Public awareness of biometrics

K.Evangelatos and S.M.Furnell

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

Abstract

A fair degree of media attention has been devoted to biometrics, with the impression often being created that either they offer a panacea to our authentication needs, or that they are a way for governments and private organizations to monitor our activities. From this basis, a survey has been created to benchmark the public awareness of biometrics and their resulting attitudes, as these have been formed by the media coverage. The results revealed that people are much more accepting of those biometric systems that they are aware of (e.g. fingerprint) and which are more convenient to operate (e.g. signature) rather than the systems that they believe to be more secure (e.g. iris). Thus, it has been concluded that convenience, awareness and practical experience are essential requirements for the public acceptance of biometrics.

Keywords

Authentication, Biometrics, Survey, User Awareness

1. Introduction

Nowadays with the wide adoption of Information Technology (IT) and the Internet, identity thieves continuously find more sophisticated ways to perform frauds. To protect people from this threat, user authentication has been accepted as being the first line of defense against identity theft (Furnell *et al.*, 2000). Until today the pubic was relying on the "classic" authentication mechanisms of passwords and tokens, considering biometrics as something that belongs in science fiction. But nowadays the increased usage of electronic transactions and the increased level of frauds and terrorist attacks made passwords and tokens inadequate to prevent identity frauds; the 'crime of the century' as it has been characterized by the United States Department of Justice (2006). For this reason biometrics are constantly proposed in more and more applications, especially after the terrorist attacks of 9/11. This has unavoidably drawn a fair degree of media attention and as a result it is expected that a far greater number of people have now heard of biometrics. But how are biometric technologies presented by the media and how does this coverage affect the end users? This question is of particular interest since the public perception can impact upon user acceptance of biometric technologies as authentication mechanisms, which is one of the most important barriers to their wide deployment. From this basis, a survey has been conducted to benchmark the public awareness of biometrics and their resulting attitudes, based upon what they have seen or heard from the media. This paper begins by presenting the way that biometrics are presented by the media. Then details of the survey and an analysis of the obtained results are presented, leading to the conclusions that have been drawn.

2. Biometrics and the media

There are numerous movies, such as *Minority Report* and *I Robot*, where the heroes have to use their biometric characteristics in order to gain access to restricted areas, computers and files with sensitive data or even to start their cars. Although such movies present biometric systems as a 'James Bond' technology capable of providing absolute security (Black, 2002), they have made known to the general public the existence of the various biometric technologies and their potential applications. In addition there are articles, such as Chowdhary (2006), which suggest that with biometrics people will not have to remember numerous passwords and PINs or to worry if they forget their keys, their passports and of course their passwords. All these have created great expectations and formed the opinion that biometrics can be a panacea to our security problems. As a result the biometric industry has to overcome this 'Hollywood cure' (Wait, 2003) if users are to realise the true benefits of biometrics.

Additionally, the larger part of the media expresses concerns that biometrics are a threat to our privacy and civil liberties, especially in the case of passports and ID cards. Numerous articles mention that government agencies will want to obtain records with our biometric data, so that they can link them together with other information (e.g. criminal and tax records) and "have a complete picture of our private existence" (Mogg, 2006), creating the fear of Big Brother. Other articles are going further, considering the security of the centralised databases that will hold our personal data. Characteristic is the statement of Wood (2006): "creating one huge database could be the perfect gift for sophisticated computer hackers". This is truly a major risk since if the databases are compromised and the citizen's characteristics are stored as raw data (and not as one-way encrypted templates) they could be easily reconstructed and used by identity thefts. Such coverage most probably will have negatively affected the perception of the public, relating all the applications of biometrics with the initiatives of the various governments.

Although a significant number of commercially available biometric devices and many pilot tests have been run the last few years, only few people have a practical experience with such devices. In this context it is of interest to investigate the perception of the public about biometrics as it has been formed by the controversial media coverage described above.

3. Surveying public awareness of biometrics

In order to determine the user acceptance of biometrics as an authentication mechanism, a survey was conducted to assess public awareness about biometrics technologies and the attitudes of the potential users, as these might have been formed by the media.

