Supplement

Scanning the horizon

The International Organisation for Standardisation (ISO) has published a new standard that stipulates the security requirements for the implementation and management of biometric authentication technology within the financial services industry. The ISO 19092 standard describes the security framework for using biometric technologies, such as fingerprint scans, voice identification, iris images and facial scans. It covers the authentication of employees and customers in the sector, as well as the management and protection of biometric data throughout the enrolment, transmission and storage stage, while also covering verification, identification and termination procedures.

"ISO 19092 offers a valuable international consensus-based tool to the financial industry that will encourage the secure implementation of biometrics as an authentication method within this sector," claims Mark Laukin, chair of the ISO subcommittee that developed the standard. "It paves the way for the next generation of safer, more reliable financial transactions, which are increasingly important in today’s electronic era.”

Several factors are conspiring to increase interest in biometric technologies at the moment among banks and insurers. In addition to the ISO standard, there are the recent data loss incidents in the UK, where Skipton Financial Services and others have lost laptops, some of which would have been less worrying if there had been internal biometric data access control procedures in place. The growing problem of e-commerce and online fraud is also becoming more troublesome.

This is the real incentive to deploy biometrics – namely, to cut down on fraud throughout the banking system. For example, chip and PIN achieved significant cuts in ‘cardholder present’ fraud in the UK, but these gains are rapidly being offset by even bigger losses over internet and telephone transactions where the cardholder isn’t present, meaning that it may be time to upgrade to stronger authentication involving biometrics. Furthermore, developments such as the RBS and Payment Scheme, introduced in May 2007 to make settlement times for inter-bank payments almost instantaneous instead of taking up to three days, are putting more pressure on banks to deploy accurate robust authentication. Recently introduced anti-money laundering guidelines, which put the onus more on individual banks to safeguard the monetary system rather than follow a tickbox exercise, are having the same effect.

The counter-argument, of course, is that biometrics aren’t yet 100% per cent accurate, can be expensive and the general public doesn’t seem to like them, as the opposition to the UK government’s ID card scheme and biometric passports illustrates.

What are the options?

Authentication can be accomplished via one or more of three factors – something you know, something you possess, and something you are (i.e. biometrics). At present most online banking relies just on the first factor, something you know, such as passwords or PINs. It has become clear for some time that this system is inadequate for global e-commerce, and that a second factor is required. In principle an authentication system could combine all three factors, but in practice the first factor, something you know, is likely to be augmented by just one other factor, which should provide sufficiently strong security. The choice therefore is between the third factor, biometrics, and the second, which could be a smart card or token. Both have their pros and cons, and both require a significant investment and logistical effort to deploy across the whole population.

"The need to capture data from and distribute readers to every potential user is the main hurdle biometrics has to overcome," says Paul Meadowcroft, head of transaction security at the vendor, Thales. “Cards and tokens also face challenges though that might actually give biometrics the edge. They do not have the costs associated with managing lost or missing tokens, for instance, or the need to reset forgotten PINs and so forth.”

But there are two challenges that apply just to biometrics. One is the incidence of false acceptances and rejections, which can never be totally eliminated because the authentication process is in essence statistical, involving comparison between the data extracted when a person attempts to access the system, and the stored representation of the same biometric. These will never be absolutely identical, because they depend on factors such as accuracy of the capture process. By contrast the other factors of authentication do not normally suffer from false acceptances or rejections, at least not to the same degree.

The other issue is the potential to break biometric systems by replay attacks, whether that is by capturing somebody’s stored image data – or, more gruesomely, a severed hand/eye – and feeding it into a system to gain admission. However, that risk is one of perception rather than reality, claims Neil Fisher, vice president of identity management at Unisys.

It is possible to implement biometrics in such a way that the danger of the digital image being stolen is virtually eliminated, agrees Jim Fulton, vice president at DigitalPersona, which specialises in fingerprint authentication. This is done by not

Philip Hunter examines the arguments for and against biometric technology and wonders if the new ISO 19092 standard will help its adoption in the financial services sector.
storing the actual images at all but instead data derived from them. "Biometric solutions such as ours specifically avoid storing actual images of fingerprint," says Fulton. "Instead they compute a mathematical representation that is then encrypted and can only be used for its intended application." Theft of this data then would only compromise one particular system and even that could be made secure again simply by changing the formula used to derive the mathematical function from the fingerprint. As to severed hands or the like a simple blood heat test should prevent this outlandish theory.

