Chapter 8
Usability Evaluation of Dialogue Designs for Voiceprint Authentication in Automated Telephone Banking

Nancie Gunson
The University of Edinburgh, UK

Fergus McInnes
The University of Edinburgh, UK

Diarmid Marshall
The University of Edinburgh, UK

Hazel Morton
The University of Edinburgh, UK

Mervyn Jack
The University of Edinburgh, UK

ABSTRACT

This paper describes an empirical investigation of the usability of different dialogue designs for voiceprint authentication in automated telephone banking. Three strategies for voice authentication were evaluated in an experiment with 120 telephone banking end-users: 1-Factor (voiceprint authentication based on customers' utterances of their account number and sort code); 1-Factor with Challenge (1-Factor plus a randomly generated digit string); and 2-Factor (1-Factor plus secret information known only to the caller). The research suggests the 2-Factor approach is the most effective strategy in this context: results from a Likert questionnaire show it to be highly usable and it is rated highest in terms of both security and overall quality. Participants welcome the option to use voiceprint technology but the majority would prefer it to augment rather than replace existing security methods.

DOI: 10.4018/978-1-5225-2589-9.ch008

1. INTRODUCTION

Despite substantial research efforts devoted to the development of voiceprint authentication technology e.g. the NIST evaluation program (Martin, Przybocki, & Campbell Jr, 2005), surprisingly few studies have been reported which examine users' attitudes towards it (Gunson, Marshall, McInnes, & Jack, 2011; Tassabehji & Kamala, 2009; Toledano, Fernández Pozo, Hernández Trapote, & Hernández Gómez, 2006). This is important since the usability of new security measures is vital for customer cooperation and acceptance (O'Gorman, 2003). In this paper, an empirical study is described which provides a comprehensive usability evaluation of three different dialogue designs for voiceprint authentication in automated telephone banking. The three designs chosen offer different levels of security based on different levels of user input, with the aim of examining the relationship between security and usability. All are realistic options for deployment.

The rest of the paper is organised as follows. A review of the relevant literature is provided in Section 2. Section 3 details the three different dialogue designs for voiceprint authentication that were examined. Section 4 describes the research methodology, Section 5 the experiment design and Section 6 the participants. Results are presented in Section 7 with conclusions given in Section 8.

2. BACKGROUND

Although Internet banking is increasingly popular, with one survey reporting 47% of respondents used it in the previous month (Gartner, 2009), automated telephone banking continues to be an important service delivery channel for banking organisations around the world. The U.K. service on which the application in this research is based, for instance, has 4 million registered users, and receives 5.5 million calls per month. Its development is the subject of continued interest at the Bank.

The customer authentication process in the existing service is knowledge-based ("what you know"). Users must recall two digits selected at random from their Secret Number or 'PIN'. The service is not alone in this method - the use of a PIN or alphanumeric password (or some combination of the two) is the current *de facto* standard for customer verification in U.K. telephone banking.

When they are used correctly, such passwords and PINs play an important part in the security of automated services (O'Gorman, 2003). However, the ubiquity of their use across different applications means that users are typically required to have many, making it difficult to remember them all.

A common response to this problem is to write some of them down or to use the same one across a number of different services, both of which have inherent security risks (Adams & Sasse, 2005; Dhamija & Perrig, 2000; Gaw & Felten, 2006). In one study (Dhamija & Perrig, 2000), for example, it was found that participants had ranging from ten to fifty situations where passwords were required, but in practice used one to seven repeatedly. Users have also been shown to choose passwords and PINs that are easy to remember, and are therefore high risk (Adams & Sasse, 2005; Bishop, 2005; Yan, Blackwell, Anderson, & Grant, 2004).

Alternative and/or additional security measures are therefore increasingly being sought, particularly in the banking sector where remote fraud is on the increase (Hiltgen, Kramp, & Weigold, 2006). One possibility is 'two-factor' authentication using physical tokens such as card-readers ("what you have") in addition to memorised information. Here, any fraud depends on both knowing the secret informa-