wholist users are negatively affected, in terms of task efficiency and effectiveness, when text-recognition CAPTCHA are deployed on touch-based devices.

Finding K – The interaction device has an overarching effect on CAPTCHA type preference across users. The majority of users in all user groups preferred image-recognition CAPTCHA when these were deployed on touch-based devices, compared to text-based CAPTCHA.

Finding L – Cognitive processing abilities affects task completion performance of CAPTCHA mechanisms. Results have shown that users with enhanced cognitive processing abilities solve text-recognition and image-recognition CAPTCHA challenges faster than users with limited cognitive processing abilities.

Finding M – Enhanced complexity levels of CAPTCHA challenges negatively affect users with limited cognitive processing abilities. Users with limited cognitive processing abilities perform significantly slower on enhanced complexity levels of both text-recognition and image-recognition CAPTCHA mechanisms, than limited complexity levels.

Finding N – Enhanced complexity levels of CAPTCHA challenges could be provided to users with enhanced cognitive processing abilities. A highly complex text-based CAPTCHA could be provided to users with enhanced cognitive processing abilities in order to increase CAPTCHA security at a rather non-significant negative cost to usability. Nonetheless, in the case of image-recognition CAPTCHA, high complexity levels negatively affect users with enhanced cognitive abilities which is however expected since the enhancement of complexity entails raising the number of images to recognize which inevitably increases time to complete the task.

Finding O – Personalizing the security type and complexity level to human cognitive differences improves task performance. Results revealed that matching the user security type (textual or graphical) and the complexity to users' cognitive styles and cognitive processing abilities improves task performance, primarily in terms of task completion efficiency.

9.2 Impact

The aftermath of this research effort indicates, to our knowledge, the value of human-centered adaptation and personalization as a viable alternative direction to current "one-size-fits-all" practices of user authentication and CAPTCHA mechanisms, for supporting the users during information processing, decision making and problem solving. As seen through the methods used in this thesis, the analyses and the user studies conducted, the suggested human factors figure as elements of paramount importance for the concept of personalization and the development of adaptive mechanisms, since they have a main effect on particular design characteristics of user authentication and CAPTCHA mechanisms. By personalizing the visual experience and functionality to the users' cognitive processing characteristics, it has been revealed that users are able to complete their tasks faster and more accurately, as well as those sharing (to a measurable practical extent) the same intrinsic characteristics on the subsequent psycho-metric scales have a preference towards particular designs of security mechanisms.

User authentication and CAPTCHA tasks are performed on every moment worldwide by millions of users and thus it becomes evident that having a usability flaw in such human-computer interaction cycles or even not considering usability issues while designing them, most probably will result in unacceptable trade-offs for the users and the providers in terms of time and resources. Thus, embracing usability aspects in designing usable user authentication and CAPTCHA mechanisms has become nowadays a necessity (Fidas et al. 2011; Florencio and Herley 2007).

User authentication and CAPTCHA (text, image) is primarily a human information processing task. While such security mechanisms are becoming less usable due to the increasing strength of policies and visual complexity levels (Inglesant and Sasse 2010; Bursztein et al 2014), and users demand new approaches that will adapt according to their individual characteristics (Fidas et al. 2011; Nicholson et al. 2013; Ma et al. 2013), the main impact of the presented research is that it provides an alternative point of view in delivering personalized user authentication and CAPTCHA mechanisms to users.

Results of this thesis demonstrate that the proposed approach could be considered as an alternative to current user authentication and CAPTCHA practices, since user interactions with personalized security tasks were improved in terms of task efficiency and effectiveness. In addition, analysis of results demonstrated several interaction effects between cognitive styles and cognitive processing abilities of users on task performance and user preference towards different designs of user authentication CAPTCHA. In particular, this thesis provides evidence that individual differences in cognitive processing have a main impact on users' performance and preference of user authentication and CAPTCHA tasks and accordingly suggests enhancing current security mechanisms aiming to embrace both text-based and graphical mechanisms. Such an approach would have many positive implications from a usability and user experience point of view since, recommending security mechanisms, personalized to the users' cognitive processing styles and abilities has a positive im-

pact on the users' memorability and information processing efficiency, and thus improves task completion efficiency and effectiveness, and user satisfaction.

User security tasks are critical mechanisms that are traditionally secondary tasks of the user, interrupting the primary task of interaction. For example, a user trying to post a comment in an online blog might be interrupted by a CAPTCHA challenge, requiring him to solve the challenge to prove that he is a human and not a robot. Apparently, interrupting this human-computer interaction cycle results in a less positive user experience and creates an overhead to the performance of the user's primary task of interaction. Worse, the user might not be able to complete the security task and thus abandon the main task. Thus, while the main focus in such mechanisms should be primarily on the security layer, a task that users cannot complete, could not thus justify its existence. In this respect, focusing on the user and providing a personalized challenge with the aim to assist the cognitive processing of information will minimize this overhead, as well as create a seamless interaction for users is of paramount importance. The importance of the efficiency and effectiveness of the studied security tasks in current and future deployed E-Services and applications for the society is considered to be critical 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.

We envision that the reported research will provide useful insights for practitioners and researchers to design and develop more user-centered and usable authentication and CAPTCHA mechanisms taking into consideration heterogeneity of users with unique preferences and characteristics. Considering current "one-size-fits-all" delivery approaches of user authentication and CAPTCHA, and the diversity of users, the added value of such an endeavor entails many benefits both from the users' as well as from the service providers' perspective. For the former, the design and the deployment of personalized user authentication and CAPTCHA mechanisms would support the processing of information and the tasks execution, providing more clarity and meaning on the required information. At the same time would reduce any unnecessary steps and/or complexities, increasing the decision making and eventually leading to a positive user experience. For the latter, such an (strategic) approach would increase user acceptance and satisfaction and thus would provide an enhanced experience, assisting organizations to gain the competitive advantage through the provision of personalized services. Inevitably, in this case more consistent (user) research is required, investing on the identification and documentation of users' behaviors and operations (e.g., building qualitative personas, activity flows, use cases, etc.) in order to obtain a complete understanding of how they work and consequently create designs that will match their profiles with the appropriate interaction styles.

9.3 Limitations

Although the studies reported in this thesis yielded statistical significant results, each study itself and the proposed approach entails limitations that are inherent to the multi-dimensional character and complexity of this research work. An important limitation is related to the recruitment and sample of the studies. The sample included a rather convenient sample of participants with similar profiles and educational backgrounds (i.e., undergraduate students). Furthermore, participants were more experienced with text-based passwords and text-recognition CAPTCHA than with recognition-based graphical authentication and image-recognition CAPTCHA challenges. On the other hand, we aimed to increase the internal validity of the study by recruiting participants that were experienced, rather than novice, with computer usage, user authentication and CAPTCHA tasks. Another limitation concerns the clustering of users into two extreme user groups (e.g., Verbals and Imagers). Although a number of existing research works have used a cut-off score for grouping users into two distinct groups (Hong et al. 2012; Altun and Cakan 2006), this approach might not classify individuals that fall in between the two end points (e.g., intermediates). Nevertheless, based on the formalization of PAC in chapter 6, there has been an effort to formalize an open and extendable user modeling module that elicits the users' cognitive characteristics along a continuum scale, and depending on the application domain, set the desired number of user groups (k) for mapping these with the appropriate design factors (in our case, a text-based or graphical security mechanism).

Furthermore, the suggested adaptation rules embrace new challenges from the user modeling and security perspective that need further investigation. From the user modeling perspective, a limitation of the current implementation of PAC is based on the explicit nature of the user data collection method that requires users to conduct a series of psychometric tests in order to elicit their cognitive characteristics which might decrease user acceptance and the practical feasibility of the proposed approach. In this context, there is a need to transparently elicit the users' cognitive characteristics based on their interactions and behavior in the system. Recently, we proposed a user data collection method (Belk et al. 2013b; Papatheocharous et al. 2014) that implicitly infers the user's cognitive characteristics by tracking their navigation sequence and behavior in particular sections of the system. Other related research works include the work of Chen and Liu (2008) that proposed tracking the users' behavior with navigation tools (hierarchical maps or alphabetical index) in order to elicit their cognitive styles, the work of Chang et al. (2013) that proposed an approach for detecting users' working memory capacity based on their behavior in interactive systems, and the work of Chan et al. (2014) that measured the usage of search tools in mobile interactive systems (basic vs. advanced search) in order to implicitly infer the users' cognitive styles.

From the security perspective, given that various user authentication and CAPTCHA schemes entail different security strengths and weaknesses (Renaud et al. 2013; Biddle et al. 2012; Bursztein et al. 2011; 2014), the recommendation of a particular type and complexity level would change the

security metrics of the mechanism. For example, recognition-based graphical authentication schemes are more vulnerable to offline guessing attacks since these have a significant smaller theoretical key space than traditional text-based passwords (assuming that the level of usability remains at reasonable levels) (Biddle et al. 2012). In this respect, depending on the application domain and custom requirements of the service provider, the recommendation rules of the PAC framework could be further extended with several security factors and policies (e.g., increase the number of images in the challenge) in order to meet the security requirements of the provider.

9.4 Ethical Considerations

An intrinsic challenge of the presented research relates to the security analysis of the user generated text-based and graphical keys provided, in order to contextualize the usability results. Aiming to effectively quantify the generated authentication keys, we required access to the plaintext of the generated keys which raises several security, privacy and ethical issues. From a security perspective, in such a scenario, a participant could reuse a password from an existing account since research has shown that people reuse passwords across multiple accounts (Florencio and Herley 2007). Access to the plaintext password by a malicious person raises severe security issues for the participants. In order to avoid this issue, and at the same time quantify the security strength of the keys for the purpose of this research, we hashed and stored the authentication key in the database of the actual user authentication system, along with the rest data of the user (e.g., username, demographics, etc.). Instead, the plaintext authentication key (along with the plain cognitive factor classification and assigned conditions) was stored in a separate location during user enrolment (or during key reset), without any binding information that could relate the authentication key to any particular user. Finally, it is important to underpin that the participation of the students was voluntary and all participants agreed to a consent form that their interactions with the course's Web-site would be recorded anonymously as part of an experimental user study of the researchers' group. No further details about the aim of the study and the interaction data recorded (e.g., time to complete the tasks) were provided to the students in order to avoid bias effects. Also, throughout the semester, users were able to opt out of the study any time they like.

9.5 Future Work

Based on the work presented in this thesis, and the future challenges and requirements in the area of usable security within user authentication and CAPTCHA mechanisms, we further outline the future research prospects of this work. The primary future research prospects are listed next:

- Increase the external validity of the research conducted so far with larger samples and varying user profiles (e.g., age). In particular, 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 on security-related 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 and CAPTCHA.

- Further investigate the impact of other intrinsic human factors (e.g., emotional parameters) as well as technology factors (e.g., device type) in interactive systems;
- Increase our understanding about the effects of human factors on user authentication and CAPTCHA mechanisms through the utilization of external devices such as eye-tracking and wearables, aiming to identify correlations between high-level intrinsic human factors and physiological parameters;
- The proposed adaptation rules and recommendations will be applied on different user authentication and CAPTCHA schemes and interaction device types (desktop computers vs. mobile touch-based) in order to cross-validate the findings of this research and to increase the applicability of the PAC framework in various contexts of use;
- Design and evaluate a conceptual personalization framework aiming to organize and present information and functionalities in an adaptive format to diverse user groups, by using different levels of abstractions through appropriate interaction styles, terminology, information presentation and user modeling techniques. The framework is envisioned to be based on an object-oriented point of view considering three main objects as core elements for understanding and analyzing such interactions: (a) human factors which can be grouped in physical, cognitive and contextual; (b) technology factors (e.g., interaction device type); and (c) design factors of the particular application domain.

Finally, we stress that an interesting implication of our work is related to the ecumenical character of user authentication and CAPTCHA tasks. Scholars have provided evidence that the differences in cognitive processing styles and abilities exist not only within a certain nation, but as well across diverse nations around the globe, as they are affected by the cultural background in which they are developed (Cui et al. 2013; Varnum et al. 2010; Engelbrecht et al. 1997). From this perspective, given the globalization of Information Technology applications and services, research works like the one reported herein could be replicated on a multinational scale aiming the design and development of globalized security schemes, whose impact will affect a large number of individuals from different cultures. In this context, bearing in mind that prior research has shown cross-cultural differences in field dependence-independence (Western vs. Eastern societies (Cui et al. 2013; Varnum et al. 2010), African American vs. South African (Engelbrecht et al. 1997)), future work entails investigating the effects of inter-cultural differences on user authentication and CAPTCHA across different countries and continents.

