Biometric Authentication Adoption Issues

Gerald Ho
Greg Stephens
Rodger Jamieson - Director[1]

SEAR: Security, E-Business, Assurance Research Group
School of Information Systems Technology and Management
University of New South Wales
Ph: 61 2 9385 4414 Fax: 61 2 9662 4061
e-mail: r.jamieson@unsw.edu.au

Abstract

Biometric authentication technology is increasingly being adopted at a government and corporate level. Whilst technically feasible, we seek to understand the user acceptance issues surrounding its adoption. We compare a number of commercially available biometric techniques and develop a preliminary model of issues to be used in further case-study research.

Keywords

Biometrics, technology adoption, technology acceptance model, user acceptability.

INTRODUCTION

Biometric technology is considered the ultimate method of verification and identification, since it is dependent on who you are as opposed to what you have (a token), or what you know (a password or PIN). As the issue of security continues to grow at a global level, governments (particularly the US) are turning to biometrics to provide identity assurance. With this publicity and emphasis on the technology, companies too are turning to biometrics in order to secure their information and assets in this uncertain climate. From a managerial perspective, the driver towards biometric systems adoption appears to be greater security. However, whether such systems are acceptable from a user's perspective has not been addressed. In this paper we compare a number of biometric techniques across several criteria, and develop a preliminary model of issues surrounding user acceptance of biometric systems, showing how these criteria (and others) shape such acceptance.

CURRENT STATE OF THE INDUSTRY

Many biometric technologies have been put forward over time, and can generally be divided into two broad categories: physiological and behavioural. Physiological technologies are those based on physical characteristics such as fingerprint, face, iris, retina, hand (geometry or veins) and palm. Behavioural technologies rely on the unique way different people do things like speak, sign (a signature), use a mouse, or type. Biochip technology fits into neither of these categories, and being in a very early experimental stage (Stonehouse 2003), is not considered relevant to this research.

Since this research focuses on the commercial 'real-world' implementation issues of a biometric system, only those technologies that are commercially available will be evaluated. Thus biometrics based on the retina, palm, hand veins and mouse are also excluded – perhaps in the coming years they will become viable commercially.

The palm of the hand allows for a 'palmprint' to be created, utilising the feature points along the prominent lines of the palm. Palmprints however, are not necessarily unique, unlike the well-established fingerprint. In a small study by Duta et al (2002), there was a 5% overlap between genuine and impostor distributions. The future of palmprints is most likely as an extra discriminator to a fingerprint system, where the fingerprint cannot be properly collected, eg. in cases of dry skin, cuts, worn print, or missing finger.

Detecting vein patterns in the back of the hand is a relatively new technique involving a digital camera photographing the hand that is being illuminated by infrared light. The advantages of this technique are that veins are hidden and therefore much harder to forge than external hand geometry, are not easily damaged or obscured, and do not place high requirements on image resolution due to their large size. The oxygenated blood flow in the veins also provides for liveliness detection (Biometric Technology Today 2001). Whilst vein

1 SAFE: Security, Assurance, Fraud-prevention for E-business Research Program at the Securities Industries Research Centre of Asia-Pacific.

patterns appear promising, there has been very little published research on the technology, and one of the leading vendors in the area – BK Systems – no longer seems to exist. The other previously dominant vendor – neusciences – does not appear to be pursuing the technology anymore either.

At the moment there is a lack of sufficient research in retinal technology. Once considered a technology with great potential, the main supplier in the past (EyeDentify) has gone out of business, with no other vendors (producing commercial systems) to replace it. The situation will undoubtedly change in the coming years, with companies such as Retinal Technologies and EyeDentify Europe still in the market, however further academic and commercial research is required in the retinal technology domain.

Whilst mouse dynamics are often seen on lists of possible biometric technologies (eg. Furnell et al 2000), there is little (if any) significant research in this area. There are certainly no commercial products and it will be some time before any appear, if at all (the closest thing appears to be Predictive Media's use of mouse dynamics in conjunction with keystroke dynamics and website monitoring to help identify a user in order to tailor marketing).

OVERVIEW OF THE TECHNOLOGIES

Fingerprint and iris technologies have been selected for description as representative of physiological biometrics. Voice-based technology has been chosen as representative of behavioural biometrics. These systems have been chosen because they are the most mature and commercially adopted biometric techniques. Additional information regarding the operation of various biometric technologies can be found in Rejman-Greene (2002) and Liu & Silverman (2001).

Fingerprint

Fingerprint recognition relies on the fact that no two fingerprints are identical, making it a unique identifier for an individual. Whilst having been used by Governments, the Military and Law Enforcement agencies for some time, it is increasingly being considered in regular commercial applications as a method of authentication.

Fingerprint recognition usually involves identifying minutiae (the points were ridges end or divide), arches, loops and whorls in order to create a statistical template used to compare with samples during use. The chances of reproducing a fingerprint for fraudulent use are greatly reduced by not storing an actual physical image of the fingerprint. The sensors used to capture the print utilise digital/optical, thermal, capacitance or ultrasonic technologies.

The major advantage of fingerprint technology is that of acceptance. It is a well-known and understood form of identification, and has a reliable reputation. The accuracy, ease of use and installation of the technology are also advantages.

The major disadvantage relates to problems arising from injury to the user's finger – eg. simple cuts or burns can significantly impact the system's performance. This problem will be discussed in greater detail later in the paper.

