Interacting with Computers 22 (2010) 153–164

Contents lists available at ScienceDirect

Interacting with Computers

journal homepage: www.elsevier.com/locate/intcom

Usable security: User preferences for authentication methods in eBanking and the effects of experience

Catherine S. Weir [a,*], Gary Douglas [a], Tim Richardson [b], Mervyn Jack [a]

[a] CCIR, The Centre for Communication Interface Research, School of Engineering, The University of Edinburgh, The King's Buildings, EH9 3JL, United Kingdom
[b] Lloyds TSB Bank plc., 25 Gresham Street, London, United Kingdom

ARTICLE INFO

Article history:
Received 16 February 2009
Received in revised form 31 August 2009
Accepted 16 October 2009
Available online 31 October 2009

Keywords:
Usability engineering
Internet banking
Authentication
Usable security
Empirical evaluation
Experience

ABSTRACT

Multi-factor authentication involves the use of more than one mode in authentication processes and is typically employed to increase security compared to a fixed password (knowledge-based mode). This research compared three different eBanking authentication processes, a two-layer password (1-factor) method and two alternative 2-factor solutions. The 2-factor processes used One-Time-Passcodes (OTPs) delivered either via a small, single-use device or by text message to a mobile phone. The three authentication methods were compared in a repeated-measures experiment with 141 participants. Three user groups were balanced in the experiment to investigate the effect of experience (current users of the service) on perceptions of usability and security. Attitudes toward usability and observations were taken for each process. Other data gathered quality ratings, preferences and ranked comparisons regarding convenience and security issues. Both 2-factor methods scored significantly higher than the 1-factor method for eBanking authentication usability metrics overall, but experienced users gave higher scores to the 1-factor method they currently use. Overall preferences were spread evenly between the three methods. However, the majority of the participant sample perceived the 1-factor method they had most experience with as being the most secure and most convenient option. The results offer insight into customer attitudes important in their selection of authentication options: convenience, personal ownership and habitual experience of processes.

1. Introduction

This paper describes an experiment designed to investigate perceived usability for alternative authentication processes for logging onto eBanking services. The experiment aimed to inform the design of usable security technology for 2-factor authentication in eBanking in order to maximise customer acceptance and adoption. The usability methodology was based on previous work in eBanking interface usability (Weir et al., 2006, 2007) and in usable security (Weir et al., 2009). Measurements of usability included questions examining the user's security perceptions in detail. The experiment also investigated how previous experience of eBanking authentication effected user attitudes towards the processes.

eBanking services provide convenience for customers performing routine transactions (Centeno, 2004), however, online access also poses security issues (Schneier, 2004). Phishing and other fraud are escalating as more consumers chose the Internet channel for banking and commercial applications (Hole et al., 2006; Nilsson et al., 2005). Actual use of online services is influenced by security and trust perceptions (Furnell, 2007; Hertzum et al., 2004). Thus, providing an appropriate balance between perceptions of convenience and security is a current concern for the industry (Hiltgen et al., 2006). By evaluating the usability of eBanking authentication processes, methods can be designed that are easy to use, providing both convenience and adequate security (Weir et al., 2009). Such studies are essential to provide data to ensure eBanking and similar eCommerce activities are equipped for future growth.

1.1. Authentication approaches and limitations

Passwords are the most prevalent form of authentication, but are only one of many technological methods available to secure systems from unauthorised access. Three modalities are typically considered in an authentication model (Renaud, 2005; O'Gorman, 2003):

- Knowledge-based, some security token which is secret to the customer (e.g. password).
- Object-based, some device assigned uniquely to an individual (e.g. bank card).
- Biometric-based, some intrinsic properties of an individual (e.g. fingerprint).

* Corresponding author.
E-mail address: cath.weir@gmail.com (C.S. Weir).

0953-5438/$ - see front matter © 2009 Elsevier B.V. All rights reserved.
doi:10.1016/j.intcom.2009.10.001

Passwords provide "security at minimal inconvenience" (Morris and Thompson, 1979), offering adequate and inexpensive security in the early days of non-networked computers (Tognazzini, 2005). However, there are numerous limitations to the password approach. Forgotten passwords are perhaps the most obvious problem, causing frustration and delay for customers. A typical Internet user today has multiple passwords to memorise and recall on demand. This memory burden leads to types of behaviour that can compromise security, e.g., writing passwords down or frequently reusing them to alleviate memory limitations (Gaw and Felten, 2006; Halderman et al., 2005; Ives et al., 2004; Sasse et al., 2001; Barton and Barton, 1984). Forgotten passwords also result in lost sales, lost customers, increased helpdesk calls and administration costs for business (Brown et al., 2004).

With the boom of eCommerce there has been a steady rise in card-not-present (CNP) transactions. Reliable authentication of these transactions has been an obstacle to security and building customer trust online (Furnell, 2005). The widespread use of password authentication has caused fraud problems for the eBanking and eCommerce industry (Sinclair and Smith, 2005). There are an increasing range of potential threats in banking and commerce online (Henry, 2006; Furnell, 2005). Attackers have made good use of human factors to exploit users, e.g. social engineering methods which trick users into divulging their passwords (Sasse and Flechais, 2005). Phishing, spoofed interfaces and keystroke capture software (Sinclair and Smith, 2005; Ives et al., 2004) are other common methods of collecting authentication tokens such as passwords. When passwords are compromised in this way, the practice of password reuse across different websites and services further undermines security. Thus, an authentication solution both secure and appropriate for widespread customer use is badly needed (Furnell, 2005; Sinclair and Smith, 2005).

