International Journal of Information Management 32 (2012) 489–494

Contents lists available at SciVerse ScienceDirect

International Journal of Information Management

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

Case study

Evaluating biometrics for online banking: The case for usability

Rana Tassabehji[a,*], Mumtaz A. Kamala[b]

[a] University of Bradford School of Management, Emm Lane, Bradford BD9 4JL, United Kingdom
[b] University of Bradford School of Computing, Informatics and Media, Horton Building, Bradford, BD7 1DP, West Yorkshire, United Kingdom

ARTICLE INFO

Article history:
Available online 31 July 2012

Keywords:
Biometrics
E-banking
Biometric banking (b-banking)
System Usability Scale (SUS)

ABSTRACT

Rising cyber-crimes have heightened existing concerns about e-banking security. However currently the use of biometric technology in the banking sector is not prevalent. We developed a biometric system for authenticating e-banking and applied the established System Usability Scale (SUS) to evaluate its effectiveness from the perspective of potential users. The case demonstrates that on the whole users are very favourable towards a biometric banking system and ostensibly found the system developed usable. We found that when evaluating the biometric system, its different components needed to be considered – namely the biometric technology and the institutional process that supports verification and authentication.

1. Introduction

With e-commerce becoming the de facto standard for conducting business in the second decade of the 21st century, online banking services offered by banking institutions have also grown exponentially. E-banking plays a central and important role in the rapid and continued growth of e-business and e-services, providing a platform for supporting e-commerce applications and other e-services. As banks have recognised the operational benefits of online banking, they have realised cost savings, increased efficiency and customer benefits in terms of convenience, functionality, speed and 24/7 availability. E-banking is now considered to be a standard requirement. In the UK, there is an estimated 25 million Internet banking users (Hyde, 2012) making approximately 70% of the online population and estimated to grow further over the next five years through other media such as mobile devices. Despite this growing ubiquity of online banking services, security and privacy concerns and fears are still foremost in the minds of users and are indeed well founded. More than half of all UK bank card fraud from 2003 to 2008 was carried out online through “card-not-present attacks”, an increase of 118%, which is predicted to increase further as online banking and online shopping becomes more prevalent. According to the UK Payments Council (2012), online banking fraud in the UK was estimated to be over £35 million for the period 2010–2011 but criminal hackers are remaining one step ahead of banks finding new and ever ingenious ways of getting around the latest generation of online banking security devices given out by banks (Kelly, 2012).

Investment in the development of e-banking systems worldwide is substantial and it is of paramount importance that online systems remain secure as the survival of e-banking is dependent on the bank’s trustworthy reputation and ability to convince customers their services and assets are protected. As with all online transactions, there are risks in e-banking including security of transactions, financial loss due to personal or bank error and loss of time in using the system and rectifying errors. Banks therefore need to ensure they understand their customers and respond to developments in digital technology in a way that incorporates their customers’ requirements and addresses their concerns. Consequently, banks need to develop risk-reducing strategies to inspire greater confidence in their e-services. Current e-banking has been found to be a less verifiable and controllable environment especially, for instance, when asking for compensation when transaction errors occur (Lee, 2009). It is proposed that use of biometric banking will improve this problem.

1.1. Biometrics

While theoretically a powerful tool, commonly used PINs and passwords for e-banking authentication are in practice, a cognitive burden for users who have to remember multiple passwords and PINs which often leads to security risks where users choose memorable words or dates of birth, use the same password and often ignore advice for creating a secure password (Gunson, Marshall, McInnes, & Jack, 2011). A secure, functional and effective alternative is the use of biometrics to verify and authenticate a user remotely. Biometrics, described as “the science of recognising an individual based on his or her physical or behavioral traits” (Jain, Ross, & Pankanti, 2006), range from the use of physical features including voiceprints, fingerprints and iris recognition, to

[*] Corresponding author. Tel.: +44 01274233902.
E-mail address: r.tassabehji@bradford.ac.uk (R. Tassabehji).