The survey consisted of 34 questions, the majority being multiple choice, and was divided into three sections. The first section, questions 1 to 5, aimed to provide some demographic characteristics of the respondents. The second section, questions 6 to 10, included some general questions about the respondents' attitudes to IT and

security. These helped to identify the extent of IT and security awareness of the respondents. The third section, questions 11 to 34, intended to determine the user awareness and attitudes in relation to biometrics. The questionnaire was made available in two forms, a printed copy and an online version, and distributed through e-mails to a stratified random sample, chosen mainly from the mailing lists of the University of Plymouth, UK. These lists include staff and students from the various schools and departments of the University. Moreover printed versions of the questionnaire had been distributed randomly, to people in various locations.

The study was conducted over a four-month period, commencing in March 2006, during which approximately 350 e-mail invitations were sent to a wide range of individuals (based on their job/topic of study), their age and education level, with 154 completed responses being received. Additionally 80 printed surveys were distributed, yielding 55 responses, representing a total response rate of approximately 49%. In the following sections the results of the survey are analyzed trying to understand the public awareness and attitudes towards biometrics, as these have been formed by the media.

3.1 Demographic characteristics

The vast majority of respondents (81%) were aged below 30 indicating that they would have grown up with IT and therefore be more familiar with using it. This is justified by the fact that 59% of the survey respondents considered themselves as intermediate ability users, 35% as advanced and only 5% as novice. In terms of gender the sample was quite evenly distributed, with 57% of the respondents being female and 43% being male.

The majority of responses (79%) were from people with a higher education, reflecting the fact that the survey was mainly distributed through academic channels. Since this study was concentrated in UK, the majority of respondents (75%) were British citizens while the remaining 25% were foreigners working or studying in UK. This indicates that their perception about biometrics will have been mainly influenced by the way that the British media presents the topic.

In terms of the employment or study background a wide diversity was achieved, with 145 out of 202 respondents (72%) being from non-technological fields. This is of particular importance since the majority of the responses were from people with no or minimum IT education, indicating that their perception will have been most probably formed only from what they have experienced, heard or read about biometrics outside of academia.

Although at first glance the above demographic results do not suggest a truly representative sample of the general public, the achieved diversity can be considered as a fair reflection of the people that will form the base of the potential biometric users.

3.2 Public perception of IT security

The fact that 70% of the respondents consider IT security very important while no-one believes that it is not at all important indicates that the respondents are to some extent security aware. This conclusion is further enhanced by the fact that 75% of the respondents find identity theft a very serious threat, while only 1% of them believe that it is not a threat. Moreover the results clearly indicate that the majority of respondents (45%) have concerns about the ability of the currently employed authentication techniques to prevent theft in large scale systems (such as online banking), realizing the shortcomings of passwords and tokens.

Asking the respondents to rank their preferences from the security mechanisms used for authentication, surprisingly 125 out of 209 (60%) of them chosen as their first preference biometrics, although only 10% has used them before. The detailed results can be seen in Figure 1. This finding is in agreement with the results of a survey carried out by Unisys (2006), which found that 66% of the 1661 consumers worldwide favored biometrics. This fact further suggests the respondents' dissatisfaction with passwords and tokens, presuming that biometrics will be better. This is most probably caused by the media, which by presenting biometrics as a panacea to our security needs has increased the expectations of the users.

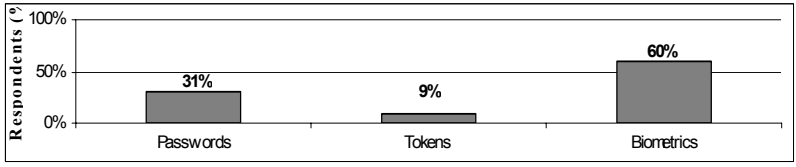

Figure 1: Respondents' preferred authentication mechanisms

3.3 User awareness

By asking the respondents if they have heard about biometrics before the survey it has been revealed that 135 out of the 209 (65%) are aware of them. However, when a list with various biometric characteristics was provided, only 10% of the respondents stated that biometrics does not suggest anything to them. This finding is in contrast with the results of the survey conducted on behalf of Citizenship and Immigration Canada (2003), which found that 44% of the 1,200 respondents "registered very low awareness", indicating that nowadays the public is much more aware of biometrics, which is a result of their extended coverage.