BIBLIOGRAPHY

Adams, A., & Sasse, A. (1999). Users are not the Enemy: Why users compromise security mechanisms and how to take remedial measures. *Communications of the ACM, 42*(12), 40-46

AdaptiveWeb (2007). An adaptiveweb system for integrating human factors in personalization of web content. Available online at http://adaptiveweb.cs.ucy.ac.cy (accessed August 2015)

Albert, D., Jeng, B., Tseng, C., & Wang, J. (2010). A study of CAPTCHA and its application to user authentication. In *Proceedings of the International Conference on Computational Collective Intelligence (ICCCI 2010)*, Springer-Verlag, 433-440

Ally, B.A., & Budson, A.E. (2007). The worth of pictures: Using high density event related potentials to understand the memorial power of pictures and the dynamics of recognition memory. *NeuroImage, 35*, 378-395

Alotaiby, F.T. & Chen, J.X. (2004). A model for team-based access control (TMAC 2004). In *Proceedings of the International Conference on Information Technology: Coding and Computing (ITCC 2004)*, 450-454

Altun, A., & Cakan, M. (2006). Undergraduate students' academic achievement, field dependent/independent cognitive styles and attitude toward computers. *Educational Technology & Society, 9*(1), 289-297

Amazon (2015). Amazon on-line shopping. Available online at http://www.amazon.com (accessed April 2015)

Anderson, C., Domingos, P., & Weld, D. (2001). Personalizing web sites for mobile users. In *Proceedings of the International Conference on World Wide Web (WWW 2001)*, ACM Press, 565-575

Anderson, J.R. (2009). Cognitive Psychology and its Implications: Seventh Edition. New York: Worth Publishers

Angeli, A.D., Coventry, L., Johnson, G., & Renaud, K. (2005). Is a picture really worth a thousand words? Exploring the feasibility of graphical authentication systems. *Human-Computer Studies, 63*(1-2), 128-152

Angeli, C., Valanides, N., & Kirschner, P. (2009). Field dependence-independence and instructional-design: Effects on learners' performance with a computer-modeling tool. *Computers in Human Behavior, 25*(6), 1355-1366

Antoniou, A., & Lepouras, G. (2010). Modeling visitors' profiles: A study to investigate adaptation aspects for museum learning technologies. *Computing Cultural Heritage. 3*(2), 1-19

Apple (2015). Apple iOS 8. Available online at http://www.apple.com/ios/ (accessed August 2015)

Ardissono L., Console L., & Torre I. (2001). An adaptive system for the personalised access to news. *AI Communications, 14*, 129-147

Ardissono, L., & Torasso, P. (2000). Dynamic user modeling in a web store shell. In *Proceedings of the European Conference on Artificial Intelligence*, 621-625

Atkins, H., Moore, D., Sharpe, S. & Hobbs, D. (2001) Learning style theory and computer mediated communication. In *Proceedings of the Conference on Educational Multimedia, Hypermedia & Telecommunications (ED-MEDIA 2001)*, 71-75

Atkinson, R.C., & Shiffrin, R.M. (1968). Human memory: A proposed system and its control processes. In *The Psychology of Learning and Motivation: Advances in Research and Theory*, Spence, K.W. & Spence, J.T (eds.), Vol. 2, Academic Press

Baddeley, A. (1986). *Working Memory*, Oxford Clarendon Press

Baddeley, A. (1990). *Human Memory: Theory and Practice*. London, Lawrence-Erlbaum Association

Baddeley, A. (1992). Working Memory. *Science 255*, 5044, 556-559

Baddeley, A. (2012). Working Memory: Theories, Models, and Controversies. *Annual Review of Psychology, 63*, 1-29

Baddeley, A.D. (2000). The episodic buffer: a new component of working memory? *Trends Cognitive Science 4*, 417-423

Baddeley, A.D., & Hitch, G. (1974). Working Memory, In *The Psychology of Learning and Motivation*, Bower, G.H. (ed.), Vol. 8, London Academic Press

Baecher, P., Buscher, N., Fischlin, M., & Milde, B. (2011). Breaking reCAPTCHA: A holistic approach via shape recognition. In *Future Challenges in Security and Privacy for Academia and Industry*, Camenisch, J., Fischer-Hbner, S., Murayama, Y., Portmann, A., & Rieder, C. (eds.), LNCS, 354, Springer-Verlag, 56-67

Baikadi, A., Rowe, J., Mott, B., & Lester, J. (2014). Generalizability of goal recognition models in narrative-centered learning environments. In *Proceedings of the International Conference on User Modeling, Adaptation, and Personalization (UMAP 2014)*, Springer-Verlag, 278-289

Banner, G. & Rayner, S. (2000). Learning language and learning style: principles, process and practice. *Language Learning Journal, 21*, 37-44

Barua, D., Kay, J., Kummerfeld, B., & Paris, C. (2014). Modelling long term goals. In *Proceedings of the International Conference on User Modeling, Adaptation, and Personalization (UMAP 2014)*, Springer-Verlag, 1-12

Basilico, J., & Hofmann, T. (2004). Unifying collaborative and content-based filtering. In *Proceedings of the International Conference on Machine Learning* (*ICML 2004)*, ACM Press, 9-

Belk, M., Germanakos, P., Fidas, C., Holzinger, A., & Samaras, G. (2013a). Towards the personalization of CAPTCHA mechanisms based on individual differences in cognitive processing. In *Proceedings of the International Conference on Human Factors in Computing & Informatics (SouthCHI 2013)*, Springer-Verlag, 409-426

Belk, M, Fidas, C., Germanakos, P., & Samaras, G. (2014a). A personalised user authentication approach based on individual differences in information processing. *Interacting with Computers*, doi: 10.1093/iwc/iwu033

Belk, M, Germanakos, P., Fidas, C., & Samaras, G. (2014b). A personalisation method based on human factors for improving usability of user authentication tasks. In *Proceedings of the International Conference on User Modeling, Adaptation, and Personalization (UMAP 2014)*, Spinger-Verlag, 13-24

Belk, M., Fidas, C., Germanakos, P., & Samaras, G. (2012a). Do cognitive styles of users affect preference and performance related to CAPTCHA challenges? In *Proceedings of the ACM SIGCHI Conference on Human Factors in Computing Systems (CHI 2012)*, ACM Press, 1487-1492

Belk, M., Fidas, C., Germanakos, P., & Samaras, G. (2013c). Security for diversity: Studying the effects of verbal and imagery processes on user authentication mechanisms. In *Proceedings of the IFIP TC13 Conference on Human-Computer Interaction (INTERACT 2013)*, Springer-Verlag, 442-459

Belk, M., Fidas, C., Germanakos, P., & Samaras, G. (2015a). Do human cognitive differences in information processing affect preference and performance of CAPTCHA? *International Journal of Human Computer Studies, 84*, 1-18

Belk, M., Fidas, C., Germanakos, P., & Samaras, G. (2015b). The interplay between humans, technology and user authentication: A cognitive processing perspective. *ACM Transactions on Computer-Human Interaction* (under review)

Belk, M., Germanakos P., Papatheocharous E., Constantinides M., & Samaras G. (2012b). Supporting adaptive interactive systems with semantic markups and human factors. In *Proceedings of the International Workshop on Semantic and Social Media Adaptation and Personalization (SMAP 2012)*, IEEE Computer Society, 126-130

Belk, M., Germanakos, P., Constantinides, A., & Samaras G. (2015c). A human cognitive processing perspective in designing e-commerce checkout processes. In *Proceedings of the IFIP TC13 Conference on Human-Computer Interaction (INTERACT 2015)*, Springer-Verlag, 523-530

Belk, M., Germanakos, P., Fidas, C., & Samaras, G. (2013d). Studying the effect of human cognition on user authentication tasks. In *Proceedings of the Conference on User Modeling, Adaptation, and Personalization (UMAP 2013)*, Springer-Verlag, 102-113

Belk, M., Papatheocharous, E., Germanakos, P., & Samaras, G. (2013b). Modeling users on the world wide web based on cognitive factors, navigation behavior and clustering techniques. *Systems and Software, 86* (12), 2995-3012

Bellotti, V., Begole, B., Chi, E., Ducheneaut, N., Fang, J., Isaacs, E., King, T., Newman, M., Partridge, K., Price, B., Rasmussen, P., Roberts, M., Schiano, D., & Walendowski, A. (2008). Activity-based serendipitous recommendations with the magitti mobile leisure guide. In *Proceedings of the ACM conference on Human factors in computing systems*, 1157-1166.

Biddle, R., Chiasson, S., & van Oorschot, P. (2012). Graphical passwords: Learning from the first twelve years. *ACM Computing Surveys, 44*(4), 41 pages

Bigham, J., & Cavender, A. (2009). Evaluating existing audio CAPTCHAs and an interface optimized for non-visual use. In *Proceedings of the ACM SIGCHI Conference on Human Factors in Computing Systems (CHI 2009)*, ACM Press, 1829-1838

Bing (2015). Bing search engine. Available online at http://www.bing.com (accessed April 2015)

Blazhenkova, O., & Kozhevnikov, M. (2009). The new object-spatial-verbal cognitive style model: Theory and measurement. *Applied Cognitive Psychology, 23* (5), 638-663

Blom, J. (2000). Personalization: a taxonomy. In *Proceedings of Extended Abstracts on Human Factors in Computing Systems (CHI 2000)*, ACM Press, 313-314

Bogonicolos, N., Fragoudis, D., & Likothanassis, S. (1999). ARCHIMIDES: An intelligent agent for adaptive personalized navigation within a web server. In *Proceedings of the Annual Hawaii International Conference on System Science*

Bonneau, J., Herley, C., van Oorschot, P., & Stajano, F. (2012). The quest to replace passwords: A framework for comparative evaluation of web authentication schemes. In *Proceedings of the Symposium on Security and Privacy (SP 2012)*, IEEE Computer Society, 553-567

Botsios, S., Georgiou, D., & Safouris, N. (2008). Contributions to adaptive educational hypermedia systems via online learning style estimation. *Educational Technology & Society, 11* (2), 322-339

Boyle, C., & Encarnacion, A. (1994). MetaDoc: an adaptive hypertext reading system. *User Modeling and User-Adapted Interaction, 4*(1), 1-19

Boyle, E. A., Duffy, T., & Dunleavy, K. (2003). Learning styles and academic outcome: The validity and utility of Vermunt's Inventory of Learning Styles in a British higher education setting. *British Journal of Educational Psychology, 73*, 267-290

Brady, T.F., Konkle, T., Alvarez, G.A., & Oliva, A. (2008). Visual long-term memory has a massive storage capacity for object details. *National Academy of Sciences, 105*(38), 14325-14329

Brown, E., Brailsford, T., Fisher, T., Moore, A., & Ashman, H. (2006). Reappraising cognitive styles in adaptive web applications. In *Proceedings of the ACM Conference on World Wide Web (WWW 2006)*, ACM Press, 327-335

Brusilovsky, P. (1996). Methods and techniques of adaptive hypermedia. *User Modeling and User Adapted Interaction, 6*(2-3), 87-129

Brusilovsky, P. (2001). Adaptive Hypermedia. *User Modeling and User-Adapted Interaction 11*(1, 2), 87-110

Brusilovsky, P. (2003). From adaptive hypermedia to the adaptive web, *Mensch & Computer 2003: Interaktion in Bewegung*, 21-24

Brusilovsky, P. (2007). Adaptive navigation support. In *The adaptive web*, Brusilovsky, P., Kobsa, A. & Nejdl, W. (eds.), LNCS, Vol. 4321, Springer-Verlag, 263-290

Brusilovsky, P., & Cooper, D. (2002). Domain, task, and user models for an adaptive hypermedia performance support system. In *Proceedings of Intelligent User Interfaces (IUI 2002)*, ACM Press, 23-30

Brusilovsky, P., & Maybury, M.T. (2002). From adaptive hypermedia to the adaptive web. *Communications of the ACM 45*(5), 30-33

Brusilovsky, P., & Millán, E., (2007). User models for adaptive hypermedia and adaptive educational systems. In *The adaptive web*, Brusilovsky, P., Kobsa, A. & Nejdl, W. (eds.), LNCS, Vol. 4321, Springer-Verlag, 3-53

Brusilovsky, P., Eklund, J. & Schwarz, E. (1998). Web-based education for all: A tool for developing adaptive courseware. Computer Networks and ISDN Systems. In *Proceedings of the International Conference on the World Wide Web (WWW 1998)*, ACM Press, 291-300

Brusilovsky, P., Farzan, R., & Ahn, J. (2006). Layered evaluation of adaptive search. In *Proceedings of Workshop on Evaluating Exploratory Search Systems (At SIGIR 2006)*