0268-4012/$ – see front matter © 2012 Elsevier Ltd. All rights reserved.
http://dx.doi.org/10.1016/j.ijinfomgt.2012.07.001

behavioural features including gait and handwriting recognition. Biometrics are inherently difficult to copy, share and distribute; difficult to forge; cannot be lost or forgotten because the individual has to be physically present. As such, biometric systems are considered more reliable than the established password based authentication systems and are the logical and arguably inevitable future of secure authentication.

Despite this, widespread implementation remains limited and research in Europe and the USA has identified the importance of understanding usability and accessibility criteria as critical to addressing this limited expansion of biometrics in different commercial application environments (Gunson et al., 2011). Although not yet commonplace, biometrics themselves have reached a certain level of maturity, where developments in biometric sensors (smaller, cheaper, more ergonomic) means they are increasingly found in IT devices such as PCs, PDAs and flash drives and are being applied in contexts driven by government initiatives such as air travel and immigration/border control.

Studies have already shown that usability and acceptance of e-services secured by biometric technology are affected by the context of use and application environments (Byun and Byun, in press). However, biometrics research within different contexts is still in its infancy and while biometrics offer a wide range of opportunities they are currently mainly driven by government initiatives centred on border control applications and national ID programmes. In one widely reported instance, the Iris Recognition Immigration System costing over £9 million, introduced in the UK to speed up airport passport control processing queues, failed to deliver on efficiency improvements and led to the "quiet" scrapping of the whole system in February 2012. Biometric technology has already been identified as potentially playing a major role in protecting banking assets and safeguarding the e-banking environment (Venkatraman & Delpachitra, 2008). Biometric ATMs have already been successfully implemented and widely used around the world. However the lacklustre uptake of biometrics in banking ATMs, in Western Europe in particular, has been attributed to a dearth of commercial incentive. But as more of our everyday devices are linked to biometrics – for instance voice recognition on mobile devices (e.g. iPhone's SIRI), fingerprint recognition on laptops and flash drives, face recognition on smartphones – customers will increasingly demand such devices to enhance security of their bank accounts which are currently reliant on easily cracked passwords and "clunky three-factor authentications with a one-time password generator" (Skinner, 2012).

Since biometric technology can effectively address security concerns in e-banking, both technically and behaviourally, the proposed solution was developed to demonstrate operational features of biometric-banking to potential users to gauge their response to it by using Brooke's (1996) modified System Usability Scale (SUS). SUS was developed as part of the usability engineering programme in integrated office systems development at Digital Equipment Co. Ltd., Reading, United Kingdom and this case study is to evaluate its application to the biometric interface to online banking discussed in more detail.

2. The proposed biometric banking system

To date, there has been no commercialised development of biometric banking services. The biometric banking system proposed here, was developed and based on the use of biometric fingerprint recognition hardware and software used to authenticate each individual user based on public/private key encryption protocols. In a test of different biometric technologies, fingerprint, voice and signature verification, users found fingerprint biometrics to be most easy to use and was considered the most secure of the modalities and was most preferred of the three. Interestingly, fingerprint biometrics were found by users to have the most impact on privacy, and evoked a higher degree of confidence than voice or signature recognition. (Toledano, Pozo, Trapote, & Gomez, 2006). Thus fingerprint recognition biometrics are used in this system.

Banks traditionally play a critical role in securing financial transactions through provision of technical infrastructures such as encryption, authentication and firewalls, which impact consumer trust in the institutions' technology. Consequently, we include the bank in the process of authentication in the biometric banking system and expect this to impact user trust and improve the system.

