User Awareness of Biometrics

B.J.Edmonds and S.M.Furnell

Network Research Group, University of Plymouth, Plymouth, United Kingdom
e-mail: info@network-research-group.org

Abstract

Biometric technologies are slowly becoming more commonplace although their growth has not been as fast as some have predicted. There is a stigma attached to biometrics in that people have concerns over their usage. It may be that they fear what people may do with their personal biometric data or it may be that they do not like the intrusive nature of the devices.

A user-trial was proposed to investigate user awareness of biometrics, in order to determine what the general public know about biometrics and their use. Five biometric devices were chosen with regards to public availability and cost: Fingerprint recognition, Iris recognition, Facial recognition, Signature recognition and Voice/Speech recognition. Thirty participants were asked to answer questions before and after using the devices in order to gain an opinion of the technology. Fingerprint recognition was found to be the most favoured of the technologies, whereas Voice/Speech and Signature were the least liked.

Keywords

Biometrics, User awareness, Iris, Fingerprint, Facial, Signature, Voice Recognition

1. Introduction

The sales of biometric technologies are steadily increasing, as a result of people becoming more aware of security concerns (Lake, 2001). People are beginning to see the limitations of more conventional methods of security such as Personal Identification Numbers and Passwords, which rely upon people being able to remember them. This of course can be quite restricting when on average people have to remember two PIN numbers and up to another eight passwords and user names to go with this. It was also found that one in four of the people asked in a recently conducted survey have twice as many as that again (Scotsman News, 2005). This of course results in people using the same password for many systems, which weakens the value of the protection.

This research has been conducted in order to gauge public perception with regards to biometrics. The study involved exposing participants to the use of biometric devices and asking for their opinions based on a variety of questions before and after this exposure.

An underlying intention of the research was to look for the influence that media presentation and other peoples' views may have upon general public opinion regarding biometrics, and to see if actual use of the devices changed this opinion.

2. What are Biometrics?

Biometrics use who you are to identify you. This obviously saves having to carry a key or remember a password. Biometrics can utilise either physiological or behavioural characteristics. Suitable physiological characteristics can include Fingerprint, Hand Geometry, Iris Scanning, Retinal Scanning, Face, and Facial Thermogram. Alternatively, behavioural biometrics can be: Voiceprint Recognition, Signature Recognition, Keystroke Analysis, and Mouse Dynamics.

Biometric devices are becoming more common as people are beginning to realise that they are one of the most secure and user-friendly methods of securing devices. Biometrics can of course be implemented in most of the places that traditional password systems have been implemented. For example on laptops, where a password system has traditionally been implemented, a fingerprint scanner could be used instead. A door that would usually use a swipe card entry system could use an Iris scanning system.

There are of course many advantages to using biometrics: The main benefit is the potential for added security. It has been estimated that the chances of two people having the same iris pattern is 1 in 10 to the 78th power (CNN News, 2004). This is of course very good odds to support the use of biometrics, given that the population of the world is only 65 to the 10th power (World Population, 2003). Thus an identical match is in reality never going to happen. Biometrics are also very hard to forge, they are not like swipe card or password that can be stolen from you. If implemented appropriately, the user actually has to be there in person for the biometric device to work.

3. Questionnaire

In order to gauge the public's views it was decided that a user-trial be conducted, involving the use of a questionnaire. This was decided the best method to gauge the public's perceptions as it is an accurate measure of what the participant is feeling.

The questionnaire consisted of 28 questions for 30 participants. Following a number of questions about the participant's background, there were a series of questions about biometrics. The participants were then invited to use the biometric devices, answering set questions after each. This allowed for a good gauge of what the participants though of the devices before and after using them, and also what they believed were good about them.

For the hands-on part of the study it was decided that users would simply enrol with the device then attempt to log in to the system. This was considered to allow the participants to get a realistic view of how these devices could be used in a security application without requiring their prolonged participation. The duration of the enrolment and log in process varied for the different applications, but the participants were given a few minutes with each application to familiarise themselves with the device.