Brusilovsky, P., Karagiannidis, C., & Sampson, D. (2001). The benefits of layered evaluation of adaptive applications and services. In *Proceedings of Workshop of Empirical Evaluation of Adaptive Systems (UM 2001)*, Springer-Verlag, 1-8

Brusilovsky, P., Kobsa, A., & Vassileva, J. (1998). *Adaptive hypertext and hypermedia*. Springer-Verlag

Brusilovsky, P., Schwarz, E., & Weber, G. (1996). A tool for developing hypermedia-based ITS on WWW. In *Proceedings of the Workshop Architectures and Methods for Designing Cost-Effective and Reusable ITSs (at ITS 1996)*

Bull, S., & McCalla, G. (2000). Modelling cognitive style in a peer help network. *Instructional Science, 30*(6), 497-528

Bulling, A., Alt, F., & Schmidt, A. (2012). Increasing the security of gaze-based cued-recall graphical passwords using saliency masks. In *Proceedings of the ACM International Conference on Human Factors in Computing Systems (CHI 2012)*, ACM Press, 3011-3020

Burr, W.E, Dodson, D.F., & Polk, W.T. (2006). *Electronic authentication guideline*. Technical report, National Institute of Standards and Technology

Bursztein, E., Bethard, S., Fabry, C., Mitchell, J., & Jurafsky, D. (2010). How good are humans at solving CAPTCHAs? A large scale evaluation. In *Proceedings of the Symposium on Security and Privacy (SP 2010)*, IEEE Computer Society, 399-413

Bursztein, E., Martin, M., & Mitchell, J. (2011). Text-based CAPTCHA strengths and weaknesses. In *Proceedings of the Conference on Computer and Communications Security (CCS 2011)*, ACM Press, 125-138

Bursztein, E., Moscicki, A., Fabry, C., Bethard, S., Mitchell, J., & Jurafsky, D. (2014). Easy does it: More usable CAPTCHAs. In *Proceedings of the ACM SIGCHI Conference on Human Factors in Computing Systems (CHI 2014)*, ACM Press, 2637-2646

Cadez, I., Heckerman, D., Meek, C., Smyth, P., & White, S. (2000). Visualization of navigation patterns on a web site using model-based clustering. In *Proceedings of the ACM SIGKDD International Conference on Knowledge Discovery and Data Mining (KDD 2000)*, ACM Press, 280-284

Carro, R.M., Pulido, E., & Rodríguez, P. (1999). TANGOW: Task-based adaptive learner guidance on the WWW. *Computer Science Report*, Eindhoven University of Technology, 49-57

Cassady, J.C. (2004). The influence of cognitive test anxiety across the learning–testing cycle, *Learning and Instruction, 14*, 569-592

Cassidy, S. (2004). Learning atyles: An overview of theories, models, and measures. *Educational Psychology, 24*(4), 419-444

Castellano, G., & Torsello, M.A. (2008). Categorization of web users by fuzzy clustering. In *Proceedings of International Conference on Knowledge-Based Intelligent Information and Engineering Systems*, Springer-Verlag, 222-229

Castellano, G., Fanelli, A.M., Mencar, C., & Torsello, M.A., (2007). Similarity-based fuzzy clustering for user profiling. In *Proceedings of International Conference on Web Intelligence and Intelligent Agent Technology Workshop (WI 2007)*, IEEE Computer Society, 75-78

Chakrabarti, S., Ester, M., Fayyad, U., Gehrke, J., Han, J., Morishita, S., Piatetsky-Shapiro, G., & Wang, W. (2006). Data mining curriculum: A proposal (Version 1.0). *ACM Knowledge Discovery and Data Mining (SIGKDD)*

Chan, C., Hsieh, C., & Chen, S. (2014). Cognitive styles and the use of electronic journals in a mobile context. *Documentation, 70*(6), 997-1014

Chan, T. (2003). Using a text-to-speech synthesizer to generate a reverse turing test. In *IEEE Conference on Tools with Artificial Intelligence*, IEEE Computer Society, 226-232

Chang, T., El-Bishouty, M., Graf, S., & Kinshuk (2013). An approach for detecting students' working memory capacity from their behavior in learning systems. In *Proceedings of the International Conference on Advanced Learning Technologies (ICALT 2013)*, IEEE Computer Society, 82-86

Chellapilla, K., Larson, K., Simard, P., & Czerwinski, M. (2005). Designing human friendly human interaction proofs (HIPs). In *Proceedings of the ACM SIGCHI Conference on Human Factors in Computing Systems (CHI 2005)*, ACM Press, 711-720

Chen, S., & Liu, X. (2008). An integrated approach for modeling learning patterns of students in web-based instruction: A cognitive style perspective. *ACM Transactions on Computer-Human Interaction, 15*(1), Article 1, 28 pages

Cheng, L., Liang, H., Wu, C., & Chen, M. (2013). iGrasp: Grasp-based adaptive keyboard for mobile devices. In *Proceedings of the ACM SIGCHI Conference on Human Factors in Computing Systems (CHI 2013)*, ACM Press, 3037-3046

Cheverst, K., Davies, N., Mitchell, K., & Smith, P. (2000). Providing tailored (context-aware) information to city visitors. In *Proceedings of Adaptive Hypermedia and Adaptive Web-based Systems (AH 2000)*, Springer-Verlag, 73-85

Chew, M., & Baird, H. (2003). BaffleText: A human interactive proof. In *Proceedings of the International Conference on Document Recognition and Retrieval (DRR 2003)*, 305-316

Chew, M., & Tygar, J. (2004). Image recognition CAPTCHAs. In *Proceedings of the International Information Security Conference (ISC 2004)*, Springer-Verlag, 268-279

Chiang, H., & Chiasson, S. (2013). Improving user authentication on mobile devices: A touchscreen graphical password. In *Proceedings of the International Conference on Human-Computer Interaction with Mobile Devices and Services (MobileHCI 2013)*, ACM Press, 251-260

Chiasson, S., Forget, A., Biddle, R., & van Oorschot, P. (2008). Influencing users towards better passwords: Persuasive cued click-points. In *Proceedings of the BCS Conference on People and Computers*, British Computer Society, 121-130

Chiasson, S., Forget, A., Stobert, E., van Oorschot, P., & Biddle, R. (2009). Multiple password interference in text passwords and click-based graphical passwords. In *Proceedings of the ACM Conference on Computer and Communications Security (CCS 2009)*, ACM Press, 500-511

Chiasson, S., van Oorschot, P., & Biddle, R. (2006). Usability study and critique of two password managers. In *Proceedings of the USENIX Security Symposium*, USENIX Association, 1-16

Chittaro, L., Carchietti, E., De Marco, L., & Zampa, A. (2011). Personalized emergency medical assistance for disabled people. *User Modeling and User-Adapted Interaction 21*(4-5), 407-440

Choa, Y.H., Kim J.K., & Kim, S.H. (2002). A personalized recommender system based on web usage mining and decision tree induction. *Expert Systems with Applications, 23*(3), 329-342

Chow, R., Golle, P., Jakobsson, M., Wang, L., & Wang, X. (2008). Making CAPTCHAs clickable. In *Proceedings of the Workshop on Mobile Computing Systems and Applications (HotMobile 2008)*, ACM Press, 91-94

Chowdhury, S., Poet, R., & Mackenzie, L. (2013). A comprehensive study of the usability of multiple graphical passwords. In *Proceedings of the IFIP TC13 Conference on Human-Computer Interaction (INTERACT 2013)*, Springer-Verlag, 424-441

Cingil, I., Dogac, A., & Azgin, A. (2000). A broader approach to personalization. *Communications of the ACM, 43*(8), 136-141

Coffield, F., Moseley, D., Hall, E., & Ecclestone, K. (2004). *Learning styles and pedagogy in post-16 learning. A systematic and critical review*. Learning and Skills Research Centre: London, UK

Conlan, O., O'Keeffe, I., & Tallon, S. (2006). Combining adaptive hypermedia techniques and ontology reasoning to produce dynamic personalized news services. In *Proceedings of Adaptive Hypermedia and Adaptive Web-Based Systems (AH 2006)*, 81-90

Conway, A.R.A., Cowan, N., & Bunting, M.F. (2001). The cocktail party phenomenon revisited: The importance of working memory capacity. *Psychonomic Bulletin and Review, 8*, 331-335

Conway, A.R.A., Cowan, N., Bunting, M.F., Therriault, D.J., & Minkoff, S.R. (2002). A latent variable analysis of working memory capacity, short-term memory capacity, processing speed, and general fluid intelligence. *Intelligence, 30*, 163-183

Corbetta, M., & Shulman, G.L. (2002). Control of goal-directed and stimulus-driven attention in the brain. *Nature Reviews Neuroscience, 3*, 201-215

Craik, F.I.M., & Lockhart, R.S. (1972). Levels of processing: A framework for memory research. *Journal of Verbal Learning and Verbal behavior, 11*, 671-684

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

Cui, G., Liu, H., Yang, X. & Wang, H. (2013). Culture, cognitive style and consumer response to informational vs. transformational advertising among East Asians: Evidence from the PRC. *Asia Pacific Business Review, 19*(1), 16-31

Curry, L. (1983). An organization of learning styles theory and constructs. In *Learning style in continuing education*, Curry, L. (ed.) Dalhousie University, 115-131

Curry, L. (1990). One critique of the research on learning styles. *Educational Leadership, 48*, 50-56

Datta, R., Li, J., & Wang, J.Z. (2005). IMAGINATION: A robust image-based CAPTCHA generation system. In *Proceedings of the ACM Conference on Multimedia*, ACM Press, 331-334

Davis, D., Monrose, F., & Reiter, M. (2004). On user choice in graphical password schemes. In *Proceedings of the USENIX Security Symposium*, USENIX Association

Davou, B. (2000). *Thought processes in the age of information: Issues on cognitive psychology and communication*, Papazissis Publishers, Athens

De Bra, P. & Calvi, L. (1998). AHA! An open adaptive hypermedia architecture. *The new review of hypermedia and multimedia, 4*, Taylor Graham Publishers, 115-139

De Bra, P., Aroyo, L., & Chepegin, V. (2004). The next big thing: Adaptive web-based systems. *Journal of Digital Information, 5*(1), 247

De Luca, A., Hang, A., Brudy, F., Lindner, C., & Hussmann, H. (2012). Touch me once and I know it's you!: Implicit authentication based on touch screen patterns. In *Proceedings of the ACM SIGCHI Conference on Human Factors in Computing Systems (CHI 2012)*, ACM Press, 987-996

De Luca, A., Harbach, M., von Zezschwitz, E., Maurer, M., Slawik, B.E., Hussmann, H., & Smith, M. (2014). Now you see me, now you don't: protecting smartphone authentication from shoulder surfers. In *Proceedings of the ACM Conference on Human Factors in Computing Systems (CHI 2014)*, ACM Press, 2937-2946

De Luca, A., von Zezschwitz, E., Pichler, L., & Hussmann, H. (2013). Using fake cursors to secure on-screen password entry. In *Proceedings of the ACM Conference on Human Factors in Computing Systems (CHI 2013)*, ACM Press, 2399-2402

Deary, I.J. (2001). Human intelligence differences: a recent history. *Trends in Cognitive Sciences, 5*(3), 127-130

Delicato, F., Pirmez, L., & Carmo, L. (2001). Fenix – personalized information filtering system for WWW pages. *Internet Research: Electronic Networking Applications and Policy, 11*(1), 42-48

Demetriou, A., Christou, C., Spanoudis, G., & Platsidou, M. (2002). The development of mental processing: Efficiency, working memory and thinking. *Monographs of the Society for Research in Child Development, 67*(1), 1-155

Demetriou, A., Spanoudis, G., & Shayer, M. (2013). Developmental intelligence: From empirical to hidden constructs. *Intelligence, 41*, 744-749

Department of Homeland Security: A Roadmap for Cybersecurity Research (2009). Available online http://www.cyber.st.dhs.gov/docs/DHS-Cybersecurity-Roadmap.pdf

Deshpande, M., & Karypis, G. (2004). Selective Markov models for predicting web page accesses. *ACM Transactions on Internet Technologies, 4*(2), 163-184

Dhamija, R., & Perrig, A. (2000). DejaVu: A user study using images for authentication. In *Proceedings of the USENIX Security Symposium*, USENIX Association.

