

BIOMETRICS: Knowing me, knowing you.

There are about 6.6 billion people on earth and if that seems like a near infinite number, imagine the amount of information each individual holds. This information has to be protected from the 'bad guys' and made sure that those who are supposed to access it, can. How then you ask, are the right people supposed to gain access to such enormous volumes of information in a secure way? The answer – Biometrics. Biometrics allows for identifying and verifying individuals based on their unique physical or behavioural characteristics. Biometrics has rapidly improved the identification process and what at first appeared to be a complicated and futuristic method, has now become commonplace.

Biometrics - A short history

The need to prove you are who you say you are is not a novel idea. Nobles in the middle ages used wax seals to prove that they were indeed the senders of certain important documents and even the poorer folk who could not afford seals used the letters 'xxx' to show that the letters were from a genuine source. Even fingerprinting - one of the most common and most recognised form of biometric processes dates back to China and India 2,000 years ago as a means to seal a contract.

2,000 years later, this need has been transferred to our increasingly digitised society to make it easier for individuals to access information anytime and anywhere. Currently, passwords, Personal Identification Numbers (PIN numbers) or identification cards are used for identification and verification. However, cards can be stolen and passwords and pin numbers can be guessed or forgotten. To solve these problems, biometric technology, which identifies people by their unique biological information, is attracting attention. The icing on the cake in this area is that the person requesting access is required to be physically present at the point of identification. Therefore, biometrics can be used to protect sensitive data, reduce password related problems, and control access to sensitive areas as well as knowing who has accessed what information.

Getting under the skin

So how does it work? In simple terms, a person's physical characteristics, behaviour or habits are registered in a database, so the next time the person tries to access a system or building, the system recognises their characteristics and grants access. The physical characteristics, as the name implies, refers to the unique traits of a certain part of an individual's anatomy. For example, fingerprints, palm prints, iris pattern and vein pattern. Behavioural characteristics are more to do the everyday behaviour of a person e.g. writing patterns, voice patterns and keystroke recognition. This flexibility of biometric solutions means that they can be applied to a range of security challenges when correctly implemented.

Naturally, it would seem that the physical form of identification or verification is the more secure as it will not change if there is a variation in mood, emotion or the environment. For instance, when someone is nervous, their voice pattern is likely to change - perhaps become high pitched or their writing might become a bit shaky, whereas an individual's fingerprint will remain the same regardless of the situation.

Identification or Verification

There has been some discussion as to what part exactly biometrics has to play in the security space. Should biometric processes be used primarily for identification or verification? Both these two different ways can be used to recognise a person but one can be more suited to one industry than the other.

Identification is a process that registers and recognises the characteristics of the people who are allowed to access the system. It is more suited to the airport industry where you only need to be identified as a particular individual to be able to pass through customs and the authorities simply need to bring up your information again if needed.

Verification however, is a process that makes sure people are who they say they are. This is possible because there is already information on the system to which the characteristics are being matched to. This method will be more useful in the medical industry where certain qualifications are required to be able to prescribe certain medications. So whilst you will be identified as part of the organisation, you still need to be verified as having the required authority to prescribe the medication.

Whilst biometrics is generally accepted as a common and reliable security measure, no security system is 100% risk free and like any other security measures, there are limitations to this particular technology. The accuracy of any biometric system can be characterised by two error statistics - a false rejection rate (FRR) and a false acceptance rate (FAR). The FRR is where the system identifies the biometrics measurement of an individual as being from another person, while FAR is where the biometric measurement of two different people is identified as being from the same person. When you think about it, there are a couple of everyday scenarios that can make the recognition process fail. For instance, a dirty hand or a hand scarred by an accident could cause an error in fingerprint recognition. Hair growth, facial expression and aging can also cause errors in facial recognition.

Palm Vein Pattern Verification Technology

So in light of these limitations, which biometric security measure should organisations be adopting? The most innovative biometric technology available at the moment is Palm Vein Pattern Verification Technology. Palm vein verification works by comparing the pattern of veins in the palm of a person being verified with a pattern stored in a database. According to research by Fujitsu, vascular patterns are unique to each individual – even identical twins have different patterns. And since the vascular patterns exist inside the body, they cannot be stolen by means of photography, voice recording or fingerprints, thereby making this method of biometric verification virtually impossible to manipulate or falsify thereby making it more secure than other biometric solutions. These advantages have led to more developments in this area.

Fujitsu has been working on a new technology to identify and authenticate individuals using palm vein recognition. The technology called PalmSecure is a biometric authentication solution offering optimum levels of security, it works by detecting the structure of the veins in the palm of the human hand by emitting an infrared beam which is absorbed by the blood, causing the vein pattern to be revealed. This can achieve a FAR of 0.00008% with a FRR of 0.01%, making it one of the most accurate forms of biometric recognition at the moment. This product has proven popular amongst the

consumers especially in the financial industry, who find it both easy to install and practical to use. Not only does it offer convenience with maximum security and precision but since it is contactless it allows for total hygienic handling which realizes major advantages across a wide range of applications.

Any biometric system should be applicable across various organisations and industries such as healthcare, financial and education. This could mean implementing a system for PC and Web login or an ATM for withdrawing money, cashless payment means in EPOS systems as well as Match on Card applications. In the medical industry, it can be used for access control to stations, laboratories, pharmacies, operating theatres as well as clocking in/out clinical staff. Biometrics can provide a high level of security and confidentiality where traditional options are no longer satisfactory and as technology continues to improve, so will the ways in which we identify ourselves. You have to wonder what unique and wonderful ways will be available in five years.