Iris

Iris recognition establishes a person's identity through scanning the unique patterns found in the iris. It is a non-invasive, non-contact process where a stereo camera takes a digital image of the iris. The image is then compared with a template to verify the identity of the user.

The advantages of iris recognition are many. The iris is an internal organ and thus highly protected, yet still visible externally from a distance. Combined with the stability of the iris pattern over time and its high degree of randomness, it becomes an ideal biometric. There is limited genetic penetration (eg. identical twins have different irises), and liveliness testing is available through the changing pupil size.

The disadvantages of iris recognition relate to the nature of the iris inside the eye. It can be obscured by eyelashes, eyelids or reflections, deforms non-elastically with changes in pupil size, and moves considerably. The technology tends also to have negative connotations due to perceptions that it may affect one's vision (Daugman, 2000).

Voice

The features of a person's voice may be used for a variety of purposes, such as authentication, identification, classification, differentiation and lie detection. These are generally referred to as 'speaker recognition' (Markowitz 2002), however only speaker authentication and identification are of concern here.

Three different methods of operation for speaker authentication and identification exist. Text-prompted is a challenge-response form where the system requests the user to say a particular word or phrase, text-dependent involves using a fixed "voice password" which does not change, and text-independent allows the user to say any arbitrary set of words. A Linear Prediction technique is often used to create a "voiceprint" at enrolment that is used in subsequent comparisons.

The text-prompted method has the advantages of a lower model size (as the password is not stored), the user does not need to remember a password, and liveliness testing is assured due to the randomly changing text-prompts. (Broun et al, 2001) More generally, the advantages of voice authentication centre on its versatility. It can be used over the telephone for password resets, help identify criminals robbing a bank, keep track of people on parole or even keep journal secrets safe (Markowitz 2002). Additionally, it is much cheaper to implement than other biometric systems such as those using the fingerprint or iris. This is due to it not requiring dedicated hardware. However, it is important to note that poorer quality hardware (such as the telephone) decreases the performance of the system significantly (Ramachandran 2002).

COMPARISON OF TECHNOLOGIES

In order to compare the biometric technologies, several criteria have been selected. These appear to be the most significant in the literature, and were also mentioned in the pilot study interview (with practitioners involved in commercial biometrics):

- security – the confidentiality, integrity and availability of information used
- cost – the financial cost involved in adopting a particular technology
- accuracy - the ability to correctly match a biometric sample with its template
- visibility – the level of direct interaction required during system usage
- perceived invasiveness – the apparent degree one's self is impinged upon
- privacy invasiveness – the disruption to one's ability to control personal information

Further justification for the selection of these criteria is provided in the section following the comparisons, 'Development of a Preliminary Issues Model'. There are other issues important in the *overall* adoption of a biometric system (eg. the sensitivity of the information being protected) that are not relevant to a *comparison* of different techniques and therefore not included here. They have, however, been included in the section dealing with the development of the research model.

A summary of the technologies and issues is depicted in Table 1 below:

	Fingerprint	Facial	Iris	*Hand Geometry*	Voice	Dynamic Signature	Keystroke Dynamics
Security	Low	Medium	High	Medium	Medium	Medium	Low
Cost	Low	Low	High	Medium	Low	Low	Low
Accuracy	High	Low	Very High	Medium	Medium	Low	Low
Perceived Invasiveness	Medium	Low	Medium-High	Medium	Low	Low	Low
Visibility	Medium	Medium, possibly low	Medium	Medium	Medium, possibly low	Medium, possibly low	Medium, possibly low
Privacy Invasiveness	High	Medium	High	Medium	Low	Low	Low
Current vendors	Identix, Authentec, Veridicom	Identix, Cognitec,	Iridian, EyeTicket	Recognition Systems, Acroprint,	VeriVoice, Nuance	CIC, Cyber-SIGN, HESY	biopassword

Table 1 Summary of biometric technologies and issues

Security

Most research in the biometric field has centred on technical feasibility, new algorithms, techniques and so forth. It is perhaps a reflection of the relative immaturity of the field that there has been little research into the security aspects of the technology – such as the possibility of spoofing, replay or brute-force attacks.

The opportunities for replay attacks (where the digital biometric signal is 'replayed' back to the system, fooling it into thinking that the actual biometric has been presented) depends significantly on the way the system is implemented. Bolle et al (2002) provide a possible solution involving the server generating a pseudo-random challenge that is received by the client and used to create a response dependent on both the challenge and the biometric. Thus the information transmitted varies each time. Bolle et al (2002) also analyse the effectiveness of brute-force attacks on biometrics, however the factors involved do not provide any particular distinction between the different biometric techniques.

The popularity of fingerprint technology has resulted in it being trialled for spoofing more than other techniques. van der Putte & Keuning (2000) were able to defeat all six fingerprint systems they tried, both with co-operation from the authorised person and also without (eg. lifting the print from a glass surface or the scanner itself). The techniques they used were not expensive nor particularly complex – the inability of fingerprint scanners to accurately detect the liveliness of the 'finger' was the main problem. More recently, Matsumoto et al (2002) was able to defeat all eleven fingerprint systems that were trialled by using fake silicon and gelatine 'fingerprints'. These findings also highlight the need for independent testing apart from the claims of the vendors who produce biometric systems.

van der Putte & Keuning (2000) highlight the security problems with fingerprint authentication in that it is "the only system where the biometrical characteristic can be stolen without the owner noticing it or reasonably being able to prevent it." (p13) This is a great concern for the security of the technology, so much so that the Atos Origin consultants consider fingerprint scanners the least secure means of verification except for keystroke dynamics. Their ranking of the various technologies is shown in the comparison table(Table 1).