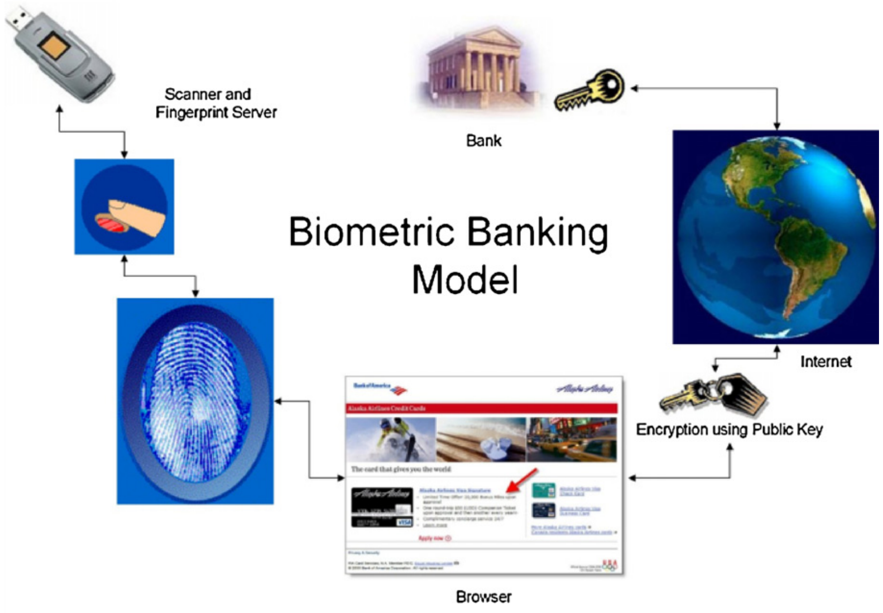
Figs. 1 and 2 illustrate the schematics of the b-banking system and the control method respectively. Users would first physically visit the bank to register their fingerprints in a secure manner. A fingerprint reading device would be provided to the user with their user's unique fingerprint information and embedded secured password. To access their bank online, they would insert the device in a PC USB port and place their finger on the scanning device to authenticate themselves. Once authentication is established, the device will launch a web browser on the PC that cannot accept any Uniform Resource Locator (URL) input. Using a browser that cannot accept URLs will prevent any potential tampering with web addresses that may redirect the Internet connection to a different address. The key that is securely stored on the device will then establish a secured connection with the correct bank (using a built-in URL belonging to the bank). The key will logon the authenticated user. Users can freely access their accounts until the users log out. If the wrong fingerprint is used a number of times determined by the bank, then the key will lock itself and users will need to go back to the bank for re-validation.

The benefits of using this approach include (a) less data vulnerability: as there is no communication with the PC before the user is authenticated, (b) improved data security: upon user identification, there will be no access to usernames and passwords, (c) ease of access: no input from the user is needed apart from their fingerprint, (d) limited virus/malware damage: the browser is stored in the hardware with no write access to it thus viruses, worms, etc. cannot be injected, and (e) reduced phishing impact: because no user data input is needed, harvesting information becomes ineffective.

Technologically this concept can and has been proven by providing the hardware and simulating the software to test it. However no system can ever be used in isolation of human beings and thus in order to understand whether users will find this a viable solution, further user testing was conducted to assess their perceptions of the device's usability. Brooke's (1996), System Usability Scale (SUS) which was developed as part of the usability engineering programme in integrated office systems development at Digital Equipment Co. Ltd., Reading, United Kingdom, will be applied in this case study and is discussed in more detail in the following section.

3. Evaluating the biometric banking system

The System Usability Scale (SUS) is considered to be an inexpensive, yet effective tool for assessing the usability of a whole range of products and systems, including web sites, cell phones, interactive voice response systems, TV applications, and others. It is commonly employed by usability professionals and reported to provide an easy-to-understand score (0–100) based on a ten statement questionnaire, each having a five-point scale ranging from Strongly Disagree to Strongly Agree, which makes it relatively quick and easy to administer and score. One of the criticisms of the System Usability Scale is that the numeric score is not an absolute and is sometimes difficult to interpret qualitatively. For instance, is an SUS score of 50 sufficient or is 75 or 100 required? We include an



Disclaimer: Above Images are downloaded from different web sites for demonstration purposes (Accessed on 28/11/2007)

Fig. 1. Schematic diagram of proposed biometric banking cycle.

additional adjective rating scale to help interpret the SUS scores and provide a qualitative dimension to the results.

The proposed biometric banking system was piloted with a group of 116 people. The groups were based in the UK with a mix of male (58%) and female (42%) participants across the two broad age groupings split into the under 25's (54%) and 25 or over (46%).

