Biometrics – problem or solution ?

Summary

Biometrics are a security approach that offers great promise, but also presents users and implementers with a number of practical problems. Whilst some of these are technical, and possess technical solutions, however difficult they may be to implement, others are social and cultural. Social and cultural barriers are much more complicated to resolve, and need much more thought by would-be implementers as well as the manufacturers and suppliers before they will succeed. Culturally, one size does not fit all, and that may increase the cost and complexity of solutions.

Introduction

For some considerable time now the personal identification segment of the IT security industry has been trying to improve on the use of the identifier and password as the means of authenticating the user of an IT service. The problems of managing password based systems, their weaknesses, and the (now) classical ways of attacking or subverting such systems are well documented and need not be considered here.

Many consider that such simple authentication measures need to be reinforced, and refer to multi-factor authentication, based upon:

- a secret that you know (password);
- something that you have (a token);
- something that you are (a biometric).

In the IT world, probably the most commonly implemented method for token authentication is the SecureID token. (Smart cards for mass transit rail systems and telephone cards are more numerous, although they do not really authenticate the user. Possession of the token authorizes the holder to have a use.)

The introduction of advanced security techniques such as public key cryptography (better known as PKI – public key infrastructure) has increased the need to be able to store secret information (a private key), because a user could never remember a randomly constructed password that long (RSA 2048 would require you to remember a mere 256 characters worth of information and be able to input it reliably!).

The rapid increase in fraud, and in particular credit card fraud, is creating demands for greater security methods than magnetic stripe cards and handwritten signatures offer. This has seen many card issuers issue chip or smart cards which require a password (commonly a four digit PIN) before they can be used. However, these are by no means generally implemented. A spot check on the various cards in my pocket showed only 50% of the various bank/credit cards have chips, whilst none of the others have that facility.

Why move to biometrics?

The principle pressure to move to biometrics comes from two sources: the biometric industry and the finance industries.

The finance industries are continuing to search for a cost-effective means of reducing fraud. If that means can also be used to prove who authenticated the financial transaction, or could ensure that only the authorized individual could make it, then so much the better.

The biometrics industries clearly wish to see their commercial potential fulfilled. Since they form the 'third pillar' of the security authentication process, there is a logical requirement for their services if you need to improve the 'quality' of the security functionality of a system. Exactly how the 'quality' is improved in some mathematical calculation is less clear, although work has been done by the UK security agency CESG to consider how it might be represented.

Overall, however, it is obvious enough that using more than one mechanism to authenticate a user is going to make the system stronger provided that the mechanism is effective and not related to any other mechanisms being used.

Which biometrics?

Biometrics are about measuring specific characteristics of a person, including:

- voice;
- handwriting;
- fingerprint(s);
- face;
- retina of the eye;
- iris of the eye.

In an ideal world you want to choose a characteristic of a person that has helpful measuring characteristics such as:

- unlikely to change;
- likely to prove unique;
- not invasive;
- difficult to copy or steal and reproduce.

If you turn these into a matrix you might get the following results. The measuring characteristics are shown as low, medium, high because not every technique is considered precise.

	can't change	unique	invasive	copy
voice	L	M	L	H
handwriting	M	M	L	M
fingerprint	M	M	L	M/H
face	L	L	L	H
retina	H	H	H	?
iris	H	H	M	?

The desired result is to have H,H, L,L; meaning that they never change, are unique, can be checked without the user feeling they are exposing themselves to any special procedure and are impossible for attackers to copy.

The results of ? for copy are given because at this stage there is little reported evidence of trying to capture and reproduce retina and iris prints, whereas the other techniques listed have been subjected to deliberate attacks with publicized results.

Are the measuring characteristics precise?

Unfortunately when we talk of measuring biometrics we are not talking about the precision of zero or one, but about statistical measures. Samples are taken of the biometric that is being measured, sample points analyzed and compared with information previously captured. This is not, then, the absolute precision that we associate with digital computing, but about matching samples of information to a level that makes us confident that they are identical.

The extent to which we can make the measuring method accurate is related to the degree of invasiveness of the measuring method, both when the initial user measurement is made and when the sample is taken. The more precise the measures are, the more likely they are to give the right result.