Cost

The financial cost of a biometric system varies markedly, depending on many factors besides the simple cost of the hardware and software associated with the technique. This is particularly significant since different techniques are better suited to different applications (eg. behavioural for continuous monitoring), impacting the total cost of the application. For the purposes of this comparison however, we assume that as far as possible, all areas of the system are identical except for the particular biometric technique being considered.

The developments in fingerprint technology have resulted in fairly low prices for sensors (which are incorporated into specific devices) – as low as US$2.50 for a swipe sensor and US$12.50 for an area sensor (Biometric Technology Today, 2002). Most other technologies (eg. hand geometry and iris recognition) are not as mature and therefore tend to be more expensive. Iris technology demands prices in the range of thousands of dollars for physical security solutions, and several hundred dollars for desktop-level devices (eg. Panasonic Authenticam). Lower hardware costs required for the behavioural techniques (voice, signature and keystroke) result in overall lower cost, particularly for large-scale deployments. These differences in price are reflected in Table 1.

Perceived Level of Invasiveness

No literature was found relating to the perceived level of invasiveness of various biometric techniques. Deane et al (1995) and Furnell et al (2000) consider overall acceptability but do not attempt to discover empirically the reasons for such acceptability. The ratings for perceived invasiveness are therefore based on knowledge of the technique and expected attitudes of the public.

Invasiveness is largely dependent on the level and type of physical contact involved, and the possibility of harm being caused. Thus the behavioural techniques (voice, signature, keyboard) invade the user least, followed by the physiological technique of facial recognition. Hand-associated techniques (fingerprint, hand geometry) have a moderate level of perceived invasiveness, since there is some contact (eg. an optical scan of the finger) – however, it is partly negated by the hand not being a particularly 'sensitive' area of the body. The eye, on the other hand, is considered much more sensitive and fragile. Iris recognition therefore has a greater perceived invasiveness – despite the technique essentially involving only a photograph of the eye, it is easier to perceive a possibility of harm compared with a simple scan of a fingerprint or photograph of the face (see Table 1).

Other biometric techniques with far higher levels of invasiveness include retina scanning, DNA sampling, and biochipping. These techniques are currently not in commercial use, however.

Visibility

The visibility of a biometric system depends mainly on the way in which it is implemented (particularly in a continuous monitoring sense), not the particular technology involved. However, some technologies – particularly behavioural – do lend themselves to being used in systems where low visibility is required. For

example, a voice-based telephone system may utilise voice authentication technology invisibly, a document-management system incorporate dynamic signature technology, or an operating system integrating keystroke dynamics. In each case, the user would be prompted for additional authentication information (eg. a password) only if the biometric reading varied too far from the template.

Physiological techniques tend to have greater visibility since the process involved in authentication tends not to be part of the regular usage of any application or system (as opposed to a technology like keyboard dynamics which needs only typing information). Thus the user must stop and perform the particular operation for the specific purpose of identification or verification. The exception to this could be in face recognition, where a mounted camera could be used to automatically provide access if an authorised user appeared before it – and indeed remove access should the user walk away during usage of the system. Table 1 shows the differences in visibility ratings for behavioural and physiological techniques.

Privacy Invasiveness

The level to which a biometric technique invades a person's privacy is dependent on the uniqueness of the biometric, the sensitivity of the information, and the possibility for combining data with other databases. A summary of the levels of privacy invasiveness of each technology can be seen in Table 1.

Behavioural techniques such as voice, signature and keystroke tend to be used mainly for verification, not identification. This is a result of the general limited uniqueness of behavioural biometrics (or possibly our current inability to detect differences to the required degree) – however it also means that one's privacy is impinged upon less by such techniques. Unique identifiers such as the fingerprint and iris open up the possibility of combining databases of personal information, or linking up to police databases of criminals.

Bolle et al (2002) provides a creative solution to the privacy problems of unique identifiers. They suggest the use of "cancellable biometrics", where a non-invertible distortion transform is applied to every presentation of the biometric information. Thus a fingerprint image is distorted at enrolment, and subsequently only distorted images are ever compared. The actual fingerprint of the user is never stored, and since the transform algorithm is non-invertible, even if someone obtains the algorithm and the transformed biometric, the original biometric cannot be recovered. This technique also solves the problem of the inability to reissue a new biometric should it become compromised (as one would do, say if a password were compromised), a problem with the intrinsic link between person and biometric. A new transform can simply be issued if a compromise occurs. Bolle et al (2002) apply this technique to face, fingerprint, iris and voice biometrics.

Facial and hand geometry techniques lack the identifying capabilities of fingerprint and iris. They are, however, more favourable from a privacy perspective because such information is less sensitive. Photographs of faces are commonplace on existing identification cards (although such ubiquity could be used for comparison/joining of databases, IBG 2003), and a set of numbers representing the size and structure of a person's hand would also not be of great concern. Similarly, signatures are already stored on countless documents, and keystroke or voice statistics are fairly meaningless outside of the system that created them.