3.1. The biometric banking prototype: System Usability Scale

The usability questionnaire applied to the respondents was based on the original Brooke, questionnaire with a slight modification made by Bangor, Kortum, and Miller (2008) who suggested a change in the "cumbersome" to "awkward" as being more current and was used in this case. We did not however follow their use of the term "product" and retained the original "system" when referring to the biometric banking system under examination.

The value of the SUS is in the single reference score collated from the 10 questions eliciting participants' opinions on the system's usability. The sole use of this single composite score is recommended by the SUS creator, as the individual statements are considered to be irrelevant and secondary to the calculated individual score. However, in practice, practitioners tend to highlight individual statements to gain more detailed information (Bangor et al., 2008) which is against the intended objectives of the scale and Brooke specifically states that "scores for individual items are not meaningful on their own" (1996: 5).

A strong positive correlation was found between all 10 statements and the consistency of the scale was also found to be very

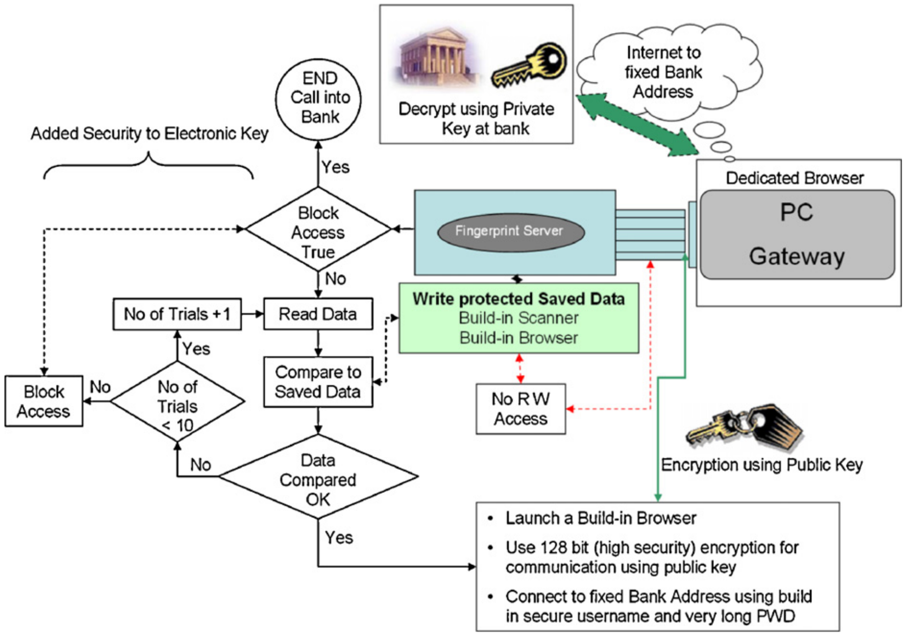
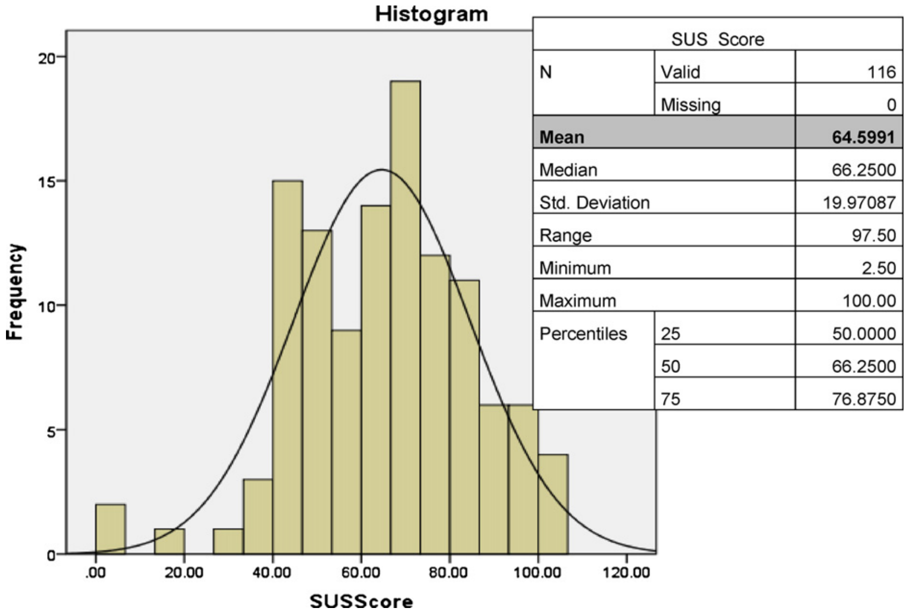