Díaz, A., & Gervás, P. (2005). Personalisation in news delivery systems: Item summarization and multitier item selection using relevance feedback. *Web Intelligence and Agent Systems, 3*(3), 135-154

Dieterich, H., Malinowski, U., Kühme, T., & Schneider-Hufschmidt, M. (1993). State of the art in adaptive user interfaces. In *Adaptive user Interfaces: Principles and Practice*, Schneider-Hufschmidt, M., Kühme, T., & Malinowski, U. (eds.), North-Holland: Amsterdam

Dillon, A., & Watson, C. (1996). User analysis in HCI-the historical lessons from individual differences research. *International Journal of Human-Computer Studies, 45*(6), 619-637

Driscoll, M. (2001). *Psychology of learning for assessment: Second Edition*. Allyn and Bacon: Boston

Dumais, S., Cutrell, E., Cadiz, J., Jancke, G., Sarin, R., & Robbins, D. (2003). Stuff I've seen: a system for personal information retrieval and re-use. In *Proceedings of ACM SIGIR Conference on Research and Development in Information Retrieval (SIGIR 2003)*, ACM Press, 72-79

Dunn, R., Dunn K., & Price, G.E. (1985). *Learning styles inventory (lsi): An inventory for the identification of how individuals in grades 3 through 12 prefer to learn*. Lawrence, KS: Price Systems

Dunphy, P., & Yan, J. (2007). Do background images improve "draw a secret" graphical passwords? In *Proceedings of the ACM International Conference on Computer and Communications Security (CCS 2007)*, ACM Press, 36-47

Eggen, P., & Kauchak, D. (2007). *Educational psychology, windows on classrooms: Seventh Edition*. Upper Saddle River, NJ: Pearson Merrill Prentice Hall Publishing

Eirinaki, M., & Vazirgiannis, M. (2003). Web mining for web personalization. *ACM Transactions on Internet Technology, 3*(1), 1-27

EKPAIDEION (2008). Adapting E-Learning Environments based on Human Factors. Available online at http://www3.cs.ucy.ac.cy/ekpaideion (accessed August 2015)

Eliasmith, C. (2001). *Memory. Dictionary of philosophy of mind*. Pullman, WA: Washington State University

Elson, J., Douceur, J., Howell, J., & Saul, J. (2007). Asirra: A CAPTCHA that exploits interest-aligned manual image categorization. In *Proceedings of the International Conference on Computer and Communications Security (CCS 2007)*, ACM Press, 366-374

Encarnação, L. (1997). Multi-level user support through adaptive hypermedia: A highly application independent help component. In *Proceedings of Intelligent User Interfaces (IUI 1997)*, ACM Press, 187-194

Engelbrecht, P., Engelbrecht, P., Natzel, S., & Natzel, S. (1997). Cultural variations in cognitive style: Field dependence vs field independence. *School Psychology International, 18*(2), 155-164

Engle, R.W. (2002). Working memory capacity as executive attention. *Current Directions in Psychological Science, 11*, 19-23

Everitt, K., Bragin, T., Fogarty, J., & Kohno, T. (2009). A comprehensive study of frequency, interference, and training of multiple graphical passwords. In *ACM International Conference on Human Factors in Computing Systems (CHI 2009)*, ACM Press, 889-898

Eysenck, M. (1988). *A handbook of cognitive psychology*. Lawrence Erlbaum Association: London, UK

Eysenck, W.M., & Keane, R.M. (2005). *Cognitive psychology – A student's handbook: Fifth Edition*, Psychology Press: Taylor & Francis Group, NY

Felder, R.M., & Silverman, L.K. (1988). Learning and teaching styles in engineering education. *Engineering Education 78*, 674-681

Ferwerda, B., Yang, E., Schedl, M., & Tkalcic, M. (2015). Personality traits predict music taxonomy preferences. In *Extended Abstracts on Human Factors in Computing Systems (CHI EA 2015)*, ACM Press, 2241-2246

Fidas, C., Hussmann, H., Belk, M., & Samaras, G. (2015). iHIP: Towards a user centric individual human interaction proof framework. In *Proceedings of the ACM Conference Extended Abstracts on Human Factors in Computing Systems (CHI EA 2015)*, ACM Press, 2235-2240

Fidas, C., Voyiatzis, A., & Avouris, N. (2011). On the necessity of user-friendly CAPTCHA. In *Proceedings of the ACM SIGCHI Conference on Human Factors in Computing Systems (CHI 2011)*, ACM Press, 2623-2626

Fidas, C.A., Voyiatzis, A.G., & Avouris, N.M. (2010). When security meets usability: A user-centric approach on a crossroads priority problem. In *Proceedings of the Panhellenic Conference on Informatics (PCI 2010)*, IEEE Computer Society, 112-117

Findlater, L., Wobbrock, J., & Wigdor, D. (2011). Typing on flat glass: Examining ten-finger expert typing patterns on touch surfaces. In *Proceedings of the ACM SIGCHI Conference on Human Factors in Computing Systems (CHI 2011)*, ACM Press, 2453-2462

Flanagan, O. (1991). *The Science of the Mind: Second Edition*. MIT Press

Florencio, D., & Herley, C.A. (2007). Large-scale study of web password habits. In *Proceedings of the ACM Conference on World Wide Web (WWW 2007)*, ACM Press, 657-666

Forget, A., & Biddle, R. (2008). Memorability of persuasive passwords. In *Extended Abstracts of the ACM SIGCHI Conference on Human Factors in Computing Systems (CHI 2008)*, ACM Press, 3759-3764

Forget, A., Chiasson, S., & Biddle, R. (2014). Towards supporting a diverse ecosystem of authentication schemes. In *Proceedings of the Who are you?! Adventures in Authentication Workshop (WAY 2014) at the Symposium on Usable Privacy and Security (SOUPS 2014)*, USENIX Association

Forget, A., Chiasson, S., van Oorschot, P., & Biddle, R. (2008). Improving text passwords through persuasion. In *Proceedings of the ACM Symposium on Usable Security and Privacy (SOUPS 2008)*, ACM Press, 1-12

Frias-Martinez, E., Chen, S.Y., Macredie R.D., & Liu, X. (2007). The role of human factors in stereotyping behavior and perception of digital library users: A robust clustering approach. *User Modeling and User-Adapted Interaction, 17*(3), 305-337

Frias-Martinez, E., Magoulas, G., Chen, S., & Macredie, R. (2005). Modeling human behavior in user-adaptive systems: Recent advances using soft computing technique. *Expert Systems with Applications, 29*(2), 320-329

Fu, Y., Sandhu, K., & Shih, M.Y. (1999). Clustering of web users based on access patterns. In *ACM SIGKDD International Conference on Knowledge Discovery and Data Mining*, Springer-Verlag

Gao, H., Guo, X., Chen, X., Wang, L., & Liu, X. (2008). YAGP: Yet another graphical password strategy. In *Proceedings of the IEEE Conference on Computer Security Applications*, IEEE Computer Society, 121-129

Gao, H., Liu, H., Yao, D., Liu, X., & Aickelin, U. (2010). An audio CAPTCHA to distinguish humans from computers. In *Proceedings of the International Symposium on Electronic Commerce and Security (SECS 2010)*, IEEE Computer Society, 265-269

Garlatti, S., & Iksal, S. (2000). Context filtering and spacial filtering in an adaptive information system. In *Proceedings of Adaptive Hypermedia and Adaptive Web-based systems (AH 2000)*, Springer-Verlag, 315-318

Gauch, S., Speretta, M., Chandramouli, A., & Micarelli, A. (2007). User profiles for personalized information access. In *The adaptive web*, Brusilovsky, P, Kobsa, A, & Nejdl, W, (eds.), LNCS, Vol. 4321, Springer-Verlag, 54-89

Georgiadis, C., Mavridis, I., Pangalos, G., & Thomas, R. (2001). Flexible team-based access control using contexts. In *Proceedings of the ACM symposium on Access control models and technologies*, ACM Press, 21-27

Germanakos, P., Belk, M., Constantinides, A., & Samaras, G. (2015). The personaweb System: Personalizing e-commerce environments based on human factors. In *Extended Proceedings of the International Conference on User Modeling, Adaptation, and Personalization (UMAP 2015)*, CEUR Workshop Proceedings 1388

Germanakos, P., Tsianos, N., Lekkas, Z., Belk, M., Mourlas, C., & Samaras, G. (2009). Proposing web design enhancements based on specific cognitive factors: An empirical evaluation. In *International Conference on Web Intelligence (WI 2009)*, IEEE Computer Society, 602-605

Germanakos, P., Tsianos, N., Lekkas, Z., Mourlas, C., Belk, M., & Samaras, G. (2007). An adaptiveweb system for integrating human factors in personalization of web content. In *Proceedings of the International Conference on User Modeling (UM 2007)*, Springer-Verlag, 25-29

Germanakos, P., Tsianos, N., Lekkas, Z., Mourlas, C., Samaras, G. (2008). Capturing essential intrinsic user behaviour values for the design of comprehensive web-based personalized environments. *Computers in Human Behavior, 24*(4), 1434-1451

Ghinea, G., & Chen, S.Y. (2008). Measuring quality of perception in distributed multimedia: Verbalizers vs. imagers. *Computers in Human Behavior, 24*(4), 1317-1329

Gibson, J. (1966). *The senses considered as perceptual systems*. Boston: Houghton Mifflin.

Gibson, J. (1979). *The ecological approach to visual perception*. Boston: Houghton Mifflin.

Glaser, R., & Pellegrino, J.W. (1978). Uniting cognitive process theory and differential psychology: Back home from the wars. *Intelligence, 2*(3), 305-319

Glass, A., & Riding, R.J. (1999). EEG differences and cognitive style. *Biological Psychology, 51*, 23-41

Golle, P. (2008). Machine learning attacks against the asirra CAPTCHA. In *Proceedings of the ACM Conference on Computer and Communications Security (CCS 2008)*, ACM Press, 535-542

Google (2015a). Google search engine. Available online at http://www.google.com (accessed April 2015)

Google (2015b). Gmail. Available online at http://www.gmail.com (accessed May 2015)

Gossweiler, R., Kamvar, M., & Baluja, S. (2009). What's up CAPTCHA?: A CAPTCHA based on image orientation. In *Proceedings of the International Conference on World Wide Web (WWW 2009)*, ACM press, 841-850

Goy, A., Ardissono, L., & Petrone, G. (2007). Personalization in e-commerce applications. In *The adaptive web*, Brusilovsky, P., Kobsa, A., & Nejdl, W. (eds.), LNCS, Vol. 4321, Springer-Verlag, 485-520

Graber, D.A. (2000). *Processing politics*. The University of Chicago Press

Graf, S., & Kinshuk (2009). Advanced adaptivity in learning management systems by considering learning styles. In *Proceedings of International Workshop on Social and Personal Computing for Web-Supported Learning Communities*, 235-238

Graf, S., Liu, T., Kinshuk, Chen, N., & Yang, S. (2009). Learning styles and cognitive traits - Their relationship and its benefits in web-based educational systems. *Computers in Human Behavior, 25*(6), 1280-1289

Gregory, R. (1970). *The intelligent eye*. London: Weidenfeld and Nicolson.