Accuracy

The accuracy of biometric systems has been the subject of much research, since it is clearly one of the main determinants of its feasibility. As mentioned previously, accuracy is determined by the error rates of the system. The False Non Match Rate (FNMR, Type I error) is the percentage chance of rejecting a match that should have been accepted, whilst the False Match Rate (FMR, Type II error) is the percentage chance of accepting a match that should have been rejected. They are analogous to the terms False Reject Rate (FRR) and False Accept Rate (FAR), which relate to matching a sample within the *entire population* (ie identification) rather than between a *single pair* of samples (ie verification). Thus if the population is very large, the FRR and FAR will be substantially greater than the FNMR and FMR (technically, $FAR = 1-(1-FMR)^N$ and $FRR = 1-(1-FNMR)^N$ where N is the number of templates in the database).

There tends to be a trade-off between FNMR and FMR – adjusting the threshold of an algorithm so that the FNMR is low tends to raise the FMR, and attempting to lower the FMR tends to raise the FNMR (see Figure 1). The point where FNMR equals FMR is known as the equal-error rate (EER), and is often used to quickly assess the performance of a biometric system.

The Failure to Enrol Rate (FER) measures the percentage of users that cannot use a system, eg. a fingerprint sensor that is unable to detect worn fingerprints of manual labourers. When a user cannot enrol, an alternative form of authentication must be provided, and this may weaken the overall security of the system (eg. resorting to reliance on a PIN).

The National Physical Laboratory in the UK did the most comprehensive testing of comparative biometric technologies in 2000. Figure 1 shows the results of the relative accuracy of each product, as the threshold is manipulated. The iris technique is clearly the most accurate, with FAR of 0.0001 and FRR of 0.25 (only one measurement exists due to the fixed threshold of the product).

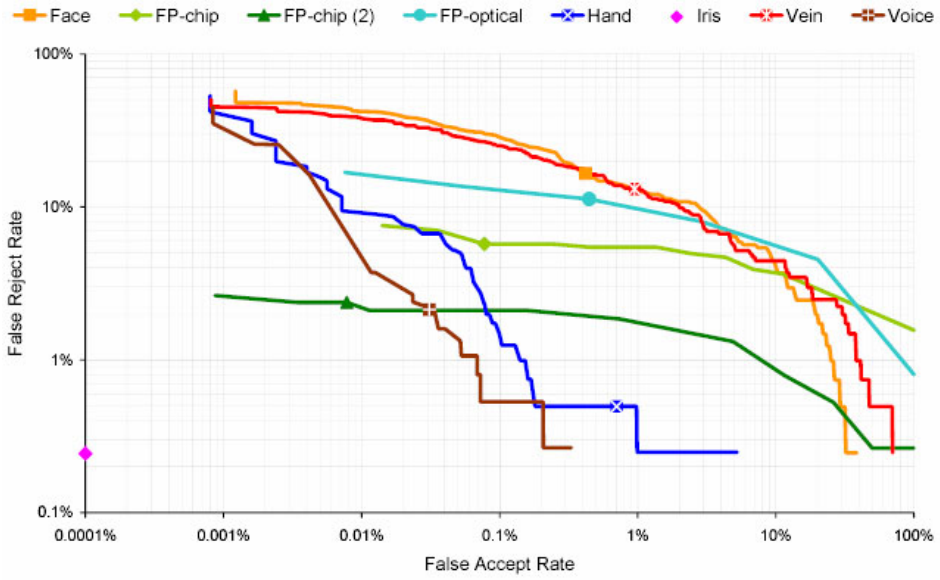

Figure 1 Accuracy of different biometric technologies: the FNMR vs FMR trade-off (best of 3 attempts) (Mansfield et al., 2001, p.11)

Research in fingerprint matching is relatively mature compared to other biometric technologies. The results of the Second International Fingerprint Verification Competition (FVC2002) are indicative of this, with outstanding results from some entrants. The most successful algorithm in FVC2002 achieved an average EER of only 0.19%, and an average ZeroFMR (the lowest FNMR for FMR=0) of 0.38%. Thus even if maximum security is desired (FMR=0% – no false acceptances), according to these results there would be less than one false rejection per 250 matches.

Despite such positive results, fingerprint technology is influenced by non-ideal factors such as: i) bruises or injuries on fingers, ii) peeling of the skin on the finger, and iii) dryness of the finger (Jain et al., 1999b). Optical fingerprint readers are particularly susceptible to artificial marks. Although fingerprints do not naturally change over time, fingerprints can wear down throughout life (particularly with manual labourers), reducing the accuracy of fingerprint matching. Despite these concerns, the overall accuracy of the technology is still quite high.

In the face recognition field, the Face Recognition Vendor Test (FRVT) 2002 provides a faithful indication of the accuracy of commercially available products. FRVT 2002 was the largest evaluation of automatic face recognition to date, using 37,437 individuals and multiple images of each individual taken on different days. The most accurate product had a FMR100 of 10% and a FMR1000 of 18%. These rates vary depending on characteristics such as whether the image is taken indoors (indoor images have about a 40% lower FMR100), the age of the individual (older people are easier to identify), and the time elapsed between the database and new images (the greater the time the more difficult the identification).

Despite great improvements in facial recognition technology, there is still a long way to go to reach the accuracy levels of technologies such as fingerprint recognition – current performance is comparable to that of fingerprint technology in 1998 (http://torch.nist.gov/public_affairs/releases/n03-04.htm). The use of three-dimensional morphable models was shown to raise performance in FRVT 2002, indicating a possible avenue for further development (Phillips et al., 2003).