END Call into Bank
Decrypt using Private Key at bank
Internet to fixed Bank Address
Added Security to Electronic Key
Yes
Block Access True
No
Fingerprint Server
Dedicated Browser
PC
Gateway
No of Trials +1
Read Data
Write protected Saved Data
Build-in Scanner
Build-in Browser
Yes
Block Access
No
No of Trials < 10
Compare to Saved Data
No R W Access
No
Data Compared OK
Yes
Encryption using Public Key
Launch a Build-in Browser
Use 128 bit (high security) encryption for communication using public key
Connect to fixed Bank Address using build in secure username and very long PWD

Fig. 2. Proposed control method.



SUS Score		
N	Valid	116
	Missing	0
Mean		**64.5991**
Median		66.2500
Std. Deviation		19.97087
Range		97.50
Minimum		2.50
Maximum		100.00
Percentiles	25	50.0000
	50	66.2500
	75	76.8750

Fig. 3. Histogram of SUS scores and corresponding mean SUS score.

good/excellent ($\alpha = 0.89$). Having established that the instrument was reliable and consistent, the SUS scores were calculated according to Brooke's instructions: "To calculate the SUS score, first sum the score contributions from each item. Each item's score contribution will range from 0 to 4. For items 1, 3, 5, 7, and 9 the score contribution is the scale position minus 1. For items 2, 4, 6, 8 and 10, the contribution is 5 minus the scale position. Multiply the sum of the scores by 2.5 to obtain the overall value of SU." (1996:6).

The SUS yields a single number representing a composite measure of the overall usability of the system being studied for each of the statements and the mean is thus calculated. In this case, the Standard Usability Score for the biometric system is 64.599 (Fig. 3).

With no prior benchmark it is difficult to interpret an SUS score of 65 – does this mean the system is usable or not? Bangor et al. (2008) have compiled data from 2324 SUS surveys and have found that the average score for these studies is 69.69 with a standard deviation of 18 and range from 30 to 93.93 which is relatively consistent with our study.

Having obtained the SUS core, there remain some problems in terms of understanding qualitatively what these scores might mean. While the benchmarking from previous studies might be useful, the different systems and contexts do not necessarily provide an accurate assessment of this single figure. Bangor et al. (2008) recommend the introduction of an *adjective rating* which qualitatively describes the usability of the system. In this study, we adopt an adjective rating scale to add a qualitative aspect to the SUS score.

With this additional adjective rating scale, it becomes possible to correlate this with the SUS score to get a more qualitative understanding of the System Usability Scale score. In this instance, from Fig. 4, we can see that SUS scores over 80 would be considered to the best imaginable system, SUS scores of 70–80 would be considered Excellent, SUS scores of 65–70 would be considered good, SUS scores 60–65 would be considered OK, SUS scores 55–60 would be considered poor, SUS scores 45–55 would be considered awful and those 45 or below are considered worst Imaginable. Although this is purely a qualitatively notional scale it is very useful for contextualising the SUS score for the biometric banking system developed in this case study.

To ensure that the inference being made above is not purely conjecture and is based on a sound relationship between the SUS score and the adjective scale, we conducted a correlation test and found that the Pearson product-moment correlation coefficient was $r = 0.601$, $p < 0.001$ (2-tailed), which is considered a strong correlation and validates our interpretation. From these results, we were able to judge the usability of the system.

