CPNI
Centre for the Protection of National Infrastructure

Biometrics for Access Control

A Guidance Document

September 2014

Disclaimer:

Reference to any specific commercial product, process or service by trade name, trademark, manufacturer, or otherwise, does not constitute or imply its endorsement, recommendation, or favouring by CPNI. The views and opinions of authors expressed within this document shall not be used for advertising or product endorsement purposes.

To the fullest extent permitted by law, CPNI accepts no liability for any loss or damage (whether direct, indirect or consequential and including, but not limited to, loss of profits or anticipated profits, loss of data, business or goodwill) incurred by any person and howsoever caused arising from or connected with any error or omission in this document or from any person acting, omitting to act or refraining from acting upon, or otherwise using, the information contained in this document or its references. You should make your own judgement as regards use of this document and seek independent professional advice on your particular circumstances.

Introduction

This document aims to provide the reader with a brief introduction to biometric technologies in order to aid the decision making process when first considering the use of biometrics. The term biometric technologies refer to automated systems which recognise people based on their bodily characteristics; for example, fingerprints, iris scanning, palm scanning. This document links biometrics to access control, though the technology is not limited to this application.

Are biometrics for me?

Biometric technologies provide an aid to controlling access to a site or space. They should not be used on their own but in conjunction with another access control measure. It should be remembered that they may not be suitable for all applications. Listed below are some key factors to consider when making the initial decision whether to deploy biometric technologies in an access control environment.

- Biometric technologies can automatically recognise people **already known** to the system.
- A program of **'enrolment'** must be carried out before the system can be employed.
- Biometrics **should not** be used as 'stand-alone' systems: rather as part of an integrated access control system. An example might be a fingerprint used with a smartcard.
- Personal information used for enrolment must be verified at time of enrolment.
- The enrolment process can be complex and time consuming.
- Biometrics can operate, if required, without any personal information being stored.
- It is possible to ensure that duplicate enrolments do not happen and to build in anti-tamper which will increase security.
- Biometrics are not infallible, cases of 'false positives' and 'false rejections' are possible.
- Depending on the application, biometrics may increase or decrease the time taken to access a site. This should be considered when selecting the technology. Some methods may be more suitable than others depending on the environment.

Types of biometric system

There are a number of commercially available biometric technologies based on a number of human characteristics.

- Fingerprints
- Iris pattern
- Face recognition
- Finger/palm vein
- Hand geometry
- Voice pattern

A short description of each of these technologies is given below. This is intentionally brief as it is intended as a pointer to the types of technology available. Expert advice should be sought if further information is required.

Fingerprints

This is probably the best known technique. In modern access control applications, users place their finger onto the glass plate of a fingerprint scanner. A light shining from below reflects only where there is a fingerprint 'valley', not a ridge. This reflected image is recorded and stored. Normally two fingers would be scanned per subject. This allows for one fingerprint being damaged.

Iris pattern

The iris has long been recognised as distinctive and individual. Iris recognition devices take a greyscale photograph of the iris pattern using an invisible and harmless infrared light for illumination. By processing the image, a binary code is produced. It is this code which is used for comparison. Although the image can be obscured by cosmetic contact lenses, **standard lenses** cause no problems. Iris recognition systems are accepted as one of the better biometrics techniques.

Hand geometry

Hand shape has long been used as a biometric technology. It requires the hand to be placed on a reflective surface. Illumination from above reflects from the exposed part creating a silhouette of the hand which is captured by the camera. It is the shape of the hand only that is recorded, not the palm print or the fingerprint.

Face recognition

This system uses a digital image of the subject for comparison. Consistency of pose, lighting and facial expression is required. The photograph must also be recent. These exacting requirements make this system difficult to manage in an access control application.

Finger/palm vein

This is a newer technique and involves the imaging of veins in the hand or finger. This system exploits the fact that veins absorb more near-infrared light than other types of tissue beneath the skin. The hand or finger is illuminated with low intensity infrared light which can be imaged with a standard CCD sensor. The light absorbing veins return a dark pattern against the more translucent skin and other tissue.

Voice pattern

This technique uses the voice patterns of a subject for identification. This requires the subject to speak a known phrase. It is this exact phrase that is used for comparison. As yet there are no standards for voice biometric access control systems.

Some important questions

Before a biometric system is implemented there are a number of questions that need answering.

- Will biometrics help? Why are tokens and readers not suitable?
- Is there a business case? Cost? Cost saving?
- Are there any current legal or legislative issues to be considered?
- Will privacy be an issue? What data is being stored and who will have access to it? (Data Protection Act)
- Will PINs and/or tokens be used as well? (2nd Factor Authentication)
- How user friendly will the system be? Will training be required for operators and users?
- What are the risks of false positives and false rejections? (Threshold of approx. 2%)
- What will the usage environment be like? Will CCTV oversight be required? What will the environment be like? Outdoors, light levels, PPE, office, noisy, etc.
- What about people who can't use Biometric systems?

There are numerous questions which will need to be answered before the decision to implement biometrics is made. The question then is what type of biometric technology will be employed. This may emerge from the answers to the above questions based on cost, application, environment and so on.

Not all solutions will be suitable for every situation. The overriding consideration must be usability. If the system is not suitable for the users, then administration issues will make the system unworkable. If it is difficult to use, access times may be extended, access may be denied to authorised people and it may become labour intensive with staff having to resolve problems. This would completely negate the rationale for having an automated system.