

Honest it's me! Self service verification

Lynne Coventry, Antonella De Angeli and Graham Johnson

Advanced Technology and Research

NCR, Discovery Centre

3 Fulton Road, Dundee, UK

+44 1382 598325

Lynne.coventry@scotland.ncr.com

ABSTRACT

At NCR we have been involved with tracking and evaluating different biometric technologies for a number of years. We have adopted a pluralistic approach evaluating from both a technology and user perspective. Multiple evaluation techniques have also been used. Some of our findings and implementation implications have been summarised in this paper, from the consumers' perspective. We cover the issues of selecting a biometric, enrolment, consumer fears and ultimately consumer acceptance.

Keywords

Biometric, verification, usability

INTRODUCTION

As services such as retail and finance have become automated, security measures have been put in place to ensure that only authorized access by legitimate people is allowed. These security measures usually take the form of personal identification number (PIN) and/or a plastic card. The PIN is the least secure of three levels of security. It is something only the account owner should know. It is more often the case that it is something which is forgotten, or written down (sometimes even on the card), and can be accidentally or deliberately revealed to someone [8].

The second level is the physical card. This provides the user's unique identifier and details of which account can be accessed. This belongs to the account holder and is believed to always be in their possession. The most common form of these cards has the information stored on a magnetic strip. Smart cards and RFID tags are gradually replacing this form. These can be forgotten, lost, stolen or forged.

The third level is that of biometrics, i.e. a unique physical or behavioural characteristic which can not be separated from its owner. Physical characteristics include retina, iris, fingerprint or geometry even body odour. Behavioural characteristics include signature and voice.

For extra security these levels of access security could be used in combination with each other.

On the surface, there appears to be many valid reasons to replace the PIN/card combinations at the ATM or signature/card combination with credit cards. There are potential benefits to the consumer of not remembering

numerous PINs and passwords. From a security perspective the card/PIN combination does not prove who is actually using them and can be defrauded and from a cost perspective, the cost incurred by bank IT departments to replace lost and stolen cards as well as forgotten PINs can be significantly reduced. The banks also have to deal with the increasing cost of card fraud.

Pioneering work on biometrics has been on going since the 1960's [1]. Despite this, we still have not reached a point where biometrics are in widespread use. The reason for this are succinctly summarized by Clark [2] in his list of desirable characteristics of an ideal biometric which still has not been achieved. The characteristics are that it be

- Universal – everyone should possess the characteristic,
- Unique and exclusive – each individual should have a unique version of the characteristic,
- Permanent through life,
- Indispensable,
- Digitally storable,
- Precise
- Easy and efficient to record,
- Acceptable to contemporary social standards.

Many systems do not live up to expectations because they fail to take into account the needs of people or to effectively cope with the enormous variations among large populations [6].

As with any technology, a large factor in its success is whether or not users will accept it. Within the financial sector, the technology needs to be easy to deploy and use, be convenient, and give individuals the feeling that they are in control of their data.

Our usability research, based on consumers and their behaviour and attitudes, has been instrumental in directing developments of these technologies and their use in self-service settings. It is too easy to forget that advanced technologies *per se* will not succeed without easy adoption by the intended users. Biometric technologies are a good example of advanced technology that impresses many, without understanding the impact users may have on successful implementation.

BIOMETRIC USABILITY RESEARCH AT NCR

As part of a multidisciplinary advanced technology and research group, the HCI team has been involved with tracking and evaluating biometric technology for around a decade. We have been involved in various studies throughout the world, using different technologies at different levels of maturity and utilizing different evaluation methodologies.

These methods include focus groups, large scale surveys, functional prototype testing and iterative design, lab based usability evaluation and field trials. This pluralistic approach has given us a unique depth and breadth of insight into the consumer issues with biometric technologies, within the context of implementing a solution in a self-service financial environment. During this time we have seen the rise of biometric testing groups and standardized methodologies such as the UK biometric group [10] and the International Biometric Consortium [9]. Unfortunately these remain laboratory-based evaluations and concentrate on technical measures rather than usability issues. While essential, these evaluations only provide a limited view of the technology. This position paper will look at issues impacting successful adoption from the consumer's perspective, discussing the consumer issues identified during our research and how they may be addressed.

The main issues we have identified are the selection of a biometric, enrolment, universality, consumer fears, and consumer acceptance.

Selection of a biometric

As well as performance, security and cost differences between biometric technologies, each kind of device presents its own set of user issues. Users react differently to different devices. Biometrics such as iris verification are seen as belonging in the realms of science fiction. This results in fear, suspicion, mistrust and disbelief in their abilities. Fingerprints and facial recognition systems are believable and acceptable to consumers. This initial acceptance can be eroded by experience of poor performance. In one of our studies we evaluated two facial systems and two fingerprint systems over a 6-week period. During this we found a before-use preference for facial over fingerprints was reversed after using actual systems. The problems with being recognised over time with a facial system became apparent. We also found that one fingerprint system was preferred over the other as it provided better feedback to the user (camera showing the image being collected) about the appropriateness of their behaviour.