A total of five biometric techniques were involved in the trial, three of which were physiological (face, fingerprint, and iris) and two behavioural (signature and voice). These were selected on the basis of being techniques that were all commercially available for use on end-user systems at a reasonable unit cost.

3.1 Iris Recognition

An Iris in a person is completely unique to themselves, even in identical twins. The iris is one of the best biometric solutions. There are many advantages of Iris recognition over other biometric technologies ranging from: Speed, Stability and accuracy.

The hardware was chosen with regards to availability and also how feasible it was to actually use the hardware for the survey. For the Iris recognition the hardware used was the Panasonic authenticam this hardware was used in conjunction with SecureSuite made by I/O software Inc.

3.2 Facial Recognition

Facial recognition is one of the newer biometric technologies due to its complex nature. The face is an important part of who people are and we as humans use it to identify people from one another. It thus seems to make sense that Facial recognition be used as a biometric technology. The human face has around 80 nodal points that are used by biometric software to authenticate people. Only around 14-22 of these are used for facial recognition. The Nodal points that are recorded are made into a string of numbers represent the face, which are then stored in a database.

For the study, a program called FaceIt by Visionics be used. This program can be used with any camera to authenticate a face, so the authenticam was used again for this application.

3.3 Fingerprint recognition

Fingerprints are unique to each person this is due to them being influenced by the environment around them. The ridges on the fingerprint are formed during the foetal stage of life when the general shape is defined. These ridges remain the same throughout life, enlarging as the person reaches adult size. Fingerprints can reconstruct so long as the injury to them is not too severe.

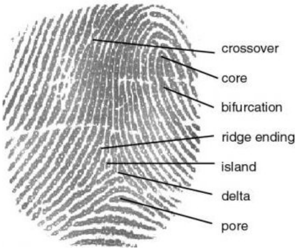


Figure 1: Minutiae of the fingerprint (Biometric Information, 2006)

As Figure 1 illustrates, there are a number of areas involved in a fingerprint although the complete range of characteristics is not always used in recognition, depending on the fingerprint device in use. Collectively the areas of a fingerprint are called Typica (Forensics Information, 2006).

The fingerprint recognition device used was made by Targus and was of the more expensive capacitive type. Again the software used was supplied with the device, and in this case was a security suite called OmniPass.

3.4 Signature

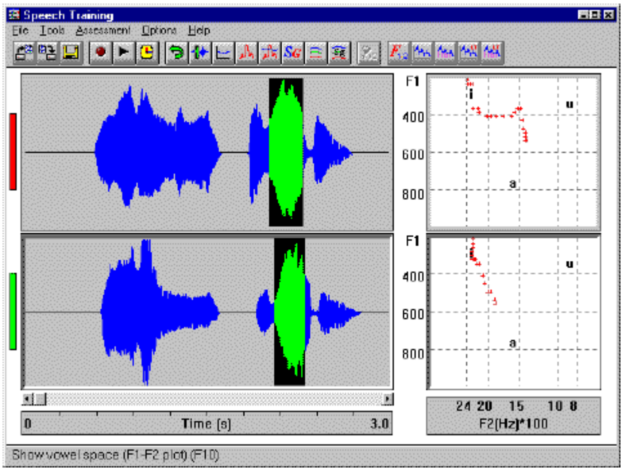
Signature recognition started life in a similar way to that of fingerprint recognition in that we have been signing to verify things for a long time in other contexts. As such, it only seems natural that it be used for biometric authentication.

Biometric signature recognition software does not treat the signature as just an image, but can compare a range of factors. Various signature dynamics (such as speed, relative speed, stroke order, stroke count and the pressure applied) are analysed. So the signature is not only being compared on how it looks but also by how it was generated (PDA Lok Company, 2006).

For the signature recognition a PDA was required due to touch screen. A readily available program called PDA Lok was downloaded as a trial version. Initially the program was tested on an MDA compact device, which is a smaller PDA. Writing a signature on such a small screen proved to be a problem so a Dell Axim was used instead.