The largest and most recent study of iris recognition performance was conducted by Cambier (2002) for Iridian Technologies (the dominant maker of commercial iris recognition products). There were 983,736,000 template pairs, and tests were carried out using a variety of HD (Hamming Distance) thresholds. With an appropriate threshold for the database, no false matches were observed. The estimated FMR was 3.0×10^{-11}, and the estimated FAR 3.0×10^{-6}. Similarly impressive results with the Daugman algorithm (the basis for Iridian and essentially all current iris recognition products) have been achieved by Daugman (2003) and the UK National Physical Laboratory (2001).

For voice authentication, the method of operation (text-prompted, text-dependant or text-independent) plays a large role in determining the accuracy of a voice authentication system. Text-independent operation is significantly worse than text-prompted operation – Lamel & Gauvain (2000) obtained an EER of approximately 6.5-7% for text-independent compared with around 2% for text-prompted.

Lamel & Gauvain (2000) also showed that linguistic content influences accuracy. When using digit strings, the EER was 4.1%, with sentences, 2.7%, and SEPT (five phonetically controlled sentences), 2.3%. SEPT sentences performed better due to the smaller number of phonetic contexts (allowing for more accurate acoustic methods to be estimated), they were easy to remember and pronounce (the other sentences were taken from a newspaper), and users' familiarity with digit strings likely resulted in worse pronunciation, adversely influencing accuracy. Undoubtedly there are many more factors involved in the complex process of speaker authentication.

Speaker authentication may be carried out over a number of different mediums, and the quality of these play a considerable role in the accuracy of the system. Ramachandran et al. (2002) obtained the following equal error rates using a text-dependent system: landline 0.84%, cellular 3.71%, multimedia (through a PC microphone) 0.03%. Overall, the speaker authentication domain is still quite immature, with great variations in accuracy rates and much research still underway in regards to the best algorithms and techniques.

Hand geometry-based verification systems have been in existence since the early 1970s, however there is little open literature available, with much of it in the form of patents (Jain et al., 1999). The prototype system developed by Jain et al. (1999) and tested with 50 users had reasonable results (for a prototype), eg. with a 0.1 FAR the FRR was 8%. The results of the NPL study (Figure 1) are far better due to the use of a commercial product. Hand-geometry has the advantage over (particularly optical) fingerprint techniques due to its ability to function well despite dirt, sweat or worn prints. This benefits accuracy by providing consistent data in varying conditions, although there are possible hygiene concerns as sweat and dirt accumulate on the sensor. Overall, it is difficult to judge the accuracy given the little information, however the NPL results and the technique's maturity and flexibility suggest that it is reasonable.

Dynamic signature analysis has the advantage of being acceptable due to its pre-existing usage. However, it suffers from an accuracy standpoint, due to the sometimes large intra-class variation (ie an individual's signature may change significantly). Jain et al. (2002) undertook an experiment using 1232 signatures of 102 individuals, with the best results of a 2.8% FRR and 1.6% FAR. These results used writer-dependent thresholds (computed from the reference signatures), as opposed to a common threshold (which resulted in 3.3% FRR and 2.7% FAR).

Despite a significant amount of research into keystroke dynamics both prior to 1990 (see review in Joyce & Gupta, 1990), and post-1990 (Monrose & Rubin, 2000), there seems to be little in the way of commercial products and therefore accuracy data. Due to its promising nature for continuous monitoring however (Furnell et al., 2000) it has been included in this comparison. A study involving 63 users by Monrose & Rubin (2000) achieved correct identification rates varying between 83.22% and 92.14%. Greater accuracy is achieved using structured text rather than arbitrary 'free-text', which would favour applications such as a password-based system. As a verification system alone however, the accuracy is far lower than other techniques. Table 1 provides a simple summary of the varying degrees of accuracy of the biometric techniques.

It is clear that there is no single biometric technique that is ideal for all circumstances. Those with high accuracy (iris, fingerprint) tend to have potentially greater privacy invasiveness, whilst behavioural techniques (voice, signature, keystroke) have lower accuracy and yet lower invasiveness (both privacy and bodily). Thus it is all the more important that a decision to implement a biometric authentication system be carefully considered, with all aspects taken into account – including those in the issues model, which follows.

DEVELOPMENT OF A PRELIMINARY ISSUES MODEL

The revised technology acceptance model (TAM) by Davis et al (1989) provides a foundation for understanding the issues surrounding the adoption of biometric technology. In this context, the traditional constructs of perceived usefulness and perceived ease of use must be moulded somewhat from their original definitions to be appropriate for biometric systems.

We propose that a number of factors and issues contribute to the formation of perceived usefulness and perceived ease of use in a biometric context. These are outlined in Figure 2.

