Biometrics Under the Microscope

Looking forward to getting rid of your passwords? Well don't get too excited – fooling some biometric devices is breathtakingly easy

BY STEPHEN WILSON

The expression "the devil is in the detail" applies to biometrics like no other security technology today. Biometrics appear profoundly simple in operation, but the associated science, engineering and product design are still in their infancy. It is tempting to think that using an ATM of the near future will be as simple as staring into a camera lens to activate one's account, but if we take a close look at this technology, it's not as simple as it first appears.

The typical lay person has come to believe that biometrics are as simple as scanning their hand or face, after which the computer looks up a database, and instantaneously their identity pops out. Unfortunately, the reality of biometrics is rather more nuanced.

There is a sort of innate optimism about biometrics based on common ideas about the uniqueness of personal traits. It is lore for instance that fingerprints are unique. However, a number of criminal prosecutions based on fingerprint analysis have recently been over-turned on appeal. The very foundations of fingerprinting are therefore being re-examined; it turns out that nobody has ever proven the doctrine that no two fingerprints are alike (see *http://fp.bio.utk.edu/evo-eco/resources-this_semester/Cole-fingerprints.pdf*).

Even when biometrics are biologically unique, we must remember that cameras, scanners and microphones – like human eyes and ears – are imperfect. The ability of a biometric authentication system to distinguish between subtly different people is limited by the precision of the technology.

Let's look at the claim by one supplier of iris scanners that the probability of two individual iris patterns matching is one in ten to the power of 78. These are literally astronomical odds; there are fewer atoms in the universe than this! But this figure doesn't tell us how sensitive the end-to-end security system really is.

Consider the fact that there are about 10 billion stars in the Milky Way. If two people look up in the night sky and each pick a star at random, is the probability of a match one in ten billion? Not at all, because our apparatus – in this case the naked eye – is not perfect, and we're always plagued by interference, especially in the big city.

Evaluating biometrics...

- **Check with candidate vendors how their security systems support revoke and re-issue if a biometric is compromised**
- **Consider identity theft from latent fingerprints left around retail environments, including lost and stolen cards; insist on "liveness detection" in any fingerprint scanner to avoid being spoofed by replica fingers**
- **Look at measured performance on Failure to Enrol as well as the more typical False Detect and False Reject rates; sometimes the enrolment rate is traded off to improve accuracy by ensuring users have "good" body parts**
- **Have a contingency plan for those customers who cannot be enrolled.**

So given the interplay of camera resolution, variability in lighting and head position, and other practical factors, the actual false accept rate of iris scanners is typically measured as no better than 0.0001 per cent. Tellingly, this is trillions of times worse than one in ten to the power of 78.

Large scale, real world biometrics testing was performed by the UK Passport Office last May (see *http://www.identitycards.gov.uk/library/UKPS_Biometrics_Enrolment_summary.pdf*).

Over 10,000 people (including 750 disabled persons) were tested on each of three different technologies: fingerprint, face and iris. The results were sobering. The average verification times measured in that trial were 39 seconds for face, 58 secs for iris and 73 secs for fingerprints. The average times for disabled participants were longer: 63 secs for face, 78 secs for iris and 80 secs for fingerprints. In banking applications, especially ATMs where queue length is critical, this type of performance would be problematic.

But the bottom line in security is surely accuracy. The measured success rates in the UK Passport Trial were 96 per cent for iris, 81 per cent for fingerprints, and 69 per cent for face.

No doubt biometric technology will continue to develop rapidly, and these performance figures will improve over time. It's a lively area for R&D, with cutting edge work being done in many different university labs on hybridising multiple biometrics to improve accuracy (if not cost and ease of use).

However, an inescapable problem remains: biometrics are far from immune to identity theft. Worse still, there is no way to revoke and re-issue a biometric ID in the event it is compromised.

In 2002, a German popular electronics magazine bench-tested a host of low price biometric systems, aimed at the small office/home office market (*http://www.heise.de/ct/english/02/11/114*). They found most of these devices were almost comically easy to thwart. Some face and iris scanners could be tricked by photos; some fingerprint readers were readily made to trigger on the latent print left behind by the last user simply by breathing on the sensor. While these results are not typical of more expensive products, they do illustrate how biometrics are vulnerable to identity theft. More serious vulnerability assessments have been conducted. Japanese researchers have found that 80 per cent of fingerprint readers were susceptible to attack using replica fingers made from Gummy Bears! (see *http://cryptome.org/gummy.htm*)

Disaster recovery and contingency planning are the mainstays of good security practice. It is axiomatic that no system is ever 100 per cent secure. Therefore, acceptable levels of holistic or system-wide security are always based on contingency plans to cope with the event of a critical breach, even where the likelihood of a breach is thought to be low. The only way to recover from a customer's biometric ID being stolen would appear to be to fall back to conventional authentication, like name and password.

Stephen Wilson is a leading international authority on identity management and information security. In early 2004, Stephen established Lockstep Consulting to provide independent security advice and to develop new smartcard solutions to identity theft.

swilson@lockstep.com.au