Gulliver, S.R., & Ghinea, G. (2004). Stars in their eyes: What eye-tracking reveals about multimedia perceptual quality. *IEEE Transactions on Systems, Man and Cybernetics, 34*(4), 472-482

Halderman, J.A., Waters, B., & Felten, E. (2005). Convenient method for securely managing passwords. In *Proceedings of the ACM International Conference on World Wide Web (WWW 2005)*, ACM Press, 471-479

Hale, S., & Fry, A.F. (2000). Relationships among processing speed, working memory, and fluid intelligence in children. *Biological Psychology, 54*, 1-34

Hauger, D., & Köck, M. (2007). State of the art of adaptivity in e-learning platforms. In *Proceedings of the Workshop on Adaptivity and User Modeling in Interactive Systems*, 355-360

Hayashi, E., Das, S., Amini, S., Hong, J., & Oakley, I. (2013). CASA: context-aware scalable authentication. In *Proceedings of the ACM Symposium on Usable Privacy and Security (SOUPS 2013)*, ACM Press, Article 3, 10 pages

Hayashi, E., Pendleton, B., Ozenc, F., & Hong, J. (2012). WebTicket: account management using printable tokens. In *Proceedings of the ACM SIGCHI Conference on Human Factors in Computing Systems (CHI 2012)*, ACM Press, 997-1006

Heitz, R.P., & Engle, R.W. (2007). Focusing the spotlight: Individual differences in visual attention control. *Experimental Psychology, 136*, 217-240

Henry, J. (2007). *Professor pans 'learning style' teaching method*. The Telegraph

Herder, E., & van Dijk, B. (2002). Personalized adaptation to device characteristics. In *Proceedings of the International Conference on Adaptive Hypermedia and Adaptive Web-Based Systems (AH 2002)*, Springer-Verlag, 598-602

Herder, E., Siehndel, P., & Kawase, R. (2014). Predicting user locations and trajectories. In *Proceedings of the International Conference on User Modeling, Adaptation, and Personalization (UMAP 2014)*, Springer-Verlag, 86-97

Herley, C., & van Oorschot, P. (2012). A research agenda acknowledging the persistence of passwords. *Security and Privacy, 10*(1), 28-36

Herley, C., van Oorschot, P., & Patrick, A. (2009). Passwords: If we're so smart, why are we still using them? In *Financial Cryptography and Data Security*, Dingledine, R., & Golle, P. (eds.), LNCS, Vol. 5628, Springer-Verlag

HighCharts (2015). Interactive JavaScript Charts for Web-pages. Available online at http://www.highcharts.com (accessed July 2015)

Hock, R.R. (1999). *Forty studies that changed psychology, explorations into the history of psychological research: Third Edition*, Prentice-Hall

Hohl, H., Böcker, H., & Gunzenhäuser, R. (1996). Hypadapter: An adaptive hypertext system for exploratory learning and programming. *User Modeling and User Adapted Interaction, 6*, 131-156

Hollink, V., Someren, M., & Hage, S. (2005). Discovering stages in web navigation. In *Proceedings of The International Conference on User Modeling (UM 2005)*, Springer-Verlag, 473-482

Holman, J., Lazar, J., Feng, J.H., & D'Arcy, J. (2007). Developing usable CAPTCHAs for blind users. In *Proceedings of the ACM SIGACCESS Conference on Computers and Accessibility (ASSETS 2007)*, ACM Press, 245-246

Honey, P. & Mumford, A. (2006). *The learning styles questionnaire, 80-item version*. Maiden-head, UK, Peter Honey Publications

Hong, J., Hwang, M., Tam, K., Lai, Y., & Liu, L. (2012). Effects of cognitive style on digital jigsaw puzzle performance: A GridWare analysis. *Computers in Human Behavior, 28*(3), 920-928

Hori, M., Ono, K., Abe, M., & Koyanagi, T. (2004). Generating transformational annotation for web document adaptation: Tool support and empirical evaluation. *Journal Web Semantics: Science, Services and Agents on the World Wide Web, 2*(1), 1-18

Hsu, Y., & Chen, S. (2011). Associating learners' cognitive style with their navigation behaviors: A data-mining approach. In *Proceedings of the International Conference on Human-Computer Interaction: Users and Applications (HCII 2011)*, Springer-Verlag, 27-34

Huitt, W. (2000). *The information processing approach*. Educational Psychology Interactive. Valdosta, GA: Valdosta State University

Hussein, T., Linder, T., Gaulke, W., & Ziegler, J. (2014). Hybreed: A software framework for developing context-aware hybrid recommender systems. *User Modeling and User-Adapted Interaction, 24*(1-2), 121-174

Hutchison, K.A. (2007). Attentional control and the relatedness proportion effect in semantic priming. *Experimental Psychology: Learning, Memory, and Cognition, 33*, 645-662

Inglesant, P., & Sasse A. (2010). The true cost of unusable password policies: Password use in the wild. In *Proceedings of the ACM SIGCHI Conference on Human Factors in Computing Systems (CHI 2010)*, ACM Press, 383-392

James, W. (1890). *Principles of psychology*. NY: Holt

Jawaheer, G., Szomszor M., & Kostkova, P. (2010). Comparison of implicit and explicit feedback from an online music recommendation service. In *Proceedings of International Workshop on Information Heterogeneity and Fusion in Recommender Systems*, ACM press, 47-51

Jermyn, I., Mayer, A., Monrose, F., Reiter, M., & Rubin, A. (1999). The design and analysis of graphical passwords. In *Proceedings of the USENIX Security Symposium (Security 1999)*, USENIX Association, 1-1

Jin, X., Zhou, Y., & Mobasher, B. (2005). Task-oriented web user modeling for recommendation. In *Proceedings of the International Conference on User Modeling (UM 2005)*, Springer-Verlag, 109-118

John, D. & Boucouvalas, A.C. (2002). Multimedia tasks and user cognitive styles. In *Proceedings of the International Symposium on Communication Systems Networks & Digital Signal Processing (CSNDSP 2002)*

JQuery (2015). The write less, do more, javascript library. Available online at https://jquery.com (accessed July 2015)

Kane, M.J., Conway, A.R.A., Hambrick, D.Z., & Engle, R.W. (2007). Variation in working memory capacity as variation in executive attention and control. In *variation in working memory*, Conway, A.R.A., Jarrold, C., Kane, M. J., Miyake, A., & Towse, J.N. (eds.), 21-48

Kao-Li, C., Yang, T., & Lee, W. (2011). Personalized multimedia recommendation with social tags and context awareness. In *Proceedings of the World Congress on Engineering (WCE 2011)*, 1046-1051

Kaplan, C., Fenwick, J., & Chen, J. (1993). Adaptive hypertext navigation based on user goals and context. *User Modeling and User-Adapted Interaction, 3*(3), 193-220

Karat, C., Blom, J. O., & Karat, J. (2004). Designing personalized user experiences in ecommerce. LNCS, Springer-Verlag

Kelly, D., & Teevan, J. (2003). Implicit feedback for inferring user preference: a bibliography. *ACM SIGIR Forum, 37*(2), 18-28

Kinley, K., Tjondronegoro, D., & Partridge, H. (2010). Web searching interaction model based on user cognitive styles. In *Proceedings of the International Conference of the Computer-Human Interaction Special Interest Group of Australia on Computer-Human Interaction (OZCHI 2010)*, ACM Press, 340-343

Kleanthous-Loizou, S., & Dimitrova, V. (2013). Adaptive notifications to support knowledge sharing in close-knit virtual communities. *User Modeling and User-Adapted Interaction, 23*(2-3), 287-343

Klingberg, T. (2009). *The overflowing brain: Information overload and the limits of working memory*. Oxford University Press, New York

Kluever, K., & Zanibbi, R. (2009). Balancing usability and security in a video CAPTCHA. In *Proceedings of the ACM Symposium on Usable Privacy and Security (SOUPS 2009)*, ACM Press, Article 14, 11 pages

Kobsa, A., Nithyanand, R., Tsudik, G., & Uzun, E. (2013). Can jannie verify? Usability of display-equipped RFID tags for security purposes. *Computer Security, 21*(3), 347-370

Koffka, K. (1935). *Principles of gestalt psychology*. New York: Harcourt, Brace & Co

Kohler, W. (1947). *Gestalt psychology*. New York: Liversight

Kolb, A.Y., & Kolb, D.A. (2005). *The kolb learning style inventory – version 3.1*. Technical Specifications, Experience Based Learning Systems, Inc.

Komanduri, S., Shay, R., Kelley, P., Mazurek, M., Bauer, L., Christin, N., Cranor, L., & Egelman, S. (2011). Of passwords and people: Measuring the effect of password-composition policies. In *Proceedings of the ACM SIGCHI Conference on Human Factors in Computing Systems (CHI 2011)*, ACM Press, 2595-2604

Konstan, J., & Riedl, J. (2012). Recommender systems: From algorithms to user experience. *User Modeling and User-Adapted Interaction, 22*(1-2), 101-123

Korfhage, R.R. (1997). *Information storage and retrieval*. Wiley Computer Publishing, New York

Koved, L., & Stobert, E. (2014). *Who are you?! Adventures in authentication (WAY)*. Workshop at the Symposium on Usable Privacy and Security (SOUPS 2014), USENIX Association

Kozhevnikov, M. (2007). Cognitive styles in the context of modern psychology: Toward an integrated framework of cognitive style. *Psychological Bulletin, 133*(3), 464-481

Krulwich, B. (1997) Lifestyle finder: Intelligent user profiling using large-scale demographic data. *Artificial Intelligence Magazine, 18*(2), 37-45

Kuo, C., Romanosky, S., & Cranor, L. (2006). Human selection of mnemonic phrase-based passwords. In *Proceedings of the ACM International Symposium on Usable Privacy and Security (SOUPS 2006)*, ACM Press, 67-78

Lankhorst, M.M., Kranenburg, Salden A., & Peddemors, A.J.H. (2002). Enabling technology for personalizing mobile services. In *Proceedings of the Annual Hawaii International Conference on System Sciences (HICSS 2002)*, 1464-1471

Leite, W.L., Svinicki, M., & Shi, Y. (2009). Attempted validation of the scores of the vark: Learning styles inventory with multitrait–multimethod confirmatory factor analysis models. *Educational and Psychological Measurement*

Leonhard, M.D., & Venkatakrishnan, V.N. (2007). A comparative study of three random password generators. In *Proceedings of the IEEE International Conference on Electro/Information Technology (EIT 2007)*, IEEE Computer Society, 227-232

Li, A., Sbattella, L., & Tedesco, R. (2013). Polispell: An adaptive spellchecker and predictor for people with dyslexia. In *Proceedings of the International Conference on User Modeling, Adaptation and Personalization (UMAP 2013)*, Springer-Verlag, 302-309

Linden, G., Smith, B., & York, J., (2003). Amazon.com recommendations: Item-to-item collaborative filtering. *IEEE Internet Computing, 7*(1), 76-80

Loftus, E., & Loftus, G. (1980). On the permanence of stored information in the human brain. *American Psychologist, 35*(5), 409-420

Lutz, S., & Huitt., W. (2003). Information processing and memory: Theory and applications. *Educational Psychology Interactive*

Ma, Y., Feng, J., Kumin, L., & Lazar, J. (2013). Investigating user behavior for authentication methods: A comparison between individuals with Down syndrome and neurotypical users. *ACM Transactions on Accessible Computing, 4*(4), Article 15, 27 pages

Mabroukeh, N., & Ezeife, C. (2010). A taxonomy of sequential pattern mining algorithms. *ACM Computing Surveys, 43*(1), Article 3, 41 pages

MacLeod, C.M. (1991). Half a century of research on the stroop effect: An integrative review. *Psychological Bulletin, 109*, 163-203

Maglio, P. & Barret, R. (2000). Intermediaries personalize information streams. *Communications of the ACM, 43*(8), 96-101

Markham, S. (2004). *Learning styles measurement: a cause for concern*. Technical Report, Computing Educational Research Group

Marr, D. (1982). Vision – A computational investigation into the human representation and processing of visual information. W.H. Freeman and Company, NY

Massey, J. (1994). Guessing and entropy. In *Proceedings of the IEEE Symposium on Information Theory*, IEEE Computer Society, 204

Matuszyk, P., & Spiliopoulou, M. (2014). Hoeffding-CF: Neighbourhood-based recommendations on reliably similar users. In *Proceedings of the International Conference in User Modeling, Adaptation, and Personalization (UMAP 2014)*, Springer-Verlag, 146-157

McAvinue, L.P., & Robertson, I.H. (2007). Measuring visual imagery ability: A review. *Imagination, Cognition and Personality, 26*, 191-211

McGrew, K.S. (2009). CHC theory and the human cognitive abilities project: Standing on the shoulders of the giants of psychometric intelligence research. *Intelligence, 37*(1), 1-10

McKay, M.T., Fischler, I. & Dunn, B.R. (2003). Cognitive style and recall of text: An EEG analysis. *Learning and Individual Differences, 14*, 1-21

Messick, S. (1984). The nature of cognitive styles: Problems and promises in educational research. *Educational Psychologist, 19*, 59-74

Micarelli, A., & Sciarrone, F. (1996). A case-based system for adaptive hypermedia navigation. In *Proceedings of Advances in Case-Based Reasoning*, 266-279

Microsoft (2015). Outlook free personal e-mail. Available online at http://www.outlook.com (accessed June 2015)

Mihajlov, M., & Jerman-Blazic, B. (2011). On designing usable and secure recognition-based graphical authentication mechanisms. *Interacting with Computers, 23*(6), 582-593

Miller, G. (1956). The magical number seven, plus or minus two: Some limits on our capacity for processing information. *The psychological review, 63*, 81-97

Milosevic, D., Brkovic, M., Debevc, M., & Krneta, R. (2007). Adaptive learning by using SCOs metadata. *Knowledge and Learning Objects, 3*, 163-174

Mitchell, T., Chen, S.Y., & Macredie, R. (2004). Adapting hypermedia to cognitive styles: Is it necessary? In *Proceedings of Workshop on Individual Differences in Adaptive Hypermedia (at AH 2004)*, Springer-Verlag

Mitrovic, A., & Martin, B. (2002). Evaluating the effects of open student models on learning. In *Proceedings of the International Conference on Adaptive Hypermedia and Adaptive Web-Based Systems (AH 2002)*, Springer-Verlag, 296-305