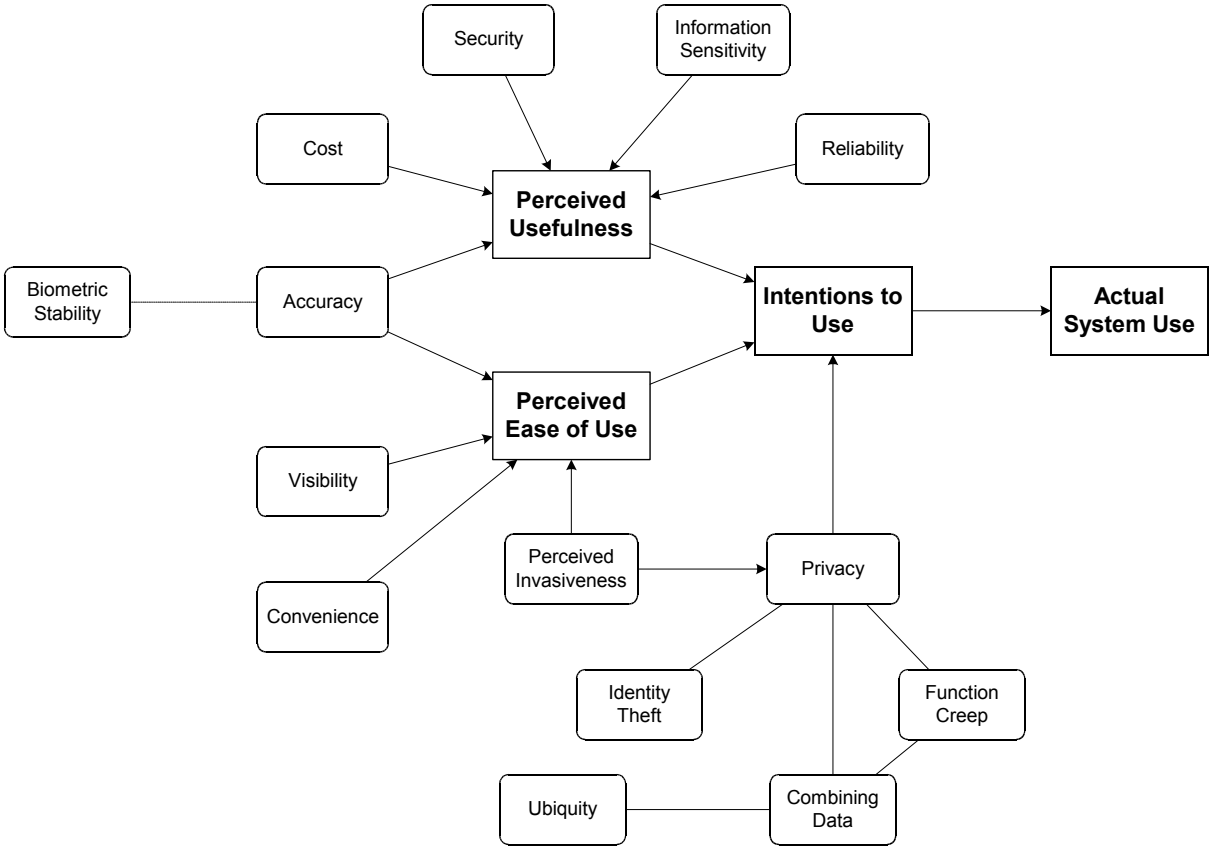

Figure 2 Proposed adaptation of the revised technology acceptance model (Davis 1989)

Davis defined perceived usefulness to be "the degree to which a person believes that using a particular system would enhance his or her job performance" (Davis 1989, p.320). The perceived usefulness of a biometric authentication system is not as directly related to job performance as the systems Davis probably had in mind when developing the TAM. However, given the importance of security in today's corporate environment, the protection of physical assets or information for which employees have responsibility is a fundamental aspect of job performance – with serious consequences should they fail. Even without a direct responsibility for security, any breaches would negatively impact the company, whose good health employees are reliant upon. Thus we define perceived usefulness more broadly to be the degree to which a person believes that using a particular biometric system would fulfil the organisation's security access requirements in a particular domain.

Based on this definition, the security, accuracy, cost, information sensitivity and reliability (Deane et al 1995, for latter three) of a biometric system are determinants of perceived usefulness. Only the first three factors were considered in the comparison, since information sensitivity is independent of the technology, and reliability was felt to be determined more by particular products (and their maturity) than the technique in general – however this may change in the future.

Security relates to the confidentiality, integrity, and availability of the information that is being processed and stored by a system (Institute for Telecommunications Sciences Telecom Glossary 2000). In the biometric context, security is determined by factors such as the ease of counterfeit (fake biometric), the possibility of replay attacks and the susceptibility to brute-force attacks (Ernst 2002, Bolle et al 2002). The greater the security of the system, the better it will be at fulfilling the organisation's security access requirements and therefore the greater perceived usefulness.

Commercial biometric systems are generally quite immature and may utilise expensive hardware and software. Financial cost is a significant concern in determining perceived usefulness, since system deployment cost may be too great to justify the protection of the particular information or asset in question. The various technologies differ markedly in their cost (pilot study interview, 10 June).

Accuracy is the degree to which the system is able to correctly match a biometric sample with its pre-existing template (for either identification or verification) in a real-world setting. The accuracy of a biometric system is dependent on its error rates, namely the False Acceptance Rate (FAR), False Rejection Rate (FRR) and Failure to Enrol Rate (FER). Over time these are affected by the stability of the biometric, eg. whether one's iris will change in a year. Accuracy is perhaps one of the biggest determinants of both perceived usefulness – since an

inaccurate system will accept impostors, compromising security – and perceived ease of use, since the system will reject legitimate users and cause frustration and wasted time.

The sensitivity of the information being protected is a determinant of perceived usefulness, as the negative aspects of a biometric system appear more justified when the sensitivity is greater. This positive correlation between acceptability of biometric systems and sensitivity of information was found by Deane et al. (1995). Similarly, an opposite effect was obtained in regards to the acceptability of passwords – it was evident that the survey respondents were familiar with the their shortcomings.

The reliability of a system, "the probability that the system remains successful (does not fail) in achieving its intended objectives" (Zahedi 1987) will always be important in determining its perceived usefulness (simply by its definition). For a biometric system, however, its ongoing success is even more important due to its use in a security context.

