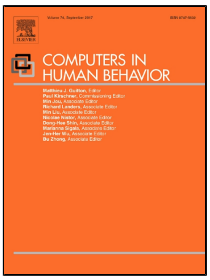
Accepted Manuscript



The Interplay between Humans, Technology and User Authentication: A Cognitive Processing Perspective

Marios Belk, Christos Fidas, Panagiotis Germanakos, George Samaras

PII:	S0747-5632(17)30412-0
DOI:	10.1016/j.chb.2017.06.042
Reference:	CHB 5053
To appear in:	*Computers in Human Behavior*
Received Date:	12 April 2017
Revised Date:	19 June 2017
Accepted Date:	30 June 2017

Please cite this article as: Marios Belk, Christos Fidas, Panagiotis Germanakos, George Samaras, The Interplay between Humans, Technology and User Authentication: A Cognitive Processing Perspective, *Computers in Human Behavior* (2017), doi: 10.1016/j.chb.2017.06.042

The Interplay between Humans, Technology and User Authentication: A Cognitive Processing Perspective

Abstract: This paper investigates the interplay among human cognitive processing differences (field dependence *vs.* field independence), alternative interaction device types (desktop *vs.* touch) and user authentication schemes (textual *vs.* graphical) towards task completion efficiency and effectiveness. A four-month user study (N=164) was performed under the light of the field dependence-independence theory which underpins human cognitive differences in visual perceptiveness as well as differences in handling contextual information in a holistic or analytic manner. Quantitative and qualitative analysis of results revealed that field independent (FI) users outperformed field dependent users (FD) in graphical authentication, FIs authenticated similarly well on desktop computers as on touch devices, while touch devices negatively affected textual password entry performance of FDs. Users' feedback from a post-study survey further showed that FD users had memorability issues with graphical authentication and perceived the added difficulty when interacting with textual passwords on touch devices, in contrast to FI users that did not have significant usability and memorability issues on both authentication and interaction device types. Findings highlight the necessity to improve current approaches of knowledge-based user authentication research by incorporating human cognitive factors in both design and run-time. Such an approach is also proposed in this paper.

Keywords: Knowledge-based User Authentication; Human Cognitive Differences; Field Dependence-Independence; Task Performance; User Study.

1. INTRODUCTION

User authentication is a cornerstone of security in today's interactive systems [Koved and Stobert, 2016]. 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 or she claims to be. Numerous user authentication schemes are currently deployed which can be classified into knowledge-based (*what the user knows*, *e.g.*, secret passwords, pictorial keys, sketches) [Biddle et al., 2012], token-based (*what the user has*, *e.g.*, credit cards) [Mare et al., 2016], and biometric-based (*what the user is*, *e.g.*, fingerprint, interaction behavior) [Renaud, 2005]. *Knowledge-based authentication schemes* are widely used today since: *a)* they are easy, fast and inexpensive to implement [Biddle et al., 2012]; and *b)* they don't entail the security and privacy flaws found in tokens (*e.g.*, loss or theft of credit card [Wang and Katabi, 2013]) and in biometrics (*e.g.*, users' fingerprints can be extracted from the objects they touch [Cao and Jain, 2016]). Research also indicates that knowledge-based approaches will continue to prevail in the next decays [Herley and van Oorschot, 2012], even in combination with other approaches (*e.g.*, token, biometric). Two important quality dimensions of an effective knowledge-based authentication scheme are related to its *security* and *usability* aspects. The security level determines its strength against adversary attacks, whereas usability levels are commonly determined by *memorability of selected secrets* and *task completion efficiency and effectiveness* [Biddle et al., 2012].

A plethora of knowledge-based authentication schemes have been proposed leveraging on different user experience and security factors, with the most prominent ones focusing on *text-based solutions* (passwords, PINs, etc.) [Herley and van Oorschot, 2012] and *graphical solutions* (pictorial, sketches, etc.) [Biddle et al., 2012; Nelson and Vu, 2010]. Text-based solutions require from users to memorize a secret that is represented by a sequence of textual characters, whereas graphical solutions are based on secret keys that typically consist of a sequence of images chosen by end-users from a pool of alternatives. Research on knowledge-based user authentication has become a complex endeavor since it embraces several parameters (human,