Towards a new, more acceptable face for biometric security

September 30 2004

Biometric security implies different things to different people. For some, applications that identify individuals based on their physical and behavioural characteristics will lead to a safer and more secure world. For others, they elicit fears of an Orwellian scenario where governments and corporations run roughshod over personal privacy.

In a world where the threat of terrorist attacks, organised crime and lapses in data protection is ever present, however, the use of biometrics is increasingly being seen as the most efficient way to enhance security, whether in airports, government buildings or the local high street. Take, for example, a face recognition system at an airport security check that could prevent known terrorists from boarding a plane, or a fingerprint reader on an ATM machine that would do away with PIN codes and avert credit card fraud.

“Biometrics is a term often used too broadly to describe many different applications and many different technologies at very different levels of maturity,” says Marek Rejman-Greene, a senior identity management consultant at BT Exact.

Rejman-Greene headed a team of European researchers who produced the IST programme-funded BioVision Roadmap, a comprehensive document plotting the course of the biometrics sector over the coming years and identifying the key challenges that lie ahead.

Technological developments are expanding the uses for biometrics and

the range of applications at the same time as making the public more aware. Both the United States and Europe are planning to use microchips to store biometric data in passports, and the US has started to electronically scan the fingerprints of some foreign nationals entering the country in the wake of 11 September 2001.

“These changes are making biometrics more visible to the public,” the BioVision coordinator says. Awareness, however, does not necessarily imply acceptance.

Overcoming fears

One of the principal challenges identified in the BioVision Roadmap is the need to overcome the concerns, or even fears, that biometric systems elicit among some sectors of the population. A certain number of people may feel apprehensive about offering part of their anatomy up for inspection on ethical grounds, others are concerned about the medical effects of recognition systems, such as those that use high intensity light to perform iris scans, and for many the central concern is what data will be taken, what it will be used for and what happens if something goes wrong.

“I think the principal question people are asking themselves is: what would be the worst possible situation if someone stole my iris pattern?,” Rejman-Greene says.

As the BioVision coordinator notes no security system is watertight, and both computers and humans are fallible, which in the case of biometric data could open the door to identity theft, fraud or worse. Increasing the security of biometric systems is therefore essential if they are to be deployed widely and effectively, and also gain public acceptance.

Improving security

“Improving the technology itself to the point where there is virtually no

possibility for misuse would certainly increase confidence in biometrics," says Orestes Sánchez-Benavente, the coordinator of BioSec, an IST project launched last December.

In seeking to address 20 of the 38 research challenges identified by BioVision, the BioSec project is developing methods to improve the security of biometric devices, and the storage and transmission of data. During the course of two years, BioSec will carry out evaluations of best-practice implementation methods, develop scenarios on physical and remote access, create a database on multimodal biometrics for the research community, and produce a combined speaker and speech recognition system. It will also advance several much-needed technologies: 3D imaging and aliveness detection - to ensure an individual is not deceased or dismembered and that a photograph, model or recording cannot be used - and ID tokens as a form of data storage.

"ID tokens could be in the form of a smart card or USB tags containing biometric data that an individual carries around with them to prove who they are," Sánchez-Benavente explains. "The idea is to put biometrics in the hands of users and not necessarily in databases, which is likely to increase acceptance."

Such technological enhancements in the use and protection of biometric data will go someway to waylaying public concerns, but further action is needed if people are to accept having parts of their anatomy turned into mathematical equations and kept on file for inspection. Both Sánchez-Benavente and Rejman-Greene agree that education will be crucial to ensuring the widespread deployment of biometrics.

"People may have rational or irrational concerns about biometrics, but from my own experience the majority of the population would accept such systems if they are informed of how they work, what data is retained, how that information is used and, especially, if they are given

some form of redress if something goes wrong," Rejman-Greene says. "It's a question of providing the public with the right information in the right place at the right time."

He admits, however, that there are other issues that go beyond the question of data protection and 'Big Brother' scenarios. Some members of the population, such as amputees, will never be able to use certain recognition systems, leading to possible social exclusion. In addition, some people are not only concerned about how biometrics systems could affect their health but also what they could reveal about their medical history or their current physical and mental state. A retina scan, for example, could pickup optical problems, while voice recognition could determine someone's state of nervousness or sobriety.

"Though they have that potential, security systems are not designed to gather that information, which some would consider a step too far," the BioVision coordinator says. "Certainly in the EU I don't think it would be acceptable – it all depends on the culture of privacy that exists in different countries."

The need for regulation

In that regard, regulation is crucial. Through the European Biometrics Forum (EBF), the BioVision partners and others are developing codes of practice for system operators and end users so, in the words of Rejman-Greene, "everyone knows what their obligations and rights are."

Launched in June, the BioSecure project is taking additional steps down that road. Participating in the EBF, BioSecure's 30-member network of excellence is integrating multidisciplinary research efforts and evaluation methods with the aim of increasing trust in biometrics. It will address technical challenges as well as standardisation and regulatory questions, which according to Bernadette Dorizzi, the scientific coordinator of the project, are "determinant issues for the future of biometrics."

“Regulation, standardisation and interoperability at the EU and international levels are critical to ensure people become convinced that biometrics is good for everybody in everyday life,” Dorizzi says.

Though common EU frameworks exist in areas such as personal privacy, and health and safety no such legislation yet governs the use of biometrics, which is seen principally as a data protection issue and therefore remains the responsibility of individual Member States. Regulation at an EU level, however, is necessary not only to increase public confidence but also to foment the adoption of biometrics systems by the private sector so companies can be assured that an application they are using in one country is acceptable in another.

Similarly, the development of biometric applications should be standardised so that the technologies are compatible. In turn that would impel their use from a cost-benefit perspective and would ease integration into existing security systems.

“It’s not sufficient to merely replace a password or identity card with iris or fingerprint recognition because the whole system requires important changes, from educating end users to training security guards and integrating it with other elements,” Rejman-Greene notes. “Most importantly, any deployment of biometric systems - be it in the public or private arena - should involve consultation with all interested parties, especially end users.”

In the eyes of BioSec’s Sánchez-Benavente one way to make biometrics more acceptable is to start with deployment in areas where it represents a clear benefit to the population. “The way to go may be to employ biometrics for security in banking, social security and welfare systems, for example, eliminating PINs and passwords, and making it more efficient and secure,” he says.

But will the use of biometric systems ever become as natural as entering a PIN on an ATM machine or displaying a passport at an airport?

For Rejman-Greene the answer is yes.

“I foresee biometrics becoming less prominent and more transparent to the point where people won’t even notice the applications,” he says. “In doing so it will create a more secure environment, one in which people will be able to go around knowing their money won’t be stolen, where travellers will be less restricted and everyday life will become simpler and more efficient.”