3.2. The biometric banking prototype: evaluation of the process

Questions relating to the role of the banks in the authentication and verification process were posed to the respondents. Two thirds were prepared to visit the bank for the initial set up of biometrics information in the first instance (67%) and believed the bank was crucial for the verification process (65%) in the first stages. Thus, the institutional role of banks in the initial authentication stage appeared to be important in the process of setting up biometric banking. However those that were reluctant were afraid that:

> *"Authentication with the bank will take a longer time"*
>
> *The bank should not keep a copy of my biometric information, this should be made clear to the customer.*
>
> *this technology gives the government and banks too much power to abuse it! In the future the abuse could be potentially detrimental"*,
>
> *"sounds interesting, but the idea of an organisation holding the biometric details of people is scary, considering the amount of confidential information which has been lost of recent"*

When asked whether participants would be prepared to return to the bank for re-verification and re-authentication, only 44% were prepared to do this. Thus, there issues about the set up and verification process that needs some further development, including storage of biometric information, time taken for authentication at the bank and more information to users.

3.3. The biometric banking prototype: evaluation of the biometric technology

When asked about the biometric technology specifically, the majority of respondents did not have much everyday practical familiarity with biometric technologies, those that did had encountered them either on their electronic devices (computers, mobile

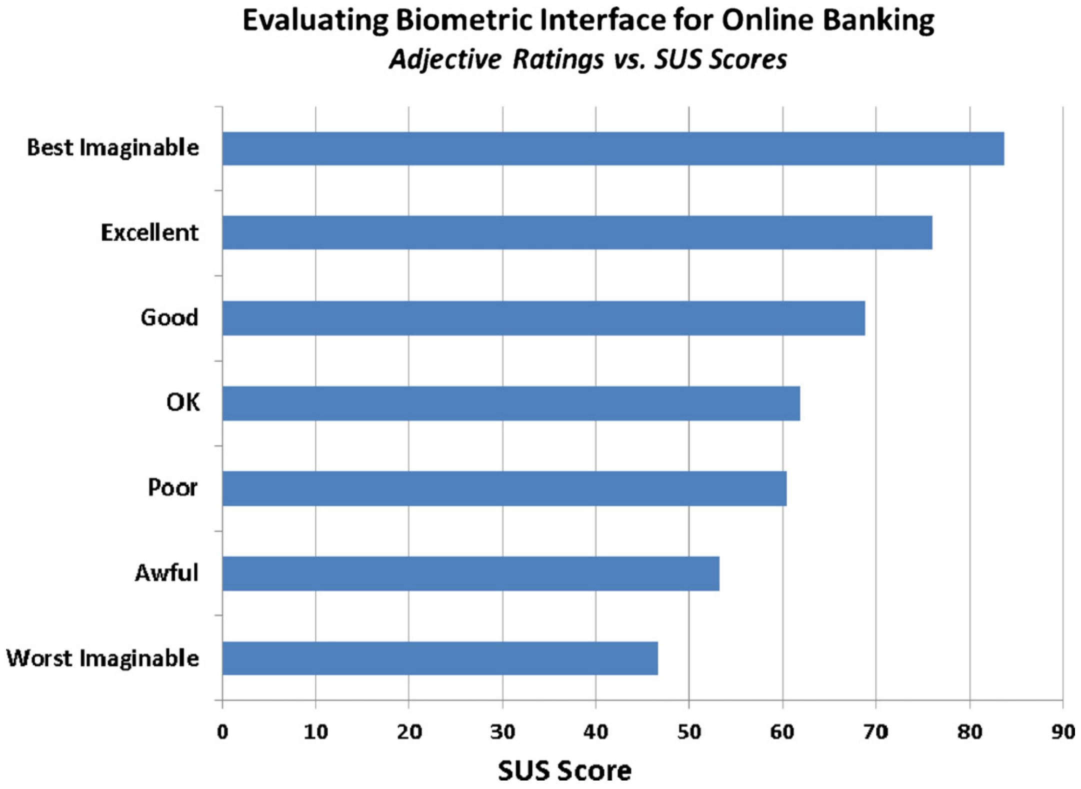


Fig. 4. Adjective rating vs. SUS scores for biometric banking.

