Biometrics under the microscope

Biometrics seem so simple and intuitive that the question sometimes arises: couldn't we just replace all our current authentication gadgets with a fingerprint reader or face scanner? Sadly the answer is no, for reasons that become apparent when we take a closer look at biometric technologies.

No biometric today provides lasting signatures on electronic transactions. Biometric security is much more focused on access control – to secure data centres or to log on to computers – than transaction authentication. Even if used for logon, a biometric doesn't let you "leave your mark" on the transactions you later create. For this reason, external consultants looking at the requirements of electronic prescribing for example have recommended PKI over biometrics (and all other authentication options). Biometrics just don't meet the business needs of paperless applications like electronic health records, medical referrals, government forms, customs declarations, trade documentation, business banking and so on.

Significant security concerns bedevil biometrics. Spoofing fingerprints especially is quite straightforward; latent fingerprints left behind on objects – especially fingerprint readers – can be lifted off with sticky tape, reproduced in fake gelatine fingers and used to fool a majority of readers on the market. All good biometric readers must have "liveness detection" to tell fake body parts from real ones, although this raises the cost of commercial devices.

Biometric devices are not perfect. Even if individuals' biometrics were intrinsically unique,[1] the ability of real world commercial devices to measure them flawlessly is limited. Lenses (and bodies) get dirty, lighting varies, body parts age and scar, and each time get presented to the scanners in subtly different ways. Therefore, every biometric system commits errors. They can confuse one user with another (a so-called False Positive) or they can fail to recognise an enrolled user at all (False Negative). The very best technologies have False Positive rates of around one in a million, which is a worry for mooted national security applications. But typical error rates are more like one in a *hundred* or worse, which has an impact in even small scale usage.

It is difficult (if not impossible) to revoke a biometric and issue a new one, in the event it is compromised. In contrast, one of the best security features of smartcards and most other authenticators is they can be cancelled and replaced if lost or stolen. No security system is perfect; all good security systems need fallback mechanisms, but for biometrics there are none.

Biometrics suffer significant performance concerns especially in large scale deployments where users must be matched against big databases. Tests were conducted by the UK Passport Office in May 2005 on over 10,000 people using fingerprint, face and iris technologies. Average verification times were 39 seconds for face, 58 secs for iris and 73 secs for fingerprints. Accuracy was disappointing too: success rates were 96% for iris, 81% for fingerprints, and 69% for face. Reference: http://europa.eu.int/idabc/en/document/4333/194.

Biometrics are not really mature technologies. Different vendors use different algorithms; biometric scanners & software applications do not interoperate across manufacturers. Single vendor solutions for the whole enterprise are usually mandatory, and migration to alternate suppliers is difficult. Many algorithms have only just come out of the R&D lab.

Biometric scanners represent an extra cost per workstation, especially for the more sophisticated devices with "liveness" detection.

Enrolling users and recording their biometric templates needs to be done locally. No central body today is set up to biometrically enrol large groups of users in an open e-business environment. Nor is there a business process to do so; it would be hugely more intrusive and cumbersome than the 100 point check done in the past for old fashioned PKI certificates. National bodies are now in a position to push out digital credentials to known doctors, lawyers and other professionals, but not if they all have to come in and have their biometrics registered as well.

However, decentralising enrolment means biometric identities have limited scope. A biometric only validates your identity to someone *who already knows you*. Nobody outside the local environment can recognise a biometric, unless they have access to the "templates". Disseminating biometric templates while protecting them from eavesdropping or theft is a major challenge. In practice, biometrics tend to be limited to local access control applications for relatively small groups of enrolled users; they are not suitable for large scale or "global" authentication of digital credentials as required across healthcare, government, the law and other sectors, nor across international borders.

[1] There is in fact an emerging body of analysis that suggests fingerprints may not actually be unique; see for example http://www.hup.harvard.edu/catalog/COLSUS.html.