The most widely used categories of biometrics so far have been facial, fingerprint, and iris scanning technologies, says Unisys’ Fisher. But two emerging contenders are voice recognition, and vein structure analysis, which have the advantage of being relatively unobtrusive and more natural to use than some other biometric methods, such as iris scanning. Fujitsu decided to use vein technology for its biometric system called PalmSecure, partly because it just requires users to rest their palms briefly on a scanner, which could be located conveniently beside the keys or buttons of an ATM for example. “The key feature is simplicity and ease-of-use,” notes Fujitsu Europe’s technical director, Tim Wright. "Palm vein technology can be easily adapted to fit a range of security and identification solutions without compromising accuracy.” But Wright admits that vein technology is not the best solution for all applications, and that no one biometric type will probably ever come to predominate.

In call centres, for example, there is a strong case for voice recognition technology because people are talking anyway so it does not impose any extra burden on the user and fits naturally with the application. Indeed as Unisys’ Fisher points out, voice as a biometric dovetails particularly neatly with first factor authentication, because the something you know will be spoken into the phone. “It’s worth noting that voice stress analysis is currently being used by call centres to authenticate you are who you say you are. For instance, callers are identified according to the way they say their mother’s maiden name, rather than the name itself,” says Fisher. ABN Amro, soon to be part of Fortis, is using this type of voice biometric in its retail banking operation in the Netherlands.

Fingerprints
But for mainstream banking applications, fingerprinting has been the most successful biometric up until now, having been deployed widely, for instance, in Japan to ensure authentication at ATMs. One issue here though lies in keeping the scanners clean given the rapid accumulation of grease from fingers. However, fingerprint technology has proved pretty robust in being able to cope with impaired images, as has been found in one of its first deployments at Banco Azteca in Mexico. The bank deployed Digital Persona technology at 850 of its branches, where it is used to authenticate account holders who can then view balances, track transactions, withdraw cash, transfer funds, and exchange currency.

“One initial concern was over the state of some of the customers’ fingers,” says Pedro Partida, one of Banco Azteca’s directors. “Many of our customers are farmers or manual workers whose fingers are damaged or worn but the technology has proved more than capable so far and has been able to authenticate even the most difficult fingerprints.” Currently 1.2 million customers have been biometrically registered, with 20,000 using the system every day, with a 97 per cent success rate on the first try.

This brings us back to the other issue with biometrics, which is that of success rate. For online applications, a higher success rate would be needed than say in a bank branch where the system can be supervised. The problem is that, as Thales’ Meadowcroft notes, “biometrics always have this ‘grey area’ of problematic acceptance that PINs and tokens do not have; they are either right or wrong [and there’s no staff to sort out disputes].”

As a result biometric systems have to be implemented carefully to achieve the right balance between false positives and negatives. Usually it is most important to cut down on the false acceptances, at the expense of having rather more false rejections. However, because too many of the latter would jeopardise user adoption, this Achilles heel of biometrics is the focus of much research and there are some claims of results in this area. “Our PalmSecure system can achieve a False Acceptance Rate of 0.0008 per cent with a False Rejection Rate of just 0.01 per cent,” claims Fujitsu’s Wright for example. However this is not the whole story, because that high level of accuracy can only be achieved on a small scale. “Improvements in matching techniques and algorithms to realise highly accurate rapid identification on a mass scale will though continue to be a focal point for development,” insists Wright.

It can be seen then that biometrics is still a work in progress but has attracted to the point of being suitable for some applications, as at Banco Azteca in Mexico. The arrival of ISO 19692 as an international standard defining best practice for implementing biometrics and securing the data may encourage increased rates of adoption by banks, in preference to secure cards or tokens, but at this moment in time it is too early to say so with any certainty.