One of the hazards of biometrics is that measurements may often have to be made in less than ideal conditions. Voice is measured against both the ambient background (a supermarket, street, sports hall?), signatures may be checked where someone is standing up (sitting down, leaning, poor shaped pen, wet hands), fingerprints taken when the finger is flat (misaligned, wet, dirty) and facial characteristics checked with glasses (sunglasses, no glasses, color of the ambient light). Measuring systems have to allow for all these hazards and still operate acceptably.

Sources of potential error create two measuring levels that biometrics build in to their calculations: false acceptance and false rejection. As these figures imply, the measurement system is set up to allow for errors. Therefore you have to understand that the operation of the system can be ‘tuned’ to be more or less precise. This is not the same thing as either knowing a secret or not, and not the same as whether you have a card in your possession or not. When you implement a biometric system you may have to think carefully about how accurate it can be in operation.

Why does method of operation matter?

The method of operation has two distinct components that must be considered:

- what the person being authenticated must do to use the service;
- what the system operator must do when failure occurs.

The person being authenticated must have registered their bio-identity before it can be authenticated. Registration processes can be extremely complicated and very inconvenient for users. This is particularly true if the user being registered is not familiar with what is happening, why it must be done and what safeguards they have over the use to which their bio-identity might subsequently be put. Registration must try to register the biometric as accurately as possible (with respect to the measuring technique being used) or subsequent comparisons will be poor and may create administrative problems.

Once the person has been registered you have to think about how their bio-identity is checked and what the context is.

It may be socially acceptable to look into a special device for retina scanning to gain access to a highly secure military establishment when it is part of your function. The same may not be true when standing in line at a supermarket checkout. Also, you may not be able to wear certain types of contact lenses.

Similarly it may be acceptable for the police to check your fingerprint(s) when that is required by law but less acceptable to have that demanded to verify a credit card transaction.

Voice recognition may be fine if there is a private booth, or if the verification can be done as part of 'normal' conversation, but less so if special number or word sequences have to be called out loudly in public.

These are social and cultural factors. In some countries or regions they may be acceptable, in others not. Collecting fingerprints may be unlawful in some countries unless you are an authorized government agency. The fact that it may be acceptable in one location does not mean it will work anywhere else, because the users themselves may refuse to behave in a manner that allows the system to work.

Up to now we have been assuming that our bio-identification system is working perfectly, but unfortunately they don't. As pointed out earlier, the information captured during registration may not have been perfect, and the information captured at the point of verification may not be perfect, or may have changed in some way, from how it was presented earlier (ever looked at your passport photograph?).

The presence of false acceptance and false rejection means that some of the time (however small) the right person will be rejected and the wrong person could be accepted. The problem for the operator is that the right person will be rejected occasionally by what might be presented as a 'foolproof' system.

So what procedures does the operator have to put in place to deal with the situation where a perfectly valid user has been refused? Do you go for 'best of three' and do you lock them out after that? Do you have some other test that you can apply, and, if so, what is it? What is the impact on the user – are they a customer that could refuse to use the service again rather than an employee who may not have such luxury of choice. What is the impact on your internal administration in any event, particularly if there is an equipment malfunction that is difficult to detect?

These are not problems for the company supplying the basic product. They are problems that the implementer has got to sort out for themselves. The answers are going to vary significantly according to the business purpose being served by the system, so there's no simple solution here until some good experience has been gained in major pilot exercises.

Conclusions

Biometrics offer a valuable approach to extending current security technologies that make it far harder for fraud to take place by preventing ready impersonation of the authorized user.

However, in order to make use of biometrics we need to register users, a procedure that may be costly, and onerous for users, and we have to have a socially/culturally acceptable means of checking the biometric at the point of authentication. These problems may also give rise to the need for safeguards over the use of the biometric.

In using biometrics we must be aware of the fact that they are not measuring perfectly, and that many operational factors may cause them to fail. In such cases administrative procedures to resolve operational failures may need to be put in place to prevent adverse customer reaction, bad publicity and failures in public acceptability. Whilst these failures may not represent a significant proportion of transactions they will have a 'publicity' effect that is far more damaging that all the success gained by the service. Insufficient information from extensive pilot studies exists at the moment to indicate either how best to manage the situation or tune the service to give acceptable financial or anti-fraud results.