devices, flash drives) and this was mainly fingerprint scanners, voice recognition or facial recognition used to access their devices but were not linked to any institutional infrastructures or services and were limited to individual devices. Where biometrics had been encountered on an institutional level, these were mainly through immigration control at airports but were mainly fingerprint and iris/retina scanning. When asked about the suitability of different devices for online use in this instance, fingerprint scanning was considered to be most suitable. Fig. 5 illustrates the difference between actual familiarity with different biometric devices and the biometric interfaces that respondents felt were appropriate for online use. In both instances, fingerprint scanning was most popular.

From this we can infer that the choice of biometric technology is not a major problem and thus the interface with the biometrics technology and the processes need to be reviewed for further development. We also allowed participants the opportunity to make comments on the biometric banking system to provide further qualitative feedback.

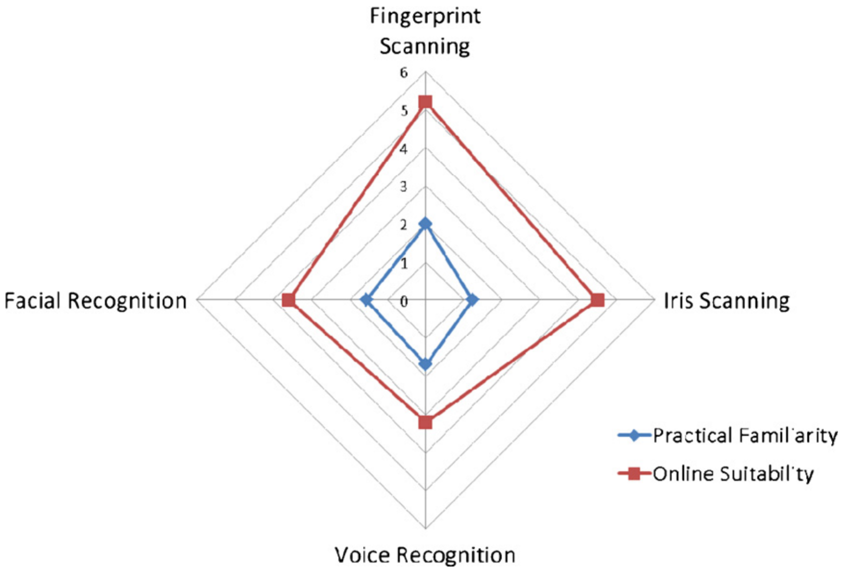


Fig. 5. User experience of biometrics.

4. Case study – lessons learned

In the context of the biometric banking system used here, the System Usability Scale was found to be very simple, cost effective and easy to apply. The analytical process presented in this case study is relatively easy to replicate and provides a good level of rigour. This makes the SUS scale a very good tool to use to evaluate usability of a system.

This measure can also be used to evaluate differences between groups (male and female, age groups). In this instance we tested for differences in the SUS score between these 2 groups and found no major differences between age groups, but a small difference in SUS scores between males and females which again provides additional information and routes for further investigation of usability between groups.

However, the results from the SUS if taken in isolation are limited and more information was needed to supplement the Usability score. The overall usability score of 64.59 appeared to be above average, however when a qualitative adjective rating is applied, this suggests that the usability is “OK” – and that in fact this usability score suggests much more work is needed on the system. In order to further benefit from the SUS tool, SUS scores need to be collated so that they can be benchmarked against other similar studies. In this instance we have presented the case for a biometric banking system using a fingerprint device. The SUS score and adjective rating suggests that the system developed needs many more iterations in the development process to improve usability.

While the SUS provides information on usability, it does not specify how this can be improved or where the problems in the system arise. Further in-depth information is needed to supplement the SUS score in order to evaluate how usability can be improved. In this instance, although the role of banks in the biometric authentication process was found to be important, users found problems with the process which needs to be addressed and streamlined. They also raised issues about the fingerprint capture device itself which also needs attention, for instance, it could be that the device is too small/big for male and female users. On the whole though, the selection of the biometric technology (fingerprint recognition) for this process was unanimously approved.

