Available online at www.sciencedirect.com

SCIENCE @ DIRECT®

ELSEVIER

Int. J. Human-Computer Studies 63 (2005) 128–152

International Journal of Human-Computer Studies

www.elsevier.com/locate/ijhcs

Is a picture really worth a thousand words? Exploring the feasibility of graphical authentication systems

Antonella De Angeli[a,*,1], Lynne Coventry[a], Graham Johnson[a], Karen Renaud[b]

[a]*Advanced Technology & Research, NCR Financial Solutions Group Ltd, 3 Fulton Road, Dundee, DD2 4SW, UK*

[b]*Department of Computing Science, University of Glasgow, 17 Lilybank Gardens, Glasgow G12 8RZ, UK*

Abstract

The weakness of knowledge-based authentication systems, such as passwords and Personal Identification Numbers (PINs), is well known, and reflects an uneasy compromise between security and human memory constraints. Research has been undertaken for some years now into the feasibility of graphical authentication mechanisms in the hope that these will provide a more secure and memorable alternative. The graphical approach substitutes the exact recall of alphanumeric codes with the recognition of previously learnt pictures, a skill at which humans are remarkably proficient. So far, little attention has been devoted to usability, and initial research has failed to conclusively establish significant memory improvement. This paper reports two user studies comparing several implementations of the graphical approach with PINs. Results demonstrate that pictures can be a solution to some problems relating to traditional knowledge-based authentication but that they are not a simple panacea, since a poor design can eliminate the picture superiority effect in memory. The paper concludes by

[*]Corresponding author. Tel. +44 161 306 3383; fax: +44 161 306 1281.
E-mail address: antonella.de-angeli@manchester.ac.uk (A. De Angeli).

[1]Present address: Centre for HCI Design, School of Informatics, University of Manchester, PO BOX 88, Manchester, M60 1QD, UK.

doi:10.1016/j.ijhcs.2005.04.020

discussing the potential of the graphical approach and providing guidelines for developers contemplating using these mechanisms.

Keywords: User authentication; Visual memory; Usability; Security

1. Introduction

User authentication is a problem for every system providing secure access to valuables, confidential information, or personalised services. Most systems make use of knowledge-based authentication mechanisms, such as *Personal Identification Numbers* (PINs) and passwords, because they are simple to administer, well understood by users and system administrators alike, and require no extra hardware or software (Renaud and De Angeli, 2004). Despite this, passwords and PINs have a number of well-known deficiencies reflecting a difficult compromise between security and memorability (Adams and Sasse, 1999; Besnard and Arief, 2004). Secure codes must be composed of a long, random selection of alphanumeric keys but unfortunately humans struggle to remember meaningless strings. Thus they choose simple and predictable words or numbers related to everyday life, and engage in insecure practices, such as writing passwords down or sharing them. The problem is so serious that the user is often referred to as the 'weakest link' in the security chain (Sasse et al., 2001).

Biometric techniques—those that make use of physiological or behavioural characteristics of an individual to confirm identity during authentication—may alleviate memory load, but they too need to resolve the security-usability balance for general usage (Coventry et al., 2003a, b). Biometrics cause additional consumer concerns about privacy. Until biometrics become more robust, easy to use and ubiquitous, knowledge-based authentication will prevail and research into this mechanism is needed.

A number of graphical authentication systems have emerged, especially in the area of handheld devices, for which typewritten input is less common than pointing at the screen (Jansen et al., 2003). The basic idea behind graphical authentication is that exact password *recall* is replaced by *recognition* of pictures. It is claimed that these mechanisms are more secure, easier to use and more appealing to the general public than PINs and passwords (Jermyn et al., 1999; Dhamija and Perrig, 2000; Weinshall and Kirkpatrick, 2004). Unfortunately, most proposals emphasise security and tend to over-estimate visual-memory capabilities, with usability being given scant attention.

This paper addresses the usability of graphical mechanisms based on two user studies carried out within the Visual Identification Protocol (VIP) project to assess the potential of graphical authentication for Automatic Teller Machines (ATMs). This is a highly constrained environment with strong usability and security issues. Consumers of all types need to 'walk up and use' the same machine engaging in a very brief goal-oriented and secure interaction. Owners of terminals cannot allow the