3.5 Voice Verification/recognition

Voice verification works by digitising a profile of a person's speech to produce a voice print stored model, or template.



Show vowel space (F1-F2 plot) (F10)

Figure 2: Speech Pattern (Speech Technologies, 2006)

Figure 2 shows two speech patterns from the same person saying the same phrase. It can be seen that there are many similarities between the two recordings. Speech recognition compares these similarities and simply verifies that the user is who they claim to be. Voice verification is one of the least intrusive biometric technologies, as it simply requires the person to say something as simple as their name. Another advantage of the voice recognition idea is that users do not normally need to purchase new hardware in order to implement the solution.

For the speech recognition software a trial version of a program called Anovea made by Anovea Inc was used. This piece of software required a microphone and also some speakers. The program was run on a laptop computer so the internal speakers were simply used for this. A Logitech desktop microphone was used for this application. This, alongside devices from the iris, fingerprint and signature experiments, is shown in Figure 3.

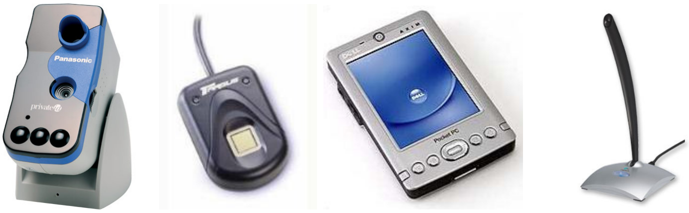


Figure 3: Biometric devices used

4. Results

An important factor that was looked at within the user-trial was how much that the general public knew about biometrics. A question was asked before the participants used each of the biometric devices simply asking whether or not they had ever used the particular biometric technology before.

The results show that the Biometric technology that the participants had used the most was Signature recognition (43% had used before). Although again this most likely due to people believing that signing for goods with a credit card is the same thing. Due to the fact that Signature recognition requires expensive equipment (PDA, or touch sensitive device) and is also one of the newest biometric technologies available, it is highly unlikely that this percentage of people had actually used it many times. Fingerprint recognition is one of the most widely used biometric technologies available and this is reflected in the fact that over one third of the people who conducted the user trial have used it before.

The two most rarely used biometric technologies were Iris recognition and Facial recognition. This is due to the fact that both these technologies have a reputation for being expensive and are more specialised to an application. Thus they are not used so much in applications that the public would have access to. Most of the reason behind Iris recognition being expensive when compared to other biometric methods was due to a twenty-year patent covering the technology, thus not allowing other researchers to develop it and create better-priced versions (ZD Net, 2006).

In conclusion to the question ‘How aware are the public of biometric technologies’ it can be seen that roughly 80% of people have heard of biometric technologies. Whereas from working out the mean 71.8% of people have never used one of the common biometric technologies used in this user trial.

An important factor of the user-trial was to see what type of biometric technology on test users favoured the most? This question was answered by asking the participant about how they perceived the security and usability of each device.

	Very				**Very**
	Secure				**Insecure**
Signature	4	8	6	3	5
	13%	26%	20%	10%	16%
Voice	3	8	9	4	2
	10%	26%	30%	13%	6%
Finger	14	12	3	2	0
	46%	40%	10%	6%	0%
Face	7	14	5	4	0
	23%	46%	16%	13%	0%
Iris	21	7	2	0	0
	70%	23%	6%	0%	0%

Table 1: How would you now rate the security of each approach?

From the results in Table 1 it can immediately be seen that the majority of people believe Iris recognition to be the most secure of the biometric technologies on test. This is of course wholly accurate; as already indicated, Iris recognition is the most accurate of all the biometric technologies. Fingerprint recognition also gained a good rating from participants this technology has been proven to be in theory very secure. It can be seen that signature and voice recognition scored the lowest in the question this is again hard to decide as their have been very little surveys on both these devices with regards to security. The only information available on security is from the manufacturers of the devices so cannot be taken to be completely accurate.