5. Conclusion

The major findings of this case study have been twofold. Firstly we have introduced an as yet untested and unimplemented biometric interface to the process of online banking. Using this as the context of our study, we wanted to evaluate its usability in the early stages of development to minimise wastage of time and resources on a system that was not usable. We applied Brooke’s “quick and dirty usability scale” (SUS) to achieve this aim. The findings show that in this new context, the SUS was effective and informative and although it had its limitations, which once understood, could provide a very simple, easy and cost effective way of evaluating new systems. The implications of this case study for managers is that the SUS is only one, albeit very effective, tool in an armoury of usability development and management tools, which yields very useful information but can and must be supplemented by more information.

This case study provides further practical implications for mangers and decision makers in the retail online banking sector (specifically), demonstrating that overall, users have a favourable attitude to our biometric banking system, and that this has much potential to be developed into a commercially successful and secure system.

References

Bangor, A., Kortum, P. T., & Miller, J. T. (2008). An empirical evaluation of the system usability scale. *International Journal of Human-Computer Interaction*, *24*(6), 574–594.

Brooke, J. (1996). SUS: A “quick and dirty” usability scale. In P. W. Jordan, B. Thomas, B. A. Weerdmeester, & A. L. McClelland (Eds.), *Usability evaluation in industry*. London: Taylor and Francis. Available from http://www.usabilitynet.org/trump/documents/Suschapt.doc (accessed 20.5.2010)

Byun, S., & Byun, S.-E. Exploring perceptions toward biometric technology in service encounters: A comparison of current users and potential adopters. *Behaviour & Information Technology*, in press. Available online: 30 March 2011.

Gunson, N., Marshall, D., McInnes, F., & Jack, M. (2011). Usability evaluation of voiceprint authentication in automated telephone banking: Sentences versus digits. *Interacting with Computers*, *23*(1), 57–69.

Hyde, D. (2012, February 6). *Hackers crack new online banking security putting 25 m people at risk*. Available from http://www.thisismoney.co.uk/money/saving/article-2096060/Hackers-crack-new-online-banking-security-putting-25m-people-risk.html (accessed 10.6.2012)

Jain, A. K., Ross, A., & Pankanti, S. (2006). Biometrics: A tool for information security. *IEEE Trans. Information Forensics and Security*, *1*(2), 125–143.

Kelly, S. (2012, February 10). *Hackers outwit online banking identity security systems*. (accessed 10.6.2012). http://www.bbc.co.uk/news/technology-16812064

Lee, M. (2009). Factors influencing the adoption of Internet banking: An integration of TAM and TPB with perceived risk and perceived benefit. *Electronic Commerce Research and Applications*, *8*, 130–141.

Skinner, C. (2012). *Who the hell needs biometrics in banking? Financial services club Blog*. (26.1.2012). http://thefinanser.co.uk/fsclub/2012/01/who-the-hell-needs-biometrics-in-banking.html

Toledano, D. T., Pozo, R. F., Trapote, A. H., & Gomez, L. H. (2006). Usability evaluation of multi-modal biometric verification systems. *Interacting with Computers*, *18*, 1101–1122.

UK Payments Council. (2012, March 7). *Credit card fraud falls to a 10-year low*. Telegraph online (accessed 10.6.2012). http://www.telegraph.co.uk/finance/personalfinance/borrowing/creditcards/9127605/Credit-card-fraud-falls-to-a-10-year-low.html

Venkatraman, S., & Delpachitra, I. (2008). Biometrics in banking security: A case study. *Information Management & Computer Security*, *16*(4), 415–430.

Rana Tassabehji is a Senior Lecturer in E-business and Information Systems. Her teaching and research interests focus on the management of innovation and technology, diffusion, implementation and adoption of new digital and e-technologies. Other interests include e-government, e-procurement and management of information security.

Mumtaz Kamala is a Senior Lecturer in Computing. His research interests include real Time monitoring systems, computer interfacing and flow visualisation systems, information systems, and information security management.