Usability Study of Fingerprint and Palmvein Biometric Technologies at the ATM

Gareth Peevers, Centre for Communication Interface Research, School of Engineering, The University of Edinburgh, Edinburgh, UK
Richard Williams, Zone, London, UK
Gary Douglas, Centre for Communication Interface Research, School of Engineering, The University of Edinburgh, Edinburgh, UK
Mervyn A. Jack, Centre for Communication Interface Research, School of Engineering, The University of Edinburgh, Edinburgh, UK

ABSTRACT

The usability of four biometric ATM designs were assessed in comparison to an existing ATM. Participants (N=46) were observed using two biometric technologies (palmvein and fingerprint) at two positions (horizontal and vertical) on the ATM in a repeated measures design. Measures included a usability attitude questionnaire, a quality metric and data from interviews and observation. Usability scores for the ATMs with biometric sensors were comparable to scores for the existing ATM even though they added an extra step to the typical ATM process. No differences were found in usability scores between palmvein and fingerprint sensors on the ATMs, or for the different positions. The quality results were more emphatic with a definite preference for horizontal positioning of sensors on the ATM, which corresponded with observations and participant comments. The horizontally-mounted fingerprint sensor was rated significantly higher in comparison to the existing ATM. Participant preference also favoured the fingerprint sensor over the palmvein sensor. It is argued that the quality metric results picked up on issues of security, whereas the usability results did not. There was a clear divide in the rankings of the existing ATM with equal scores ranking it first and last. Nearly 20% of the participants said they would not register to use biometric technologies. It is not clear how much of this is due to usability issues or underlying negative attitudes towards biometrics. Observations and comments from the participants point to the importance of improving user feedback in future designs.

Keywords: Automatic Teller Machines (ATM), Biometric Technologies, Fingerprint, Palmvein, Self Service Banking

DOI: 10.4018/jthi.2013010106
1. INTRODUCTION

Biometric technologies are becoming of increasing interest in many aspects of modern life. It is now not uncommon to encounter fingerprint sensors in High Street stores, in bars and even in schools [BBC News, 2007]. The biometrics technology industry understandably sees the financial services sector as a key market for the technologies [Coventry, 2004, Most, 2004], with its continued push to use of self-service banking channels, such as the Internet, interactive voice response (IVR) telephone banking, mobile phone banking and automated teller machines (ATM). With self-service channels there can be security and customer authentication concerns that the use of biometric technologies could address.

This paper is concerned with biometric technologies at the ATM. Countries such as Chile, Columbia, Japan, Pakistan and Poland already use ATMs equipped with biometric technology. Recent figures show that ATM fraud losses (counterfeit card fraud) in UK amounted to some £81 million in 2009-10 (The UK Cards Association, 2010), a drop of 52% from 2008-9 figures while, annual ATM losses in Europe were approaching 500 million Euros (www.scmagazineuk.com, 2009), data which include a rise of 149% in attacks on ATMs. One solution to this fraud problem is to add another level of security at the ATM by including biometric technology. There are a number of different biometric technologies that can be employed on ATMs, and it is known that usability and user experience issues can affect biometric technology performance (Fernandez-Saavedra, 2010), and that user acceptance could affect the performance and the success of implementation. The relationship between these factors has been found to be complex (Fernandez-Saavedra, 2010; Riley et al., 2007), but it is argued (Coventry, 2004) that the user experience aspect is central to the successful deployment of biometric technologies. The goal of the research presented here was to compare and contrast customer attitudes to usability in deployment of fingerprint and palmvein technologies on ATMs, and to contribute to the better understanding of the issues surrounding the implementation of biometrics from a user experience perspective - the importance of considering the end user of a biometric system has been stressed by earlier research (Ashbourn 2000; Chandra & Calderon, 2005; Langenderfer & Linnhoff, 2005).

1.1. Context for Research

This research was carried out with customers of one of the UK’s leading High Street banks. The purpose was to investigate the impact on user experience and usability from introduction of 3-factor authentication at the ATM by using biometric technology to extend the existing 2-factor approach based on card plus PIN security. Such 2-Factor authentication is based on using two complementary sources of information to verify the customer’s identity – one of the two factors normally being a piece of secret information, a PIN (‘what you know’), and the other being a physical token, a debit or credit card (‘what you have’). The weaknesses with this type of security method are that typically, today’s customers will have multiple accounts / cards / PIN which makes it more difficult for them to remember each (or worse from a fraud viewpoint, they have the same PIN for every card). As a result, when customers are allowed to define their own PIN they tend to select numbers that are easy for them to remember and these are often therefore based on information from their everyday life – rendering them easier to predict (Gong et al., 1993). All of these issues result in a trade-off between security and usability (Adams & Chang, 1993; Adams & Sasse, 1999).

Card theft at the ATM occurs in a variety of ways (ENISA, 2009). The simplest is where the criminals (ATM crime is normally a team activity) acquire the PIN number by eavesdropping at the ATM as the customer enters the PIN digits on the keypad (‘shoulder surfing’) and then acquire the card itself by theft/mugging: often using it immediately at nearby ATMs to steal funds from the victim’s account before the crime can be reported. A variant of this
Internet-Mediated Communication at the Cultural Interface

www.igi-global.com/chapter/internet-mediated-communication-cultural-interface/13148?camid=4v1a