The use of a single mode (single-factor) in authentication, particularly in the era of advanced computing and eCommerce, is proving insufficiently secure. Multi-factor authentication, the use of more than one type of authentication approach, has been recommended by the security industry (Viega, 2005). In this model, each modality makes up for deficiencies in the other (Renaud, 2005). Two-factor (2-factor) authentication makes use of two such components. The Automatic Teller Machine (ATM) has always made use of 2-factor authentication, via a bankcard (object) and a secret (knowledge) Personal Identification Number (PIN). The component of physical presence and use of the bankcard allows for a somewhat weaker PIN. This approach has also been rolled out to authenticate card transactions on the high street using chip and PIN instead of relying on signatures. The added security level compared to signatures has seen a reduction in fraud in the industry (BBC News, 2007).

eBanking services worldwide are moving towards the implementation of 2-factor authentication solutions (Beaumier, 2006; Hiltgen et al., 2006). In the UK, several Banks are considering, piloting or have rolled out the use of security tokens in an effort to enhance security (e.g. Jones, 2006). European banks have a long tradition of using single use transaction numbers provided on small scratch cards (sent with monthly statements), these have proved successful (Hiltgen et al., 2006; Reavley, 2005). Modern digital token generators create these dynamic passcodes (One-Time-Passcode or OTP) automatically. Although these devices alleviate the memory problems of multiple passwords and are small (therefore easy to carry), they do not always extend to multiple uses. It is easy to see a situation where different tokens of this type would be required for various websites and other services. Everyday use of tokens in authentication would require possession of the device when needed, and the ability to use it. Token solutions also involve cost in rollout and support (Claessens et al., 2002). Solutions which involve one hardware device working for multiple applications might offer more convenience. Mobile phones are often proposed, due to their popularity and the relative speed which they are noticed as lost or stolen compared to bank cards (Brunswick, 2009; Dragoljub, 2007).

Although eBanking services are moving from the use of single, fixed passwords to alternative authentication approaches, expert evaluations of the usability of the array of alternative processes (e.g. Furnell, 2007; Braz and Robert, 2006) note that security vulnerabilities are still apparent on both widely used and new technologies. Security technologies are also constantly evolving in order to meet and prevent new threats (Schneier, 2005). This changing landscape increases the need for user study of security processes.

1.2. Usable security

Security is not the main goal of a user's interaction with a computer system. In the banking context, most users are prepared to tolerate some security procedure, e.g. authentication with signatures or PINs is typical of any banking task or financial transaction, on any channel. But in designing security procedures, usability issues are often overlooked in the desire to provide a technologically secure solution (Tognazzini, 2005) ignoring the human factor (Adams and Sasse, 1999). Although service providers should set appropriate levels of security, they must also consider the users' willingness to adopt procedures (Weirich and Sasse, 2001; Schultz et al., 2001). Typically, a compromise is found which balances actual security levels with user and usage perspectives. If security levels are perceived to be unwieldy, users will workaround them and compromise security or avoid use (DeWitt and Kuljis, 2006; Besnard and Arief, 2004). In an eBanking context, this could reduce adoption and the associated cost-savings of providing the service.

Perceptions of security have been suggested to relate to a range of factors including convenience, intrusion, control and clarity (Bishop, 2005; Long and Moskowitz, 2005; Nodder, 2005; Renaud, 2005; Tognazzini, 2005). The convenience of a process would particularly be expected to influence actual usage (Halderman et al., 2005; Hertzum et al., 2004). Perceived convenience rather than security has been found to be a main motivator for eBanking adoption (Lichtenstein and Williamson, 2006). Biometric authentication research, based on both market research and empirical techniques has also found speed and convenience to be the key benefits of these methods (Coventry et al., 2003).

Most authentication research has been done for knowledge-based methods with many empirical studies of password strength, guessability and memorability (e.g. Yan et al., 2005; Zviran and Haga, 1999). Additionally alternative knowledge–based mechanisms such as cognitive and associative passwords have also been studied (e.g. Zviran and Haga, 1990). Usability principles for security technologies have also been published (Smetters and Grinter, 2002), and a raft of guidelines to help designers focus on providing usable security (Berson, 2005; Johnston et al., 2003; Barton and Barton, 1984).

Some user-studies of experiences with security token devices in eBanking have been published: user preference for alternative authentication tokens followed usability and convenience ratings rather than the increased level of security in a recent study of three types of secured and unsecured OTP generators (Weir et al., 2009).

Other studies have concentrated on the level of security provided by authentication, with studies of transaction confirmation and OTP delivery, simulating a text message approach (AlZomai et al., 2008): attacks on the transaction details went unnoticed in 21% of cases (734 transactions performed by 92 participants). One-digit changes in receiving bank account numbers were overlooked more frequently than the more obvious four-digit attacks.