The TAM definition of perceived ease of use – "the degree to which a person believes that using a particular system would be free of effort" (Davis 1989, p.320) – does not need any modification to be applicable to a biometric system. It can be considered as simply another system that people use.

Although similar to regular information systems, a biometric system differs by the intrinsically personal data it utilises. This leads to information privacy – "the ability of the individual to personally control information about one's self" (Stone et al 1983) – becoming very important. The regular privacy issues summarised by Smith et al (1996) tend to be exacerbated by biometrics, and include:

- Collection – concern that extensive amounts of personal data are being collected and stored
- Unauthorised Secondary Use (internal/external) – concern that information is collected for one purpose but used for another (either internally or externally), without authorisation
- Improper Access – concern that personal data is available to people not authorised to view or work with it
- Errors – concern over inadequate protections against deliberate and accidental errors
- Combining Data (tangential) – concern that data from disparate databases may be combined into larger databases

(Smith et al.,1996, p172)

Personal privacy appears to be one of the primary concerns people have when considering biometrics against traditional authentication techniques. Such concern is quite justified considering the highly personal information involved – identity theft is taken to a new level if a biometric signal is somehow counterfeited. With current implementations there is no equivalent of a 'password reset' – the information is intrinsically *you* (Bolle et al. (2002) propose a helpful technique called 'cancellable biometrics' to overcome this problem). The combination of multiple databases in order to create a profile of one's details is seemingly made easier through uniquely identifying biometrics. Similarly, fears have been raised about a 'big brother' style monitoring through the ubiquitous use of biometrics. An 'electronic trail' of one's actions could be traced, thus reducing anonymity and pseudonymity. Such widespread use of biometric information may arise from function-creep, where information is used for purposes beyond the original intentions (Clarke, 2002 and http://www.epic.org/privacy/biometrics/). Privacy is therefore an influential factor in shaping people's intention to use a biometric system, as Figure 2above depicts.

Visibility is the level of direct interaction required of the user to use the system (ie how 'visible' the system is to the user). For a biometric system this is determined mainly by whether it is behaviourally or physiologically based. It is possible for a behaviourally based biometric approach to be almost invisible, where a continuous monitoring solution only interrupts when behaviour is deemed atypical. Deane et al. (1995) found that behaviourally based systems were less acceptable than physiological ones, however Furnell et al. (2000) found the opposite to be true. Despite the contradictory findings, it is clear that the issue of visibility does play a role in perceived ease of use and acceptance.

The invasiveness of biometric systems has been mentioned as a major drawback of the technology (Clarke 2002, Deane et al. 1995). A higher level of invasiveness leads to greater effort required to use the system, where 'effort' includes uncomfortableness and stress at possible side effects of usage. It is also linked to the issue of privacy (see Figure 2, above), since a highly invasive technique tends to reveal information of a more private nature. It is suggested that we consider *perceived* invasiveness rather than invasiveness alone, due to the level of 'familiarity' the general public has with biometric technologies from the media/movies. These depictions tend to shape opinion but do not necessarily reflect the true nature of the technologies involved.

The level of convenience associated with using the system was felt to be a significant determinant of perceived ease of use. Since biometric systems do not suffer from things such as forgotten passwords or stolen or lost tokens, they are arguably more convenient. The greater speed (Deane et al., 1995) and redcued effort involved in authentication may also raise convenience, eg. speaking a password rather than typing it. Although arguably different across the various techniques, overall convenience was deemed to be determined mostly by the particular implementation of the technique (ie the commercial product).

CONCLUSION AND INTENDED RESEARCH

We have seen that there are many issues surrounding the introduction of a biometric authentication system. It is clear that there is no single biometric technique that is ideal for all circumstances, with some having high accuracy and yet greater privacy invasiveness (iris, fingerprint), and others having lower accuracy and lower invasiveness (behavioural techniques). Implementing a biometric authentication system therefore requires careful planning and management, and a thorough understanding of the acceptance and adoption issues.

With the proposed model of issues developed here, we intend to investigate how these issues correspond to actual managerial and user attitudes in companies that have already adopted a biometric authentication system. These case-studies are among the first in this area, and will provide great insights into how these issues exist and interact. The model will therefore be validated and/or revised, being available for further research leading toward the development of an implementation methodology for biometric systems that will help alleviate the acceptance issues.

REFERENCES

Biometric Identifiers (2003), URL http://www.epic.org/privacy/biometrics/, Accessed 26 May 2003.

Bolle, R. M., Connell, J., H., and Ratha, N. K. (2002) Biometric perils and patches, Pattern Recognition, vol 35, issue 12, p2727-2738.

Broun, C. C., Campbell, W. M., Pearce, D., and Kelleher, H. (2001), Motorola Human Interface Lab, URL http://citeseer.nj.nec.com/broun01speaker.html, Accessed 27 May 2003.

Cambier, J. L. (2002), Iridian Cross-Comparison Test, Technical Report TR-02-004, VP Research, Iridian Technologies, Inc

Clarke, R. (2002), Biometrics' Inadequacies and Threats, and the Need for Regulation, URL http://www.anu.edu.au/people/Roger.Clarke/DV/BiomThreats.html, Accessed 26 March 2003.

Daugman, J. (2000), Advantages and Disadvantages of the Iris for Identification, URL http://www.cl.cam.ac.uk/users/jgd1000/addisadvans.html, Accessed May 14 2003.

Daugman, J. (2003), The importance of being random: Statistical principles of iris recognition, Pattern Recognition, vol. 36, no. 2, p279-291.