In general, many of the devices on the market provide insufficient lead through and feedback to the user. This leads to failure to acquire problems and subsequently the user fails to gain access to the system.

Enrolment

Once a company decides to use biometric technology, it is essential that it educates employees and consumers of this practice. Enrolment provides an ideal opportunity for this education. Before a person can be verified by a biometric device they must be enrolled. During this process the user must provide a number of samples of the characteristic to be used. These samples are used to form a template to compare the new samples to when the system is used. Depending on the similarity scores the user is then accepted or rejected. Enrolment for the financial industry presents three problems; firstly the quality of the template is the key to efficient and accurate verifications. This process is not automatic requiring trained staff to administer the process. Secondly at this point in the process it is essential to ensure that the biometric is being registered against a legitimate and not being used to set up a fraudulent identity. Thirdly the sheer number of customers who would require enrolment - ultimately the banking population of the world! This would be time consuming. This could be even more problematic for those people who have opened an account via the internet, phone or postal service and do not regularly use a physical location.

Universality

Biometric devices are unable to handle some people. These are known as outliers. Lack of the biometric may be obvious in some cases such as a missing finger or eye but in other cases they may only become apparent through a failure to enroll. In our experience it is sometimes hard to see why these failures are happening. This may be because the system is too sensitive to variation, or that the user can not consistently present the biometric to the system. For instance if some one has very dark brown eyes or droopy eyelids, it is difficult for iris verification to work, some fingerprints are difficult to record. Or with disabled people tremors may prevent them using the system. Some illnesses or injury can also lead to temporary or permanent exclusion. In the case of iris verification this is affected by glaucoma and cataracts.

Some comparative evaluations treat failure to acquire and failure to enroll as the same as in either case there must be a fall back strategy to enable the consumer to access the system.

Fears

There is a general concern about the potential for the misuse of personal, biometric data collected, which is seen as violating their privacy and civil liberties. This issue is reviewed extensively by Woodward [13]. Within the financial services context, there are continuing debates over central storage of biometric templates versus holding the template on a smart card and verifying locally. Keeping the biometric information in the possession of the owner, rather than having to store, protect and transmit biometric data securely may be a viable approach. A related issue is a fear that biometric codes can be reproduced and used and

interjected into a system, bypassing the actual biometric device. The fear is that if a biometric is compromised in this way then that biometric identifier is rendered useless, but unlike a PIN, where a new one can be issued, a new biometric can not be issued.

There is also a fear that a criminal may injure them to remove a biometric rather than just steal their card. This is related to a fear that biometric devices can be defrauded not only by removed body parts, but by voice recordings, photographs, or fake fingerprints. The majority of vendors have continued to market their biometric device as only working with live biometric identifiers but this has been recently brought into question by Thalheim *et al* [11] and Jan Ernst [7]. Until this issue is genuinely resolved a multi-level security system may be required.

False accepts and False rejects

Biometrics have one significant drawback. Unlike a PIN which is either right or wrong, the information picked up when a biometric device is used will vary. A biometric system therefore, can not say with 100% accuracy that this is the right person. To combat this biometrics are designed to allow the accuracy to be varied according to the security requirements of the institution. In setting this False Accept Rate, we are also determining the False Reject Rate – the likelihood that a valued customer could be falsely rejected from the system. Within the financial environment it may be possible to ask the user to attempt to verify three times, this is the same opportunity they are afforded for remembering their PIN. The financial industry is particularly concerned with false rejects. They believe that refusing access to the legitimate account holder is unacceptable.

Consumer acceptance

We have found the base level of consumer acceptance to have increased over the years we have been involved with biometric research. A recent survey published December 1992 [12] showed that 78% of the American public would find it acceptable for biometric access to be implemented at ATMs. Our focus groups suggest that acceptance is linked to a number of views about the biometrics in general, as discussed previously. We have also found that the information provided about the biometric device and experience with an actual device can improve acceptance [3,4,5]. A similar trend was also reported by the International Biometrics Group (IBG)

The International Biometrics Group (IBG) found that when it explained how biometrics worked to focus groups and then asked individuals how they felt about having biometric technology at their financial institution, 60% responded in a positive manner. The percentage of positive responses increased to 90%, however, when IBG showed the individuals exactly how the technology worked by enrolling customers in a biometric program; a finger scanning system, for example. Users in general now seem to welcome an access method that can replace the

numerous passwords and PINs that they have had to memorize over the years.

This acceptance has changed over the years, in our initial studies; consumers did not report a strong need to replace PIN with a biometric. They would rather replace the card, as it would mean it could not be stolen, lost or forgotten. However this arises from a misunderstanding of how the technology would be implemented (verification rather than identification) and does not take into consideration the need to identify the bank account to be accessed for verification or how to provide a fall back solutions should the biometric device fail.

Some people want to maintain the status quo because they do allow other members of their family to access their accounts on their behalf.

DISCUSSION

The social issues surrounding biometrics are certainly complex. While there may be stigma attached with the keeping of records that include aspects of unique biological identifiers, this is not necessarily justified. With the caveat that biometric systems are properly regulated and not used for intrusive record keeping of an individual's life, consumer groups should not be worried. Most biometric technologies also tend to be branded as being physically intrusive. Only retina scanning is intrusive (in this way), with all other biometric devices being able to capture readings overtly but without being intrusive.