Miyahara, K., & Pazzani, M. (2000). Collaborative filtering with the simple Bayesian classifier. In *Proceedings of the Pacific Rim International Conference on Artificial Intelligence (PRICAI 2000)*, 679-689

Mobasher B., Dai, H., Luo, T., Nakagawa, M., & Wiltshire, J. (2002). Discovery of aggregate usage profiles for web personalization. *Data Mining and Knowledge Discovery, 6*(1), 61-82

Mobasher, B. (2007). Data mining for web personalization. In *The adaptive web*, Brusilovsky P., Kobsa A., & Nejdl W. (eds.). LNCS, Vol. 4321, Springer-Verlag, 90-135

Mobasher, B., Cooley, R., & Srivastava, J. (2000). Automatic personalization based on Web usage mining. *Communications of the ACM 43*(8), 142-151

Moradi, M., & Keyvanpour, M.R. (2014). CAPTCHA and its alternatives: A review. *Security and Communication Networks*, doi: 10.1002/sec.1157

Mulvenna, M., Anand, S., & Boechner, A. (2000). Personalization on the net using web mining: introduction. *Communications of the ACM, 43*(8), 122-125

Nasraoui, O., Soliman, M., Saka, E., Badia, A. & Germain, R. (2008). A web usage mining framework for mining evolving user profiles in dynamic web sites. *IEEE Transactions on Knowledge and Data Engineering, 20*(2), 202-215

Nelson, D., & Vu, K. (2010). Effectiveness of image-based mnemonic techniques for enhancing the memorability and security of user-generated passwords. *Computers in Human Behavior, 26*(4), 705-715

Neumann, G., & Zirvas, J. (1998). SKILL: A scalable internet-based teaching and learning system. In *Proceedings of the World Conference of the WWW, Internet & Intranet*, 688-693

Nicholson, J., Coventry, L., & Briggs, P. (2013). Age-related performance issues for PIN and face-based authentication systems. In *Proceedings of ACM SIGCHI Conference on Human Factors in Computing Systems (CHI 2013)*, ACM Press, 323-332

Nicholson, J., Dunphy, P., Coventry, L., Briggs, P., & Olivier, P.A. (2012) Security assessment of tiles: A new portfolio-based graphical authentication system. In *Extended Abstracts of the ACM SIGCHI Conference on Human Factors in Computing Systems (CHI 2012)*, ACM Press, 1967-1972

Nikovski, D., & Kulev, V. (2006). Induction of compact decision trees for personalized recommendation. In *Proceedings of the 2006 ACM Symposium on Applied Computing (SAC 2006)*, ACM Press, 575-581

Niu, W., & Kay, J. (2010). PERSONAF: Framework for personalised ontological reasoning in pervasive computing. *User Modeling and User-Adapted Interaction 20*(1), 1-40

NuCAPTCHA Inc. (2015). NuCAPTCHA - Adaptive captcha authentication. Retrieved on May 04, 2015 http://www.nucaptcha.com

O'Gorman, L. (2003). Comparing passwords, tokens, and biometrics for user authentication. In *Proceedings of the IEEE, 91*(12), 2019-2040

Oates, J.M., & 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*, Psychological Press, 447-462

Paivio, A. (2006). *Mind and its evolution: A dual coding theoretical approach*. Mahwah, NJ: Lawrence Erlbaum Associates

Paivio, A., & Csapo, K. (1973). Picture superiority in free recall: Imagery or dual coding? *Cognitive Psychology, 5*(2), 176-206

Panayiotou, C., & Samaras, G. (2004). mPersona: Personalized portals for the wireless user: An agent approach. *Journal of ACM Mobile Networks and Applications (MONET), 9*(6), 663-677

Papanikolaou K.A., Grigoriadou M., Kornilakis H., & Magoulas G.D. (2003). Personalizing the interaction in a web-based educational hypermedia system: the case of INSPIRE. *User-Modeling and User-Adapted Interaction, 13*(3), 213-267

Papatheocharous, E., Belk, M., Germanakos, P., & Samaras, G. (2014). Towards implicit user modeling based on artificial intelligence, cognitive styles and web interaction data. *International Journal on Artificial Intelligence Tools, 23*(2), 21 pages

Paramythis, A., & Loidl-Reisinger, S. (2004). Adaptive learning environments and elearning standards. *Electronic Journal of e-Learning 2*(1), 181-194

Parka, S., Sureshb, N., & Jeonga, B. (2008). Sequence-based clustering for web usage mining: A new experimental framework and ann-enhanced k-means algorithm. *Data & Knowledge Engineering, 65*(3), 512-543

Passfaces Corporation (2009). The science behind passfaces. White paper, http://www.passfaces.com/enterprise/resources/white_papers.htm

Pazzani, M. (1999). A framework for collaborative, content-based and demographic filtering. *Artificial Intelligence Review, 13*(5-6), 393-408

Pazzani, M., & Billsus, D. (2007). Content-based recommendation systems. In *The adaptive web*, Brusilovsky P., Kobsa A., & Nejdl W. (eds.). LNCS, Vol. 4321. Springer-Verlag, 325-341

Perkowitz, M., & Etzioni, O. (1999). Towards adaptive Web sites: conceptual framework and case study. *Computer Networks 31*(11-16), 1245-1258

Perkowitz, M., & Etzioni, O. (2000). Adaptive web sites. *Communications of the ACM, 43*(8), 152-158

PersonaWeb (2015). Personalizing Generic Web Environments. Available online at http://personaweb.cs.ucy.ac.cy (accessed August 2015)

Peterson, E., Deary, I., & Austin, E. (2005). A new measure of verbal-imagery cognitive style: VICS. *Personality and Individual Differences, 38*, 1269-1281

Peterson, E., Rayner, S., & Armstrong, S. (2009). Researching the psychology of cognitive style and learning style: Is there really a future? *Learning and Individual Differences, 19*(4), 518-523

Pierrakos, D., Paliouras, G., Papatheodorou, C., & Spyropoulos, C. (2003). Web usage mining as a tool for personalization: A survey. *User Modeling and User-Adapted Interaction, 13*(4), 311-372

Pierrakos, D., Paliouras, G., Papatheodorou, C., Karkaletsis, V., & Dikaiakos, M. (2004). Web community directories: A new approach to web personalization. In *Web Mining: From Web to Semantic Web: First European Web Mining Forum (EWMF 2003), 3209*, 113-129

Pitkow, J., Schütze, H., Cass, T., Cooley, R., Turnbull, D., Edmonds, A., Adar, E., & Breuel, T. (2002). Personalized search. *Communications of the ACM 45*(9), 50-55

Polderman, T.J.C., Stins, J.F., Posthuma, D., Gosso, M.F., Verhulst, F.C., & Boomsma, D.I. (2006). The phenotypic and genotypic relation between working memory speed and capacity. *Intelligence, 34*(6), 549-560

Posner, M.I. (1980). Orienting of attention. *The VIIth Sir Frederic Barlett Lecture, Quarterly Journal of Experimental Psychology, 32A*, 3-25

Posner, M.I., & Petersen, S.E. (1990). The attention system of the human brain. *Annual Review of Neuroscience, 13*, 25-42

Posner, M.I., & Raicle, M.E. (1997). *Images of mind*. Scientific American Library, New York

Precision Conference Solutions (2015). PCS paper management system. Available online at http://precisionconference.com/ (accessed May 2015)

Proctor, R., Lien, M.C., Vu, K.P., Schultz, E., & Salvendy, G. (2002). Improving computer security for authentication of users: Influence of proactive password restrictions. *Behavior Research Methods, 34*, 163-169

Pu, P., & Faltings, B. (2002). Personalized navigation of heterogeneous product spaces using SmartClient. In *Proceedings of the International Conference on Intelligent User Interfaces (IUI 2002)*, ACM Press, 212-213

Reder, L.M., Park, H., & Kieffaber, P.D. (2009). Memory systems do not divide on consciousness: Reinterpreting memory in terms of activation and binding. *Psychological Bulletin, 135*(1), 23-49

Reinecke, K., & Bernstein, A. (2011). Improving performance, perceived usability, and aesthetics with culturally adaptive user interfaces. *Transactions of Computer-Human Interaction, 18*(2), Article 8, 29 pages

Renaud, K., Mayer, P., Volkamer, M., & Maguire, J. (2013). Are graphical authentication mechanisms as strong as passwords?. In *Proceedings of the Federated Conference on Computer Science and Information Systems (FedCSIS 2013)*, IEEE Computer Society, 837-844

Rett, J., Dias, J., & Ahuactzin, J.M. (2008). Laban movement analysis using a bayesian model and perspective projections. *Brain, Vision and AI, 4*re(6), 953-978

Reynaga, G., & Chiasson, S. (2013). The usability of CAPTCHAs on smartphones. In *Proceedings of the Conference on Security and Cryptography (SECRYPT 2013)*, 427-434

Rezaei, A.R., & Katz, L. (2004). Evaluation of the reliability and validity of the cognitive styles analysis. *Personality and Individual Differences, 26*, 1317-1327

Riding, R. (1991). *Cognitive style analysis - Research administration*. Learning and Training Technology

Riding, R., & Cheema, I. (1991). Cognitive styles - An overview and integration. *Educational Psychology, 11*(3/4), 193-215

Rist, T. (2001). A perspective on intelligent information interfaces for mobile users. In *Proceedings of the International Conference on Human-Computer Interaction (HCII 2001)*, Springer-Verlag, 154-158

Robertson, E.K., & Köhler, S. (2007). Insights from child development on the relationship between episodic and semantic memory. *Neuropsychologia, 45*(14), 3178-3189

Ross, S.A., Halderman, J.A., & Finkelstein, A. (2010). Sketcha: a CAPTCHA based on line drawings of 3D models. In *Proceedings of the ACM Conference on World Wide Web (WWW 2010)*, ACM Press, 821-830

Rossi, G., Schwade, D., & Guimaraes, M.R. (2001). Designing personalized web applications. In *Proceedings of the International Conference on World Wide Web (WWW 2001)*, ACM Press, 275-284

Rui, Y., & Liu, Z. (2004). ARTiFACIAL: Automated reverse turing test using FACIAL features. *Multimedia Systems, 9*, 493-502

Sadler-Smith, E., & Riding, R.J. (1999). Cognitive style and instructional preferences. *Instructional Science, 27*(5), 355-371

Sae-Bae, N., Ahmed, K., Isbister, K., & Memon, N. (2012). Biometric-rich gestures: A novel approach to authentication on multi-touch devices. In *Proceedings of the ACM SIGCHI International Conference on Human Factors in Computing Systems (CHI 2012)*, ACM Press, 977-986

Salton, G., & McGill, M. (1983). *Introduction to Modern Information Retrieval*. McGraw-Hill

Sandhu, R. (1998). Role-based access control. *Advances in Computers, 46*, Academic Press

Schafer, J.B., Frankowski, D., Herlocker, J., & Sen, S. (2007). Collaborative filtering recommender systems. In *The adaptive web*, Brusilovsky, P., Kobsa, A., & Nejdl, W. (eds.), LNCS, Vol. 4321. Springer-Verlag, 291-324

Schaie, W. (2013). *Developmental influences on adult Intelligence: The Seattle longitudinal study: Second Edition*, New York, NY: Oxford University Press

Schaub, F., Deyhle, R., & Weber, M. (2012). Password entry usability and shoulder surfing susceptibility on different smartphone platforms. In *Proceedings of the Conference on Mobile and Ubiquitous Multimedia (MUM 2012)*, ACM Press, 1-10

Schlöglhofer, R., & Sametinger, J. (2012). Secure and usable authentication on mobile devices. In *Proceedings of the ACM Conference on Advances in Mobile Computing & Multimedia (MoMM 2012)*, ACM Press, 257-262

Schneider-Hufschmidt, M., Kühme, T., & Malinowski, U. (1993). *Adaptive user interfaces: Principles and practice*. Human Factors in Information Technology, North-Holland, Amsterdam

Schwarzkopf, E. (2001). An adaptive web site for the UM 2001 conference. In *Proceedings of the User Modeling Workshop on Machine Learning for User Modeling*, 77-86

Securimage v.3.5.2 (2014). http://www.phpcaptcha.org

Sekuler, R., & Blake., R. (2002). *Perception: Fourth Edition*. Boston: McGraw-Hill

Shannon, C. (1949). A mathematical theory of communication. *Bell System Technical Journal, 27*, 379-423

Shay, R., Bauer, L., Christin, N., Cranor, L., Forget, A., Komanduri, S., Mazurek, M., Melicher, W., Segreti, S., & Ur, B. (2015). A spoonful of sugar? The impact of guidance and feedback on password-creation behavior. In *Proceedings of ACM Conference on Human Factors in Computing Systems (CHI 2015)*, ACM Press, 2903-2912

Shay, R., Kelley, P., Komanduri, S., Mazurek, M., Ur, B., Vidas, T., Bauer, L., Christin, N., & Cranor, L. (2012). Correct horse battery staple: Exploring the usability of system-assigned passphrases. In *Proceedings of the ACM Symposium on Usable Privacy and Security (SOUPS 2012)*, ACM Press, Article 7, 20 pages

Shay, R., Komanduri, S., Kelley, P., Leon, P., Mazurek, M., Bauer, L., Christin, N., & Cranor, L. (2010). Encountering Stronger Password Requirements: User Attitudes and Behaviors. In *Proceedings of the ACM Symposium on Usable Privacy and Security (SOUPS 2010)*, ACM Press, Article 2, 20 pages.