Deane F., Barrelle, K., Henderson, R., and Mahar, D. (1995), Perceived acceptability of biometric security systems, Computers & Security, vol. 14, issue 3, p225-231.

Dearne, K., 2003, Travellers to the US will be fingerprinted, The Australian IT Business, 27 May, p4.

Duta, N., Jain, A. K., and Mardia, K. V. (2002), Matching of palmprints Pattern Recognition Letters, vol. 23, issue 4, p477-485.

Ernst, J., (2002), Iris Recognition: Counterfeit and Countermeasures, URL http://www.iris-recognition.org/counterfeit.htm, Accessed May 15 2003.

Furnell, S. M., Dowland, P. S., Illingworth, H. M., and Reynolds, P.L. (2000), Authentication and Supervision: A Survey of User Attitudes, Computers & Security, vol. 19, issue 6, p529-539.

Hand measuring systems, Biometric Technology Today, vol. 9, issue 4 (April), p9-11.

International Biometric Group (2003), BioPrivacy Risk Ratings, URL http://www.ibgweb.com/reports/public/reports/privacy_technology.html, Accessed 30 May 2003.

Institute for Telecommunications Sciences (Telecom Glossary 2000), Definition: automated information systems security, URL http://glossary.its.bldrdoc.gov/fs-1037/dir-003/_0437.htm, Accessed May 15 2003.

Jain, A. K., Griess, F. D., and Connell, S. D., (2002), On-line signature verification, Pattern Recognition, vol. 35, issue 12, p2963-2972.

Jain, A.K., Ross A., and Pankanti S., (1999a), A Prototype Hand Geometry-based Verification System, 2nd Int'l Conference on Audio- and Video-based Biometric Person Authentication (AVBPA), Washington D.C., March 22-24, 1999, p. 166-171.

Jain, A. K., Prabhakar S., and Ross A., (1999b), Fingerprint Matching: Data Acquisition and Performance Evaluation, MSU Technical Report TR99-14, 1999.

Joyce, R., Gupta, G., (1990), Identity authorization based on keystroke latencies, Communications of the ACM, vol. 33, issue 2, p168-176.

Lamel, L.F. & Gauvain, J.L. (2000), Speaker verification over the telephone, Speech Communication, 31, 141-154.

Liu, S., and Silverman, M., (2001), A practical guide to biometric security technology, IT Professional, vol. 3, issue 1, p27-32.

Mansfield, T., Kelly, G., Chandler, D. & Kane, J. (2001). Biometric Product Testing Final Report, Centre for Mathematics and Scientific Computing, National Physical Laboratory.

Markowitz, J. (2002), Speaker Recognition, Biometric Technology Today, vol. 10, issue 6 (June), p9-11

Matsumoto T., Matsumoto H., Yamada K., Hoshino S. (2002), Impact of Artificial Gummy Fingers on Fingerprint Systems, Proceedings of SPIE Vol. #4677, Optical Security and Counterfeit Deterrence Techniques IV.

Monrose, F., and Rubin, A. D. (2000), Keystroke dynamics as a biometric for authentication, Future Generation Computer Systems, vol. 16, issue 4, p351-359.

National Physical Laboratory, UK, CESG contract X92A/4009309 (2001), Biometric Product Testing Final Report, URL http://www.cesg.gov.uk/technology/biometrics, Accessed April 20 2003.

NIST (2003) Commerce's NIST Reports Significant Advances Made in Facial Recognition Technology, URL http://torch.nist.gov/public_affairs/releases/n03-04.htm, Accessed 27 May 2003.

Phillips, P. J., Grother, P., Micheals, R. J., Blackburn, D. M., Tabassi, E., & Bone, M. (2003), Face Recognition Vendor Test 2002: Overview and Summary, URL http://www.frvt.org/DLs/FRVT_2002_Overview_and_Summary.pdf, Accessed April 20 2003.

Ramachandran, Ravi P.;Farrell, Kevin R., Ramachandran, Roopashri & Mammone, Richard J. (2002),. Speaker recognition - general classifier approaches and data fusion methods, Pattern Recognition, 35(12), 2801-2821.

Rejman-Greene, M. (2002), Secure Authentication Using Biometric Methods, Information Security Technical Report, vol. 7, no. 3, p30-40.

Silicon sensors size up, Biometric Technology Today, vol. 10, issue 7 (July/August), p9-11.

Smith, J., Milberg, S. J., and Burke, S. J. (1996), Information Privacy: Measuring Individuals' Concerns about Organizational Practices, MIS Quarterly, vol. 20, issue 2 (June), p167-196.

Stone, E. F., Gardner, D. G., Gueutal, H. G., and McClure, S. (1983) A Field Experiment Comparing Information-Privacy Values, Beliefs, and Attitudes Across Several Types of Organizations, Journal of Applied Psychology, vol. 68, issue 3 (August), p459-468.

Stonehouse, D. (2003), The Cyborg Evolution, Sydney Morning Herald, 22 March

van der Putte, T., and Keuning, J. (2000), Biometrical Fingerprint Recognition: Don't Get Your Fingers Burned, IFIP TC8/WG8.8 Fourth Working Conference on Smart Card Research and Advanced Applications, Kluwer Academic Publishers, p289-303.

Zahedi, F. (1987), Reliability of Information Systems Based on the Critical Success Factors- Formulation, MIS Quarterly, vol. 11, issue 2, p187-203.

COPYRIGHT