Following this question the 135 respondents were asked to indicate all the biometric technologies that they have either heard or used. The results showed that all of the mainstream technologies (see Figure 2) are well known, while a small percentage is even aware of newer techniques, such as the odor and gait recognition. Investigating further the user awareness, the 135 respondents were asked to indicate the proposed applications of biometrics that they are familiar with. The results showed that only 9 of the 135 (7%) respondents have not heard of any of the proposed applications (see Table 1). On the other hand, and as expected, the most known applications are citizen identification for border crossing (58%), ATM machines (58%), physical

access (53%) and PC/network access (51%), which are among the most discussed applications.

3.4 Media influence

Before investigating the influence of the media, the 135 respondents that are aware of biometrics were asked to indicate all the sources from where they have learned about them. The results showed that TV news (67%), newsprints and magazines (55%) are the primary sources of information, which is in accordance with the findings of Citizenship and Immigration Canada (2003) study. However, the rest of the findings show a major increase in the people that have heard about biometrics from various sources, reflecting the increased media coverage.

Investigating the extent of the media influence, the 135 respondents were asked to indicate any specific information that they could recall hearing or reading about biometrics. Quite few (43%) recalled various movies and articles about the proposed application of biometrics to passports and IDs, indicating the role of the media on informing the public. When these respondents were asked to state their opinion on how the media is treating biometrics, half of them described it as fair. This finding is quite important, showing that probably they have been influenced by both the part of the media that supports biometrics and by the part that criticizes them, forming a more rounded opinion.

To determine further the influence of the media, the 135 respondents were asked to state their opinion as to whether biometric systems can be easily cheated. The results showed that 72% do not believe that it is easy, indicating that the respondents have not been influenced by the media concerns that biometric systems can be cheated using fake characteristics, while 21% stated that they do not know, potentially suggesting that this coverage has confused them.

Continuing to investigate the role of the media, the 135 respondents were asked to indicate the biometric systems which in their opinion can be a health risk. Half of them stated that biometrics are not a health risk, while 37% believe that iris and 36% that retina recognition can be. This shows that quite few respondents have been affected by part of the media which consider iris and retina recognition as a health risk, and that they will most likely be reluctant to use their eyes for authentication purposes.

By asking the respondents to indicate on a 5-point scale the extent to which they believe that the mainstream biometric systems can work reliably, a rank of the of the expected reliability, Figure 2, has been obtained by adding the total number of positive responses (‘*extremely reliable’* and ‘*very reliable*’) and then subtracting the total number of negative responses (‘*not at all reliable’* and ‘*slightly reliable*’).

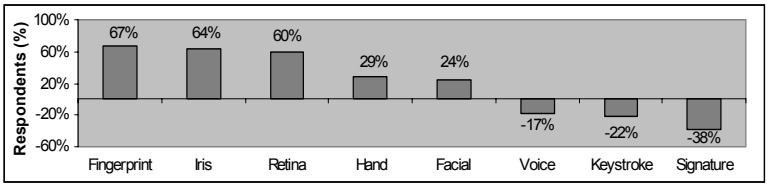

Figure 2: Ranking of the expected reliability of biometric systems

The results revealed a clear level of doubt in behavioural methods. For the case of keystroke an explanation for the negative result most probably is the minimum coverage of this method, while for the case of voice and signature the negative result reflects the fact that these methods are presented as the most easy to cheat. This view is actually reasonable, considering that the behavioural methods typically have worse False Acceptance Rates (FAR) and False Rejection Rates (FRR) than the physiological. It should be noted that no difference was observed between the respondents that have used biometrics and those that have not, indicating further the extent of the media influence.