	Very				**Very**
	Easy				**Hard**
Signature	16	10	3	0	0
	53%	33%	10%	0%	0%
Voice	7	12	6	3	2
	23%	40%	20%	10%	6%
Finger	20	7	3	0	0
	66%	23%	10%	0%	0%
Face	7	11	5	5	2
	23%	36%	16%	16%	6%
Iris	10	12	6	2	0
	33%	40%	20%	6%	0%

Table 2: How would you now rate the usability of each approach?

Again, Fingerprint recognition (Table 2) can be seen to have the highest percentage of people rating it highly, this was expected from looking at the other results. It is quite probable that people like the idea of Fingerprint recognition because it is not as intrusive (in the sense of the time and effort required) as some of the other technologies, such as Facial and Iris recognition. It was also found from the author's point of view to be the easiest to use of the biometric devices on test.

Signature recognition was also rated highly with regards to usability, again this is most likely due to the fact that it is non-intrusive it is also something that the majority of people are used to doing. Voice and Facial recognition achieved amongst the lowest scores in terms of usability. This can be related to the fact that both of these devices took the longest to enrol with, also it can be seen that both of these devices are very intrusive of the user. For instance a number of people do not like having their photo taken, which is the way in which Facial recognition works.

As Fingerprint recognition has been rated so highly it is interesting to look into what application the general public have decided it to be most useful for. Within the user-trial a question was asked 'How appropriate do you consider Fingerprint recognition in the following scenarios' from this the participants were given a number choices to select: Passports and airport check-ins, Proposed national ID cards, Cash card ATM machines, logging onto computers, Entry into buildings, Verification of mobile phone users and keeping track of employee work hours.

For Fingerprint recognition the vast majority of participants rated it highly for use with Passports and Logging onto a computer. Although interestingly with regards to the proposed national ID cards people did not rate it so highly as for the use in passports with 50% and 66% respectively.

5. Conclusions

This paper has presented a wide-angled view of the way in which the public views biometrics. In that it has shown how aware they are of biometrics and also their reactions to different types of biometric devices.

From looking at the usability and security factors, fingerprint recognition looks to achieve the most well-rounded score. There are of course many reasons as to why the public may believe fingerprint recognition to be the best in these factors. Fingerprint recognition was one of the first biometrics to be developed, so it may simply be that the public are just more accustomed to the idea of having their fingerprint read. Another factor is that fingerprint recognition is one of the least intrusive biometric technologies. But again Iris recognition also scored very well in each of the three sections, which could be considered an intrusive technology as it requires a picture of the participant's eye and also involves a lot of aligning.

6. References

David Lake (2001), "Aye for an Eye – Biometric security systems –Industry Trend or Event", 23/07/01, *The Industry Standard*

Biometrics Information Web site (2006), “Fingerprint Types” http://perso.orange.fr/fingerchip/biometrics/types/fingerprint.htm (Cited 09/06)

CNN News Web site “Iris Accuracy Estimations” www.cnn.com (Cited 11/05)

Forensics Information Web site (2006), “Fingerprint Identification techniques” http://forensicshq.com/fingerprint_identification.php (Cited 08/06)

PDA Lok Company Web site (2006), “Digital Signature recognition” www.pdalok.com/about_biometrics/digital_signature_recogntion.htm (Cited 07/06)

Scotsman News Web site (2005), “Passwords add up to information overload for brain”, 04/10/05, http://news.scotsman.com/index.cfm?id=2034192005 (Cited 11/05)

Speech Technology Web site (2006), “Feature specification” www.speechpro.com/production/?fid=45 (Cited 06/06)

World population Web site “Current world population” www.ibiblio.org/lunarbin/worldpop/ (Cited 11/05)

ZD Net Web site (2006), “Foolproof Iris recognition technology?” 26/11/05, http://blogs.zdnet.com/emergingtech/?p=88 (Cited 08/06)