Shipstead, Z., & Broadway, J. (2013). Individual differences in working memory capacity and the stroop effect: Do high spans block the words? *Learning and Individual Differences, 26*, 191-195

Shirali-Shahreza, S., Penn, G., Balakrishnan, R., & Ganjali, Y. (2013). Seesay and hearsay CAPTCHA for mobile interaction. In *Proceedings of the ACM SIGCHI Conference on Human Factors in Computing Systems (CHI 2013)*, ACM Press, 2147-2156

Sleeman, D., & Brown, J.S. (1982). Intelligent tutoring systems. *Academic Press 228*(4698), 456-62

Smyth, B. (2007). Case-based recommendation. In *The adaptive web*, Brusilovsky, P., Kobsa, A., & Nejdl W. (eds.), LNCS, Vol. 4321, Springer-Verlag, 342-376

SolveMedia (2015). SolveMedia official Web-site. Retrieved on May 04, 2015 http://www.solvemedia.com

Steichen, B., Wu, M., Toker, D., Conati, C., & Carenini, G. (2014). Te, Te, Hi, Hi: Eye gaze sequence analysis for informing user-adaptive information visualizations. In *Proceedings of the International Confernce on User Modeling, Adaptation, and Personalization (UMAP 2014)*, Springer-Verlag, 183-194

Stern, L.W. (1900). *Uber psychologie der individuellen differenzen (Ideen zu einer "differentiellen psychologie")*, Leipzig, Barth

Sternberg, R.J. & Grigorenko, E.L. (1997). Are cognitive styles still in style? *American Psychologist, 52*(7), 700-712

Stroop, J.R. (1935). Studies of interference in serial verbal reactions. *Experimental Psychology, 18*, 643-662

Su, J., Tseng, S., Lin, H., & Chen, C. (2011). A personalized learning content adaptation mechanism to meet diverse user needs in mobile learning environments. *User Modeling and User-Adapted Interaction, 21*(1-2), 5-49

Su, X., & Khoshgoftaar, T. (2009). A survey of collaborative filtering techniques. *Advances in Artificial Intelligence*, Article 4, 19 pages

SweetCAPTCHA (2015). SweetCAPTCHA - Fun and human friendly captcha. Retrieved on May 04, 2015 http://sweetcaptcha.com

Swindler, G. (2001). Mental models and hypermedia. *EDETC795 Problems/ Educational Technology (Hypermedia)*

Tao, H., & Adams, C. (2008). Pass-Go: A proposal to improve the usability of graphical passwords. *Network Security, 7*(2), 273-292

Tarpin-Bernard, F., & Habieb-Mammar, H. (2005). Modeling elementary cognitive abilities for adaptive hypermedia presentation. *User Modeling and User-Adapted Interaction, 15*(5), 459-495

Teevan, J., Karlson, A., Amini, S., Brush, A.J.B., & Krumm, J. (2011). Understanding the importance of location, time, and people in mobile local search behavior. In *Proceedings of the International Conference on Human Computer Interaction with Mobile Devices and Services (MobileHCI 2013)*, ACM Press, 77-80

Tennant, M. (1988). *Psychology and adult learning*. Routledge, London

Thomas, C. & Fischer, G. (1997). Using agents to personalize the Web. In *Proceedings of the ACM Conference on Intelligent User Interfaces (IUI 1997)*, ACM Press, 53-60

Thomas, R.K. (1997). Team-based access control (TMAC): A primitive for applying role-based access controls in collaborative environments. In *Proceedings of the ACM workshop on Role-based Access Control*

Thurstone, L. (1948). *Primary mental capabilities*. Chicago, IL: University of Chicago Press

Tolman, E.C. (1948). Cognitive maps in rats and men. *Psychological Review 55*(4), 189-208

Trajkova, J., & Gauch, S. (2004). Improving ontology-based user profiles. In *Proceedings of RIAO 2004*, 380-389

Triantafillou, E., Pomportsis, A., Demetriadis, S., & Georgiadou, E. (2004). The value of adaptivity based on cognitive style: an empirical study. *British Journal of Educational Technology, 35*, 95-106

Tsianos, N., Germanakos, P., Belk, M., Lekkas, Z., Samaras, G., & Mourlas, C. (2013). An individual differences approach in designing ontologies for efficient personalization. In *Springer Series Studies in Computational Intelligence, edited volume Semantic Hyper/Multi-media Adaptation: Schemes and Applications*. Anagnostopoulos, I., Bielikova, M., Mylonas, P., & Tsapatsoulis, N. (eds.), Springer-Verlag, 3-21

Tsianos, N., Germanakos, P., Lekkas, Z., Mourlas, C., Belk, M., Christodoulou, E., Spanoudis, G., & Samaras G. (2008). Enhancing elearning environments with users' cognitive factors: The case of EKPAIDEION. In *Proceedings of the European Conference on e-Learning (ECEL 2008)*, 877-889

Tsianos, N., Lekkas, Z., Germanakos, P., Mourlas, C., & Samaras, G. (2009). An experimental assessment of the use of cognitive and affective factors in adaptive educational hypermedia. *IEEE Transactions on Learning Technologies (TLT), 2*(3), 249-258

Tsianos, T., Germanakos, P., Lekkas, Z., Saliarou, A., Mourlas, C., & Samaras, G. (2010). A preliminary study on learners physiological measurements in educational hypermedia. In *Proceedings of the IEEE International Conference on Advanced Learning Technologies (ICALT 2010)*, IEEE Computer Society, 61-63

Tsiriga, V., & Virvou, M. (2003). Modelling the student to individualise tutoring in a web-based ICALL. *International Journal of Continuing Engineering Education and Lifelong Learning, 13*(3-4), 350-365

Tullis, T.S., Tedesco, D.P., & McCaffrey, K.E. (2011). Can users remember their pictorial passwords six years later? In *Proceedings of the ACM SIGCHI International Conference on Human Factors in Computing Systems (CHI 2011)*, ACM Press, 1789-1794

Unsworth, N., & Spillers, G. (2010). Working memory capacity: Attention control, secondary memory, or both? A direct test of the dual-component model. *Memory and Language, 62*, 392-406

van Oorschot, P.C. & Wan, T. (2009). Twostep: An authentication method combining text and graphical passwords. In *Proceedings of the International MCETECH Conference on eTechnologies (MCETECH 2009)*, Springer-Verlag, 233-239

Varenhorst, C. (2004). *Passdoodles: A lightweight authentication method*. MIT Research Science Institute

Varnum, M., Grossmann, I., Kitayama, S., & Nisbett, R. (2010). The origin of cultural differences in cognition: The social orientation hypothesis. *Current Directions in Psychological Science, 19*(1) 9-13

Vecera, S.P., Cosman, J.D., Vatterott, D.B., & Roper, Z.J.J. (2014). The control of visual attention: Toward a unified account. *Psychology of Learning and Motivation, 60*, 303-347

Vikram, S., Fan, Y., & Gu, G. (2011). SEMAGE: A new image-based two-factor CAPTCHA. In *Proceedings of the ACM Conference on Computer Security Applications (ACSAC 2011)*, ACM Press, 237-246

von Ahn, L., Blum, M., & Langford, J. (2004). Telling humans and computers apart automatically. *Communications of the ACM, 47*, 56-60

von Ahn, L., Maurer, B., McMillen, C., Abraham, D., & Blum, M. (2008). reCAPTCHA: Human-based character recognition via web security measures. *Science, 321*(5895), 1465-1468

von Zezschwitz, E., De Luca, A., & Hussmann, H. (2013). Survival of the shortest: A retrospective analysis of influencing factors on password composition. In *Proceedings of the of the IFIP TC13 Conference on Human-Computer Interaction (INTERACT 2013)*, Springer-Verlag, 460-467

von Zezschwitz, E., De Luca, A., & Hussmann, H. (2014). Honey, I shrunk the keys: Influences of mobile devices on password composition and authentication performance. In *Proceedings of the Nordic Conference on Human-Computer Interaction: Fun, Fast, Foundational (NordiCHI 2014)*, ACM Press, 461-470

von Zezschwitz, E., De Luca, A., Brunkow, B., & Hussmann, H. (2015). SwiPIN: Fast and secure pin-entry on smartphones. In *Proceedings of the ACM SIGCHI Conference on Human Factors in Computing Systems (CHI 2015)*, ACM Press, 1403-1406

Vu, K., Proctor, R., Bhargav-Spantzel, A., Tai, B., Cook, J., & Schultz, E. (2007). Improving password security and memorability to protect personal and organizational information. *International Journal of Human-Computer Studies, 65*(8), 744-757

Wærn, A., (2004). User involvement in automatic filtering: An experimental study. *User Modeling and User-Adaptive Interaction, 14*(2-3), 201-237

Walker, E., Rummel, N., & Koedinger, K. (2009). CTRL: A research framework for providing adaptive collaborative learning support. *User Modeling and User-Adapted Interaction 19*(5), 387-431

Wang, K., & Tan, Y. (2011). A new collaborative filtering recommendation approach based on naive Bayesian method. In *Proceedings of the International Conference on Advances in Swarm Intelligence (ICSI 2011)*, 218-227

Wang, K.H., Wang, T.H., Wang, W.L., & Huang, S.C. (2006). Learning styles and formative assessment strategy: enhancing student achievement in Web-based learning. *Journal of Computer Assisted Learning, 22*, 207-217

Warner, S., & Demick, J. (2009). *Field dependence-independence: Cognitive style across the life-span*. Psychology Press, New York, NY

Weber, G. & Specht, M. (1997). User modeling and adaptive navigation support in WWW-based tutoring systems. In *Proceedings of the International Conference on User Modeling (UM 1997)*, Springer-Verlag, 289-300

Weber, G., & Brusilovsky, P. (2001). ELM-ART: An adaptive versatile system for Web-based instruction. *International Journal of Artificial Intelligence in Education, 12*(4), 351-384

Wei, T., Jeng, A., & Lee, H. (2012). GeoCAPTCHA – A novel personalized CAPTCHA using geographic concept to defend against third party human attack. In *Proceedings of the International Conference on Performance Computing and Communications Conference (IPCCC 2012)*, IEEE Computer Society, 392-399

Wen, J., Dou, Z., & Song, R. (2009). Personalized web search. *Encyclopedia of Database Systems*, Springer-Verlag

Wertheimer, M. (1923). Gestalt psychology, gestalt theory. *Psychologische Forschung, 3*(4), 301-350

Whitehouse, A.J.O., Maybery, M.T., & Durkin, K. (2006). The development of the picture superiority effect. *British Journal of Developmental Psychology, 24*, 767-773

Wiedenbeck, S., Waters, J., Birget, J., Brodskiy, A., & Memon, N. (2005). Authentication using graphical passwords: Effects of tolerance and image choice. In *Proceedings of the ACM Symposium on Usable Privacy and Security (SOUPS 2005)*, ACM Press, 1-12

Wikipedia (2015). Available online at http://www.wikipedia.org (accessed May 2015).

Winkler, C., Gugenheimer, J., De Luca, A., Haas, G., Speidel, P., Dobbelstein, D., & Rukzio, E. (2015). Glass unlock: Enhancing security of smartphone unlocking through leveraging a private near-eye display.