3.5 User attitudes

One of the main objectives of the survey was to evaluate the users' attitudes towards biometrics based upon what they have heard or read from the media. This has been achieved by asking the respondents to indicate how comfortable they would be to use the mainstream biometric technologies for proving their identity. A rank of user preferences can be seen in Figure 3.

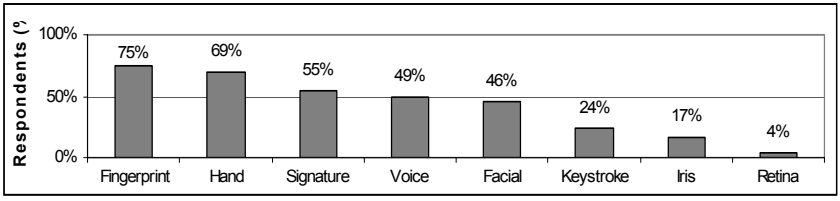

Figure 3: Ranked preference of biometric technologies

As expected, the most popular technology is the fingerprint recognition, despite the fact that it is known for its use by the police for identifying criminals. This indicates that the familiarity of the users with this method makes them extremely comfortable with the idea of using it. The above results are in contrast with the findings of the study carried by TNS / TRUSTe (2005), which found that 81% of the 1,003 American Internet users that participated consider as acceptable the fingerprint recognition, 58% the iris scan, 50% the hand geometry, 48% the voice recognition, and 44% the facial scan. This fact indicates that there are some demographical differences, which most probably are caused by cultural differences and from the different way that the media worldwide are covering the topic.

Maybe the most significant question posed in the survey asked the respondents to indicate how useful they find the use of biometrics in their various proposed applications. The ranked preferences can be seen in Table 1.

Proposed Applications of Biometrics	Percentage
1. Verify identity for passports and airport check-ins	75%
2. Check entry to government buildings	66%
3. Verify the identity of credit card holders	57%
4. Verify identity at ATMs for withdraw	56%
5. Looking for wanted criminals/terrorists at public events	53%
5. Verify identity of citizens (national ID cards)	53%
7. Check entry into schools and child services	48%
8. Check people for welfare fraud	38%
9. Verify identity for online transactions	30%
10. Verify voters during elections	28%
11. Verify identity for login to a PC/laptop/network	23%
12. Verify identity for telephone transactions	8%
13. Keep track of employee work hours	1%
14. Verify identity for using a cell phone	-7%

Table 1: Ranked preference of biometric applications

Observing the first ten preferences of the respondents reveals a pattern, which indicates that they find more useful the use of biometrics in applications relating to prevent terrorism and frauds. On the other hand the lower preferences of the users enhance the conclusion that the public prefer convenience rather than security.

Respondents were asked to indicate the time that they are willing to spend enrolling their characteristics, which then will be used by a biometric system to authenticate them. The majority (70%) of respondents are willing to spend up to half an hour, which nowadays can be sufficient in most cases for creating a profile. Once a user has registered his characteristic there is still a high possibility that the system will falsely reject him. To this end the respondents were asked to indicate the frequency with which they would be willing to tolerate such errors. The results showed that half of them are not willing to tolerate any errors, while 31% stated that they do not know. These results clearly indicate that biometric systems must have a low error rate, which is in accordance with the findings of Furnell *et al.* (2000).

Asking the respondents to indicate where their digital biometric characteristics (templates) should be stored, 40% of them stated that they prefer a central database and 25% that they do not mind. These results are quite surprisingly considering that the majority of the media express concerns for the risks associated by keeping the templates in a central database, once more indicating the users' preference to convenience.

When the respondents were asked to indicate whether they have concerns that their biometrics characteristics will be stolen with the purpose to cheat a biometric system, 56% of them (who in their majority do not believe that biometric systems can be easily cheated) stated that they are extremely or very concerned. This contradictory finding reveals the respondents' belief that criminals will find a way around this technology even though this will be very difficult.

