Security as far as the eye can see

by STEPHEN WILSON

How often is a serious new technology introduced to banking executives with the aid of a Sean Connery or Tom Cruise film clip?

Welcome to biometrics, the glamorous end of the security market, where *Diamonds Are Forever* and *Minority Report* have almost achieved case study status. But beneath the hype of biometric identification are some more pragmatic issues for their application in day-to-day banking.

In this issue, I'll look at some of the claims, and discuss real-life performance indicators that really matter, like throughput and the length of the queue at an ATM.

For years now, biometric scanners have safeguarded many institutions' data centres, recording the eyes or digits of trusted personnel and ensuring that only those with the right retina scan or fingerprint can gain access. For small numbers of people, in technical positions where they can tolerate painstaking protocols and regular re-tries, biometric access has proven very effective.

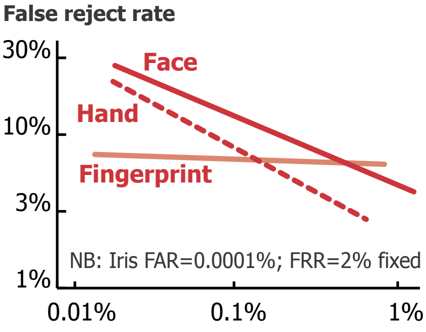
Bigger rollouts are now under way in factories and offices for time and attendance recording. There is talk of large-scale deployments just around the corner, where millions of people would be registered for biometric passports.

So what about the promise of the biometric ATM, where any banking customer could stare into a camera to gain access to their account? At this stage, the real-life performance of biometrics in million-plus populations remains unclear.

Fifteen months ago, the US General Accounting Office (GAO) reported on the feasibility of biometrics for national security. They concluded that the "performance of facial, fingerprint, and iris recognition is unknown for systems as large as a biometric visa system".

Biometrics vendors often try to distinguish themselves on the basis of how unlikely it is for two people to share a particular body feature. Some characteristics differ even between identical twins, with the implication that this makes for a superior technology. But crucially, the complex imaging, measurement and number crunching sub-systems needed to convert biological features into authentication data are not infallible.

Biometric imbalance



Source: Biometric Product Testing Final Report (www.cesg.gov.uk)

One manufacturer claims that the chance of two people having the same iris pattern is one in ten to the power of 72. This is indeed a mind-boggling figure. It's vastly bigger than the number of grains of sand in the world. But is it a true reflection of how an iris scanner performs in real life?

Consider this analogy. There are 10 billion stars in the Milky Way. If you and I were to each pick a star at random, we might think that the odds of us picking the same star is one in 10 billion. But looking up at the night sky, using the naked eye as our "scanner", it's really no better than one in a few hundred.

So no matter how good a biometric might be in theory, its real-life performance is always limited by the apparatus. This means that any biometric system exhibits two types of error.

1. A *False Negative* is when the system fails to recognise someone who is legitimately enrolled. False Negatives arise if the system cannot cope with subtle changes to the person's features, the way they present themselves to the scanner, or slight variations between scanners at different sites.

2. A *False Positive* is when the system confuses a stranger with someone else who is already enrolled. This may result from the system being rather too tolerant of variability from one day to another, or from site to site.

False Positives and False Negatives are inescapably linked.

If we wish to make a given biometric system more discriminating – so that it is less likely to confuse strangers with enrolled users – then it will inevitably give legitimate users a harder time, tending to wrongly reject them more often.

A design decision has to be made when implementing biometrics as to which type of error is more tolerable.

The diagram *(left)* shows test results from one of the most reputable biometric test programs to date, undertaken by UK government defence specialists.

In typical security applications, the FRR is significantly higher than FAR, because it is sensible to err on the side of false rejects. Less damage generally arises from occasionally asking a legitimate user to try again, than from letting an impostor through a border control gate or into a nuclear missile silo.

But for an ATM, it is harder to ignore the effect of false negatives. Each time a legitimate user is denied access to their account, not only does customer satisfaction suffer, but everyone behind them suffers too as the queue grows longer.

Another crucial performance indicator is throughput, or the time taken to process each individual's biometric.

In one of the most significant live biometric trials to date, Disney World used a type of hand scanner to automate access to the park for their season pass holders. Their target throughput was five seconds per person, but their best performance after 18 months work was just over 10 seconds (down from 30 seconds at the start of the trial).

The UK Government has found similar processing times of 10 seconds for fingerprint and hand, with 12 seconds for iris and 15 seconds for face scanners.

These figures are all considerably longer than the time taken to enter a PIN.

In high demand ATM installations, where we might expect throughput of one or more customers per minute, waiting time in the queue is very sensitive to processing time. An extra 10 seconds per transaction can double the time spent in the queue; 15 seconds can triple it. And this is without factoring in the extra delays incurred through false rejects and consequential re-tries.

It's true for all new technologies, but for biometrics especially, it's important to go in with your eyes open!

■ **Stephen Wilson is a leading international authority on identity management and information security. He offers independent advice and management consulting on authentication, e-businesss risk management, privacy and security strategy.**

stephen_g_wilson@hotmail.com