# *Biometrics – "Approach everything with scepticism"*

Report by Eugene Oscapella

THE INADEQUACIES OF TRADITIONAL identification technologies have created a pressing need to find more effective solutions. The lack of research on biometrics technology, however, means the level of success is still unclear. Organisations which rush to implement biometrics could find that such technology fails to live up to the hype.

"We should approach everything about biometrics with scepticism. Most of what we know has not been validated by research. The scientific basis for claims about biometrics is almost always tenuous." These remarks by Dr James Wayman of San Jose State University set the tone for a detailed workshop presentation entitled "What are Biometrics, and How Do They Work?," held on April 16th at the Twelfth Conference on Computers Freedom & Privacy, in San Francisco.

### Biometric characteristics

Dr Wayman defined "biometric authentication" as "the automatic identification or identity verification of living human individuals based on behavioral and physiological characteristics." Every biometric characteristic, he said, involves both behavioural and physiological characteristics. This definition would include biometrics involving voice, retinal and facial recognition, hand geometry and footprint pressure. Dr Wayman noted that this definition was very similar to that adopted by the International Biometric Industry Association (IBIA).

Biometrics, he said, is not particularly new. It merely represents an attempt to automate systems that have been in existence for well over a century - fingerprints, for example.

Biometric authentication does not include implanted devices – for example, RF (radio frequency) chips, or automatic health screening, such as PSA (Prostate-specific Antigen) tests for prostate cancer. Nor would DNA analysis be considered a form of biometric authentication, since the analysis of the DNA is not yet automatic. Similarly, hair and fibre analysis, and forensic analysis of dead bodies, would not meet this definition.

Biometrics also cannot determine name, age, race, birthplace, health, citizenship, income or gender (although voice prints may help determine gender).

> "When a technology demonstrably does not work, we should not use it."

### Benchmarking problems

One problem in assessing the value of biometrics, Dr Wayman said, lies in the lack of common standards for assessing the security of various biometric and non-biometric measures. For example, there is no scientific evidence that biometrics are more secure than personal identification numbers or passwords because there is no common standard for assessing the relative security of these measures.

### Positive/Negative uses

Furthermore, he cautioned, potential users must be careful to define the purpose of the biometric system. Will the system under consideration do what the client wants it to do? For example, are the biometrics intended for "positive" or "negative" identification?

Positive identification is used to prove that a person is who he says he is. Positive identification can prevent multiple users of a single identity by matching a biometric "presented" by the subject (for example, a hand for hand geometry analysis) with a single stored template (the analysis of the hand geometry stored in a smart card or in a central database). A false match allows fraud. A person whose hand geometry yielded a false match might, for example, be allowed to proceed through immigration pretending to be another person. A false non-match would be inconvenient. A person who encountered a false non-match (that is, a person whose hand geometry is mistakenly identified as different from that stored on a card or in a database) would not be allowed to proceed through immigration.

Negative identification, on the other hand, is used to prove that a person is not who he says he is. Negative identification can therefore prevent a single individual from obtaining multiple identities. This could be used to prevent welfare fraud using multiple identities. The biometric presented by the subject would be matched against all stored templates of biometrics. A negative identification system cannot be voluntary, since a voluntary system would permit an individual to obtain multiple identities by opting out of the system. Under a negative identification system, a false match would be inconvenient, since it would make it appear that the person has attempted to obtain multiple identities. A false non-match would permit fraud, since it would enable a person to obtain a second identity.

Dr Wayman discussed the case of one company that uses finger geometry to prevent multiple users of a single season pass to its entertainment facilities. This use is a form of positive identification – to prevent multiple users of the same identity. However, unlike a national security facility, the leisure company can tolerate a reasonably high rate of detection errors – false matches (saying that the person whose finger was scanned was the true season pass holder, when in fact he was not). Thus, it could rely on a biometric authentication technique that had a relatively high rate of detection errors, such as finger geometry.

And even once a potential client for biometric technology has determined the uses for the biometrics, the problem of false "breeder documents" remains. That is, the document or documents that a person uses to establish an identity may be fraudulent - a forged birth certificate, passport or driver's licence, for example. As a result, even with biometrics, the person being "authenticated" may still be a fraudster. Biometric identification based on breeder documents merely confirms that the person is who he says he is based on the breeder documents. It does not show who the person is in reality.

### PERFORMANCE VARIES ACCORDING TO USE

A further problem with biometrics, said Dr Wayman, lies in the total inability to predict the performance of a biometric technology in one environment based on performance in another. Research showing that a particular technology may work with people who are frequent users cannot be used to support a claim that the technology works with people who are not accustomed to using it. One system may work relatively well when used indoors, overtly and with a knowledgeable attendant present. That same system may fail completely when used outdoors, covertly and without an attendant.

> "If you buy a biometric device, there may not be a company around in two years to service it."

Dr Wayman also explained that biometric systems are vulnerable to pattern, presentation and sensor changes. A change in the retina, for example, represents a "pattern" change that could defeat a biometric system. Changes in "presentation" can also defeat a system. For example, facial recognition systems are vulnerable to changes in facial expression, the wearing of glasses, jewelry, hats, facial hair, lighting, distance from the sensing device, ageing and pose angle.

Differences in the sensors – the devices that scan retinas, faces or fingerprints – may also cause errors.

Still, he argued, facial recognition, which is not yet ready for "prime time" because of its flaws, has a significantly lower error rate than attempts by humans to match photos with the individuals before them.

### UNSTABLE TECHNOLOGY MARKET

Dr Wayman also urged those considering the use of biometrics to consider the half-life of biometrics companies. "If you buy a biometric device, there may not be a company around in two years to service it." Retinal recognition systems may provide an object lesson. There are no commercially available retinal recognition systems now, noted Dr Wayman, although some companies are interested in reviving this technology for commercial applications.

Speaking at the conference the next day, Barry Steinhardt of the American Civil Liberties Union (ACLU) echoed Dr Wayman's cautions about the frailties of biometric technology. He added a note of common sense that may be lacking in our urgent quest for security: "When a technology demonstrably does not work, we should not use it."

What emerged from the Computers Freedom and Privacy conference discussions on biometrics was clear: security is important, but biometric "solutions" may not yet be ripe for use. They involve extraordinary levels of complexity and intrusion, and in the end may give only a dangerous illusion of added security.

*The Electronic Privacy Information Centre has a list of resources on facial recognition technologies: www.epic.org/privacy/facerecognition*

*For information on the US-based newsletter Biometric Digest, see: www.biodigest.com*

*See p.26 for use of biometrics in combating terrorism.*