Moreover, by asking the respondents to indicate how confident they are that their biometric characteristics will only be used for authentication purposes, a lack of confidence to both government agencies (57%) and organizations (50%) has been

revealed. This finding is in accordance with the results of TNS / TRUSTe (2005) study, where 64% of the respondents believed that the "potential for governments to misuse the information is too high", reflecting the fear of Big Brother that the public has. However, 37% of the respondents are willing to lose some of their civil liberties for great security, as revealed by a later question. But more interesting is the fact that 22% of the respondents stated that they are not sure, revealing the confusion of the public which most probably is caused by their desire for greater security and the negative impact of the media.

Trying to further investigate the users' attitudes and the role of the media the respondents were asked to indicate their opinion as to the likely impact of biometrics in security. Surprisingly the results showed that the vast majority (76%) has realized that biometrics will only add another layer of security while only 5% of the respondents believe that they will stop terrorism and frauds.

Looking the future of biometrics the results revealed that two in three respondents believe that biometrics will be widely deployed by the end of the decade, while only one in fifty does not believe in their widespread use. This clearly indicates that the extended coverage of biometrics has prepared the public for their deployment. This conclusion is further enhanced by the fact that 70% of the respondents are willing to use biometrics despite their concerns that their characteristics can be either stolen or misused. However, most of the respondents are either not willing to pay (34%) or willing to pay less than £50 (37%) for devices with biometric capabilities. This finding indicates that cost is and will be an important barrier to the widespread use of biometrics. Moreover, it has been identified that 26% of respondents are willing to pay more than £50 if it is to protect an expensive device (e.g. a laptop above £850), indicating that they are more concerned to protect the device and not their personal data.

4. Conclusions

The survey has shown that today the public appreciates much more the importance of IT security, recognizing the need for stronger authentication mechanisms. But this is contradictory when considering that they do not even use (or at least use correctly) the current authentication methods, suggesting that user convenience is by far more important than the desire for security. This conclusion is further enhanced by the fact that the respondents are more accepting of those biometric methods that are easy to use (e.g. hand), even though they consider them to be less reliable than others (e.g. iris).

Moreover it has been identified that important factors for the acceptance of biometrics are that of awareness and practical experience. A strong relation has been revealed between those methods which the users are aware but most importantly have used and those which they feel more comfortable with the idea of using. Thus, it can be concluded that convenience and awareness (including practical experience) are essential, and that biometrics that the users will actually be willing to tolerate and use must be chosen for each application scenario.

5. References

Black, J. (2002), "A Growing Body of Biometric Tech", *BusinessWeek* [Online], http://www.businessweek.com/
technology/content/jul2002/tc2002072_9892.htm, [Accessed 18/01/06]

Citizenship and Immigration Canada (CIC) (2003), "Tracking public perceptions of biometrics" [Online], www.cic.gc.ca/english/press/03/poll-biometrics-e.pdf, [Accessed 18/01/03]

Furnell, S.M., Dowland, P.S., Illingworth, H.M. and Reynolds P.L. (2000), "Authentication and Supervision: a Survey of Users Attitudes", *Computers & Security,* Vol. 19, No. 6, pp 529-539

Chowdhary, S. (2006), "Tech on the runway" [Online], The *Financial Express*, 16 January 2006, http://www.financialexpress.com/fe_full_story.php?content_id=114581, [Accessed 17/01/2006]

Mogg, W.R. (2006), "Someone to watch over you", *The Times* (London), 16 January 2006, pp 20

TNS / TRUSTe (2005), "Consumer attitudes about biometrics in ID documents" [Online], http://www.truste.org/pdf/Biometrics_Study.pdf, [Accessed 14/01/06]

Unisys (2006), "Consumers Worldwide Overwhelmingly Support Biometrics for Identity Verification, Says Unisys Study" [Online], http://www.unisys.com/about__unisys/news_a_events/04268651.htm [Accessed 21/07/06]

United States Department of Justice (2006), "Identity Theft and Fraud" [Online], www.usdoj.gov, [Date Accessed 05/01/2006]

Wait, P. (2003), Great expectations: Biometrics, *Washington Technology*, Vol. 18, No. 13

Wood, L. (2006), "Feature - Good for nothing, Leanne Wood explains why she will refuse an ID card", *Morning Star*, 9 January 2006