A Visuo-Biometric Authentication Mechanism for Older Users

Karen Renaud

Department of Computing Science, University of Glasgow, Glasgow G12 8RZ, UK
Email: karen@dcs.gla.ac.uk

The Web is an invaluable resource for users of all ages, but it especially offers facilities which can make a huge difference to the lives of elderly users, many of whom have to contend with limited mobility and frequent illness. Whereas there is some understanding of the issues that pertain to designing websites for this group of users, the issue of specialized Web authentication has not received much attention. Web authentication is often treated as a one-size-fits-all problem with ubiquitous use of the password, and indeed authentication is seldom tailored to the needs of either the site or the target users. Sites are seldom subjected to a risk analysis before an authentication mechanism is chosen. This paper proposes a technique for matching the risk levels of a website to the security rating of an authentication mechanism and presents an authentication mechanism that is tailored to the needs of elderly users for protecting sites with a low risk rating. Usage data from a field test of this mechanism is reported, which show that the mechanism is indeed feasible and meets older users' needs.

Keywords: authentication, risk, security, elderly users, visual, biometrics.

1 Introduction

The Web has come of age, and offers immeasurable enrichment to many people's lives. The special group of interest to this paper is older users who no longer need to be excluded from things like shopping, social interchange and banking when they or their friends are house-bound due to ill health or long-term infirmity. The Web offers access to a variety of these kinds of facilities and more besides. Much attention has been paid to designing websites for the aged [Hawthorn 2003], but one of the biggest obstacles still remaining is the issue of user authentication, which often requires that
the user remember a password, something that becomes more and more difficult with age and presents an oft-insurmountable obstacle.

A popular and reliable authentication mechanism is the biometric — either physiological or behavioural. However, the former has limitations related to secure biometric capture at enrolment in an uncontrolled environment such as the Web, and many users also have concerns related to privacy [Braghin 2000; Berghel 2000] and the impossibility of replacement should it be leaked. Furthermore, recording the most popular biometric, the fingerprint, is notoriously fraught with difficulty for older users [Garfinkel 2002]. Behavioural biometrics have some potential but are often difficult to measure in a Web environment without specialized software being installed on the user's machine, something that many Web administrators are reluctant to require of their users.

Web users are thus usually authenticated by means of a knowledge-based mechanism — either a password on its own or accompanied by a token such as a smart card — implementing a stronger two-factor authentication. Smart cards work admirably and can be tailored for the use of older users [Gill 2004], but they can also be mislaid or stolen. They are currently fairly costly to issue so their use will probably be restricted to high risk sites. In knowledge-based authentication the user carries the burden of proof — having to remember a personal identification number (PIN) or password. This is a particular problem for users with short-term memory limitations, which is often the case in older users.

The direct consequence of this is that Web users are almost ubiquitously authenticated by a password and eventually they find that they have far too many passwords to remember. Since passwords rely on uncued exact recall, it becomes more and more difficult to keep track. Some schemes have been proposed which can accommodate less than perfect recall [Ellison et al. 2000] but these require special software, and are not widely used on the Web.

Passwords are no picnic for the system administrator either. The first problem is to decide whether to issue or request passwords. System-specified passwords present memorability difficulties resulting in frequent requests for replacement passwords. Reports of between a third [Walker 2001] and a half [Doran 1999] of help-desk calls being related to passwords emphasize the size of this problem. Passwords can be automatically replaced by means of email, but this is seldom encrypted, and thus easy for a determined hacker to intercept. The more memorable self-selected passwords tend also to be too predictable, which impacts security. System administrators have various strategies in dealing with the "password problem" [Dhamija & Perrig 2000]: carry out proactive password checking when the password is specified by the user to ensure that a strong password is chosen; impose a forced-renewal policy so that leaked passwords eventually age; allow a limited number of tries before locking an account; run a password cracking program regularly to identify weak passwords; or offer training and education to users to increase security awareness.

The latter has very limited success in a Web environment [Friedman et al. 2002], and the other mechanisms are essentially technical solutions to a human problem. Apart from the human (both client and administrator) problems, we need to consider the strength of the authentication mechanism. Passwords have the potential to be