However, even to reach the stage where biometrics is incorporated into the current authentication environment will take a long time. For this technology to be of real value to consumers, industry consensus must first be reached before biometric reading devices become ubiquitous.

Biometric devices will continue to improve, becoming even more accurate and reliable as technology evolves and more affordable as development costs are recouped and production techniques progress. In a financial services environment, there is some way to go before biometric technologies can be implemented en masse. Hopefully in the near future, standards will be available that will allow for greater interoperability between biometric systems. The accuracy of any given biometric system will tend to be a function of how many identifiable data points it is able to map. Thus, a system that combines different sources of biometric readings is invariably more accurate as it can rely on a greater wealth of data, and more reliable as it can rely on multiple reading devices.

CONCLUSIONS

- The world needs ever-tighter security measures to combat the rising threats in modern society. To achieve a more secure society, better means of authentication of individuals' identities (including biometric data for identification that is near impossible to forge) is very important.

- The cost of fraud across the financial services industry continues to rise. The growth of online banking and retail and the growing availability of personal data have opened new opportunities for persons wishing to perpetuate fraud. The use of biometric authentication has the potential to drastically reduce these costs.
- A possibility under discussion is a national identity card containing biometric identifiers or inclusions of biometric data on state identification cards such as driver's licenses. Although this idea is still thought of as highly intrusive by civil libertarians, there is no doubt that biometric identification is more socially acceptable now than ever before.
- Biometric providers must strive to create robust, reliable solutions that can be integrated easily as a price that is commercially viable. While price will be driven down over time by competitive pressures, recouping of development costs, and improving production techniques, vendors must collaborate where possible to create interoperable standards and systems that can leverage multiple biometric readings.
- Although there are people working toward financial service solutions that could create cardless payments environments, they will encounter much resistance before this can be accomplished. While certain biometric technology vendors (iris and fingerprint) may be striving to achieve the goal of identifying individuals quickly, accurately, and reliably among a sample size of millions, most would recognize that this objective is a long way from becoming commercially viable.
- Our evaluations with the diversity of the general public in a walk up and use environment push biometrics to their limits and see past the marketing hype. Work is still required to ensure biometric technologies are universally usable but consumer resistance is falling. Our pluralistic approach has ensured both a broad and deep understanding of the issues to be resolved and the impact of users on the success of these advanced technologies.
- Biometric authentication is a very interesting and appealing technology. It has the potential to penetrate a vast number of applications. Once reading devices become cheap enough and the use of these technologies becomes more socially accepted, there is no doubt that biometrics will penetrate the retail financial services space. The security benefits of biometrics are undeniable as they provide a form of identification that hopefully cannot be stolen.

ACKNOWLEDGMENTS

Many people and institutions have been involved with these evaluations over the years. We would like to thank them all.

REFERENCES

1. Ashbourn, J. *Biometrics: Advanced Identity Verification*. Springer Verlag, London, 2000.
2. Clark, R. Human identification in information systems: Management challenges and public policy issues, *Information Technology and People*, 7,4, 6-37, 1994.
3. Coventry, L. and Johnson, G. More than meets the eye! Usability and iris verification at the ATM interface. In S. Brewster *et al* (eds) *Proceedings of the IFIP TC 13 International Conference on Human Computer Interaction (Edinburgh)1999*
4. Coventry, L., De Angeli, A. and Johnson, G. Usability and biometrics at the ATM. *Proceedings of the ACM Human Factors in Computer Systems – Chi'03 Conference*, April 2003
5. Coventry, L., De Angeli, A. and Johnson, G. Biometric verification at a self service interface. *Proceedings of the British Ergonomic Society Conference (Edinburgh) April 2003*.
6. Davies, S.G. How biometrics will fuse flesh and machine. *Information Technology and People*, 7,4, 1994
7. Ernst, J., Iris recognition: counterfeit and countermeasure. www.iris-recognition.org.
8. Hone, K.S., Graham, R., Maguire, M.C., Baber, C. and Johnson, G.I. Speech technology for automatic teller machines: an investigation of user attitude and performance, *Ergonomics*, 41, 7, 962-981, 1998.
9. International Biometrics Group. Comparative biometric testing. http://www.ibgweb.com/reports/public/comparative_biometric_testing.html
10. Mansfield, A.J. and Wayman, J.L. Best practices in testing and reporting performance of biometric devices, <http://www.cesg.gov.uk/technology/biometrics/index.htm>, 2001.
11. Thalheim, L., Krissler, J. and Ziegler, P.M. Bodycheck: Biometric access protection devices and their programs put to the test, C'T, 11, May 22, 2002 (www.heise.de/ct/english/02/11/114)
12. Westin, A. Biometrics in the mainstream: What does the U.S. public think. *Privacy and American Business Newsletter*, 9,8, December 2002.
13. Woodward, J.D. Biometrics: Privacy's foe or privacy's friend? *Proceedings of IEEE*, 85,9, 1480-1492, 1997.

The columns on the last page should be of equal length.