In *Proceedings of the ACM Conference on Human Factors in Computing Systems (CHI 2015)*. ACM Press, 1407-1410

Winn, W., & Snyder, D. (2001). *Mental representation. The handbook of research for educational communications and technology (Chapter 5)*. Bloomington, IN: The Association of Educational Communications and Technology

Wismer, A., Madathil, K.C., Koikkara, R., Juang, K., & Greenstein, J. (2012). Evaluating the usability of CAPTCHAs on a mobile device with voice and touch input. In *Proceedings of the Human Factors and Ergonomics Society Annual Meeting (HFES 2012)*, 1228-1232

Witkin, H.A. (1962). *Psychological differentiation. Studies of Development*. New York: Wiley

Witkin, H.A., Moore, C.A., Goodenough, D.R., & Cox, P.W. (1977). Field-dependent and field-independent cognitive styles and their educational implications. *Review of Educational Research, 47*(1), 1-64

Witkin, H.A., Oltman, P., Raskin, E., & Karp, S. (1971). *A manual for the embedded figures test*. Palo Alto, CA: Consulting Psychologists Press

WordPress (2015a). Free content management system. Available online at http://www.wordpress.org (accessed July 2015)

Wordpress (2015b). Wordpress statistics. Available online at https://wordpress.com/activity (accessed July 2015)

World Wide Web Consortium (W3C) (2014). CSS specifications. http://www.w3.org/Style/CSS/specs/

Wright, N., Patrick, A., & Biddle, R. (2012). Do you see your password?: Applying recognition to textual passwords. In *Proceedings of the ACM Symposium on Usable Privacy and Security (SOUPS 2012)*, ACM Press, Article 8

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. (2007). Top 10 algorithms in data mining. *Knowledge Information Systems, 14*(1), 1-37

Xu, Y., Reynaga, G., Chiasson, S., Frahm, J., Monrose, F., & van Oorschot, P. (2014). Security analysis and related usability of motion-based captchas: Decoding codewords in motion. *IEEE Transactions on Dependable and Secure Computing, 11*(5), 480-493

Yan, J., & El Ahmad, A.S. (2008). A low-cost attack on a microsoft CAPTCHA. In *Proceedings of the ACM Conference on Computer and Communications Security (CCS 2008)*, ACM Press, 543-554

Yan, J., Blackwell, A., Anderson, R., & Grant, A. (2004). Password memorability and security: Empirical results. *IEEE Security & Privacy Magazine, 2*(5), 25-31

Yang, Q., Huang, J.Z., & Ng, M. (2003). A data cube model for prediction-based web prefetching. *Intelligent Information Systems, 20*(1), 11-30

Yantis, S., & Jonides, J. (1990). Abrupt visual onsets and selective attention: Voluntary versus automatic allocation. *Journal of Experimental Psychology: Human Perception and Performance, 16*, 121-134

Zhang, J., Luo, X., Akkaladevi, S., & Ziegelmayer, J. (2009). Improving multiple-password recall: An empirical study. *Information Security, 18*(2), 165-176

Zhu, B., Yan, J., Li, Q., Yang, C., Liu, J., Xu, N., Yi, M., & Cai, K. (2010). Attacks and design of image recognition CAPTCHAs. In *Proceedings of the ACM Conference on Computer and Communications Security (CCS 2010)*, ACM Press, 187-200

APPENDIX A: Publications

We list below research papers that were published based on the outcome of this Ph.D. thesis. We categorize the publications into journal papers (4), conference papers (9) and workshop papers (2). Among these, our work on understanding the effect of human cognitive processing abilities on CAPTCHA-related user interactions received the best paper award at the Springer International Conference on Human Factors in Computing and Informatics (Springer SouthCHI 2013), and the work on personalizing user authentication tasks based on human cognitive differences received a best paper award nomination at the Springer International Conference on User Modeling, Adaptation and Personalization (Springer UMAP 2014).

Journal Publications

1. Belk M., Fidas C., Germanakos P., Samaras G. (2015). **Do Human Cognitive Differences in Information Processing Affect Preference and Performance of CAPTCHA?** *International Journal of Human-Computer Studies*, 46, 227-240, Elsevier
    - This paper reports two studies presented in **chapter 7 (section 7.8 and 7.10)** that aimed to investigate the effects of cognitive processing styles and abilities on different designs of CAPTCHA challenges.
    - It reports a short version of the literature analysis on CAPTCHA mechanisms presented in **chapter 2**.
    - It reports the suggested personalization approach in CAPTCHA tasks reported in **chapter 6**.
    - It reports a short version of the literature analysis on cognitive styles (Verbal/ Imager, Wholist/ Analyst) and cognitive processing abilities (speed and control of processing, working memory) presented in **chapter 4**.
2. Belk M., Fidas, C., Germanakos P., Samaras G. (2014). **A Personalised User Authentication Approach based on Individual Differences in Information Processing.** *Interacting with Computers*, 27(6), 706-723, Oxford University Press
    - This paper reports the architecture and main modules of PAC for personalizing user authentication tasks reported in **chapter 6**.
    - It reports a study presented in **chapter 7 (section 7.4)** that aimed to investigate the added value of personalizing user authentication tasks based on users' cognitive processing styles.
    - It reports a short version of the literature analysis on cognitive styles (Verbal/ Imager) presented in **chapter 4**.

3. Papatheocharous E., Belk M., Germanakos P., Samaras G. (2014). **Towards Implicit User Modeling based on Artificial Intelligence, Cognitive Styles and Web Interaction Data.** *Journal of Artificial Intelligence Tools*, 23(2): 21 pages, World Scientific Publishing
    - This paper reports an implicit user data collection method for eliciting users' cognitive processing styles (Verbal/ Imager) based on their viewing preference and interaction data with Web-based environments presented in **chapter 6**.
    - It reports a short version of the literature analysis on user modeling, adaptation and personalization presented in **chapter 3**.
    - It reports a short version of the literature analysis on cognitive styles (Verbal/ Imager) presented in **chapter 4**.
4. Belk M., Papatheocharous E., Germanakos P., Samaras G. (2013). **Modeling Users on the World Wide Web based on Cognitive Factors, Navigation Behavior and Clustering Techniques.** *Journal of Systems and Software, Special Issue on Web 2.0 Engineering: New Practices and Emerging Challenges*, 86(12), 2995-3012, Elsevier
    - This paper reports the suggested Web interaction metrics for measuring the navigation behavior of users presented in **chapter 6**.
    - It reports a short version of the literature analysis on user modeling, adaptation and personalization presented in **chapter 3**.
    - It reports a short version of the literature analysis on cognitive styles (Wholist/ Analyst) presented in **chapter 4**.

Conference Publications

1. Belk M., Germanakos P., Andreou P., Samaras G. (2015). **Towards a Human-centered E-Commerce Personalization Framework.** *Proceedings of the IEEE/WIC/ACM International Conference on Web Intelligence (WI 2015)*, Singapore, IEEE Computer Society Press (to appear)
    - This paper reports the formalization of the user modeling and personalization module presented in **chapter 6**.
    - It reports a short version of the literature analysis on cognitive styles (Verbal/ Imager, Wholist/ Analyst) and cognitive processing abilities (working memory) presented in **chapter 4**.
2. Fidas C., Hussmann H., Belk M., Samaras G. (2015). **iHIP: Towards a User Centric Individual Human Interaction Proof Framework.** *Proceedings of the ACM SIGCHI Conference on Human Factors in Computing Systems (CHI 2015)*, Seoul, South Korea, 2235-2240, ACM Press
    - This paper reports an extensible framework, coined iHIP, for personalizing CAPTCHA mechanisms based on human, technology and CAPTCHA design factors.

- Results of this thesis could serve as input for realizing the suggested iHIP framework based on the studies' results presented in **chapter 7**.

3. Belk M., Germanakos P., Fidas C., Samaras G. (2014). **A Personalisation Method based on Human Factors for Improving Usability of User Authentication Tasks.** *Proceedings of the International Conference on User Modeling, Adaptation, and Personalization (UMAP 2014)*, Aalborg, Denmark, 13-24, Springer-Verlag **(Best Paper Award Nomination)**
   - This paper reports the proposed personalization approach of user authentication and CAPTCHA tasks presented in **chapter 6**.
   - It reports the suggested adaptation rules presented in **chapter 8**.
   - It reports an initial study, following the same methodological approach of the study presented in **chapter 8** that aimed to investigate the added value of personalizing user authentication tasks based on users' cognitive processing styles and abilities.
   - It reports a short version of the literature analysis on cognitive styles (Verbal/ Imager, Wholist/ Analyst) and cognitive processing abilities (speed and control of processing, working memory) presented in **chapter 4**.
4. Belk M., Fidas C., Germanakos P., Samaras G. (2014). **On Supporting Security and Privacy-preserving Interaction through Adaptive Usable Security**. *Proceedings of the International Conference on Human-Computer Interaction (HCI International 2014)*, Heraklion, Crete, 3-10, Springer-Verlag
   - This paper reports the proposed concept of personalizing security-related tasks and a high-level personalization architecture presented in **chapter 5** and **chapter 6**.
5. Belk M., Fidas C., Germanakos P., Samaras G. (2013). **Security for Diversity: Studying the Effects of Verbal and Imagery Processes on User Authentication Mechanisms.** *Proceedings of the IFIP TC13 International Conference on Human-Computer Interaction (INTERACT 2013)*, Cape Town, South Africa, 442-459, Springer-Verlag
   - This paper reports a preliminary study, following a similar approach presented in **chapter 7 (section 7.4)** that aimed to investigate the effects of cognitive styles on preference and performance in user authentication.
   - It reports a short version of the literature analysis on cognitive styles (Verbal/ Imager) presented in **chapter 4**.
6. Belk M., Germanakos P., Fidas C., Samaras G. (2013). **Studying the Effect of Human Cognition on User Authentication Tasks.** *Proceedings of the International Conference on User Modeling, Adaptation, and Personalization (UMAP 2013)*, Rome, Italy, 102-113, Springer-Verlag
   - This paper reports a study presented in **chapter 7 (section 7.6)** that aimed to investigate the effects of cognitive processing abilities on different designs of user authentication.

- It reports a short version of the literature analysis on cognitive processing abilities (speed and control of processing, working memory) presented in **chapter 4**.

7. Belk M., Germanakos P., Fidas C., Holzinger A., Samaras G. (2013). **Towards the Personalization of CAPTCHA Mechanisms based on Individual Differences in Cognitive Processing.** *Proceedings of the International Conference on Human Factors in Computing and Informatics (SouthCHI 2013)*, Maribor, Slovenia, 409-426, Springer-Verlag **(Best Paper Award)**
   - This paper reports a preliminary study, following a similar methodological approach presented in **chapter 7 (section 7.10)** that aimed to investigate the effects of cognitive processing abilities on different complexity levels of CAPTCHA.
   - It reports a short version of the literature analysis on cognitive processing abilities (speed and control of processing, working memory) presented in **chapter 4**.
8. Belk M., Germanakos P., Fidas C., Spanoudis G., Samaras G. (2013). **Studying the Effect of Human Cognition on Text and Image Recognition CAPTCHA Mechanisms.** *Proceedings of the International Conference on Human-Computer Interaction (HCI International 2013)*, Las Vegas, Nevada, USA, 71-79, Springer-Verlag
   - This paper reports a preliminary study, following a similar methodological approach presented in **chapter 7 (section 7.8)** that aimed to investigate the effects of cognitive processing abilities on different designs of CAPTCHA.
   - It reports a short version of the literature analysis on cognitive processing abilities (speed and control of processing, working memory) presented in **chapter 4**.
9. Belk M., Fidas C., Germanakos P., Samaras G. (2012). **Do Cognitive Styles of Users Affect Preference and Performance related to CAPTCHA Challenges?** *Proceedings of the ACM SIGCHI Conference on Human Factors in Computing Systems (CHI 2012)*, Austin, TX, USA, 1487-1492, ACM Press
   - This paper reports a study presented in **chapter 7 (section 7.8)** that aimed to investigate the effects of cognitive processing styles on different designs of CAPTCHA challenges.
   - It reports a short version of the literature analysis on cognitive styles (Verbal/ Imager) presented in **chapter 4**.

Workshop Publications

1. Belk M., Papatheocharous E., Germanakos P., Samaras G. (2012). **Investigating the Relation between Users' Cognitive Style and Web Navigation Behavior with K-means Clustering.** *Proceedings of the International Workshop on Web Information Systems Modeling (WISM 2012), in conjunction with ER 2012*, Florence, Italy, 337-346, Springer-Verlag

- This paper reports a short version of the suggested Web interaction metrics for measuring the navigation behavior and cognitive styles of users presented in **chapter 6**.
- It briefly reports a literature analysis on user modeling, adaptation and personalization presented in **chapter 3**.

2. Germanakos P., Papatheocharous E., Belk M., Samaras G. (2012). **Data-driven User Profiling to Support Web Adaptation through Cognitive Styles and Navigation Behavior.** *Proceedings of the Mining Humanistic Data Workshop (MHDW 2012), in conjunction with AIAI 2012*, Halkidiki, Greece, 500-509, Springer-Verlag
   - This paper reports a short version of an implicit user data collection method for eliciting users' cognitive processing styles based on their interaction data with Web-based environments presented in **chapter 6**.
   - It briefly reports a literature analysis on user modeling, adaptation and personalization presented in **chapter 3**.