Biometric ATMs

Stephen Wilson
Online Banking Review column No. 34
March 2009

I'm prompted to write once more about biometrics for two reasons. Firstly, the FBI in January released an exhaustive 249 page report, *State-of-the-Art Biometrics Excellence Roadmap* ("SABER").[1] It's a veritable encyclopaedia, invaluable in a field where independent analysis remains relatively rare.

Secondly, I came across a blog recently that advocated biometric ATMs. It contained a reference to the film Minority Report, *as if it were a case study*.

Huh? Minority Report was a movie, not a proof of concept! And if we want to take it seriously, it's a cautionary tale, showing ways to spoof the biometrics and get a jump on those who have become complacent about purportedly perfect security.

Perfection is implied in the way people talk about biometrics. For instance, former US Homeland Security chief Michael Chertoff has flatly stated that "your fingerprint is unique". Some researchers actually think that's a myth but even if it were true, no real life fingerprint scanner has the precision to tell all people apart all of the time.

Biometrics certainly have their place in security. Without question they provide powerful access control at sensitive facilities like data centres. Yet these are special cases, where only a small set of personnel are enrolled. And because it's a mission critical work function, data centre operators are tolerant of scanning delays and retries. Retail banking is very different, and it's not clear that any biometric is ready to roll out to large numbers of consumers.

Without exception, all biometrics commit occasional errors, sometimes confusing you with someone else in the database (a false match) and sometimes failing to recognise you at all (a false non-match). So in practice, "uniqueness" is *never* realised.

Is this nitpicking? I don't think so when we're talking about security, since the main thing anyone needs to know is that no security is perfect. Abuse of the term may give a false sense of confidence. It just doesn't gel to claim that a certain trait is "unique" while real life performance of the biometric system falls well short of 100%.

False matches and false non-matches are sadly unavoidable. Every biometric system takes its measurement with a sensor of some sort, such as a microphone, camera or scanner. Sensors and body parts alike suffer wear and tear; they inevitably deteriorate, get dirty and damaged, and otherwise vary from one day to another. No two scans of the one person will ever be exactly the same, and the greater the time that elapses between scans, the greater the margin for error.

---

[1] The report is available at the FBI Biometric Centre of Excellence: http://www.biometriccoe.gov/SABER/index.htm.

False match and false non-match are polar opposites: to improve either of them, the other must suffer. It's easy to see why. A biometric might be tuned to be very "specific" so that it is good at distinguishing different people, but because the same person scans differently from day to day, such a system is prone to false negatives. On the other hand, a very "sensitive" system will be tuned so as to recognise the same person under a wide range of conditions, but then it will be prone to false positives.

Balancing false negatives and false positives in an ATM or an e-commerce system is a tough trade-off. It can come down to this difficult question: Is customer convenience or security more important?

Recent experience in the Netherlands with a fingerprint based payment system shows how hard it is to get right. After a six month trial involving just 500 customers, "Tip2Pay" was shelved by the Albert Heijn supermarket chain, due to fraud concerns.

New biometric technologies are continually emerging. In ATMs, "vascular" technologies are making in-roads, where the blood vessels of a finger or the hand are imaged using infrared cameras. These features are much harder to spoof than fingerprints, and they may be more socially acceptable than face and iris recognition. Some marketing for vascular biometrics claims false positives of one in a million and false negatives of one in ten thousand. These are impressive figures indeed, but they cannot be achieved simultaneously. Independent testing by the International Biometrics Group in 2006[2] showed that when false positives are reduced to one in a million, false negatives run at 19% (one in five). And they showed that the best case false negative rate was in fact 0.4% (one in 250); the corresponding false positive rate was 2.5% (one in 40).

Standardised testing of biometric performance remains elusive. The FBI in its SABER report cautions that: *"For all biometric technologies, error rates are highly dependent upon the population and application environment. The technologies do not have known error rates outside of a controlled test environment."*

What's worse, almost all biometric testing is based on the "Zero Effort Impostor" assumption, and looks only at accidental false matches. That is, the testing assumes that no impostor has made a special effort to fool the system. The FBI warns that lab results do not reflect resistance to deliberate attack: *"When a dedicated effort is applied toward fooling biometrics systems, the resulting performance can be dramatically different."*

In other words, the stated performance specifications of biometrics solutions don't necessarily tell us how well they stand up to criminal attack. Resistance to robbery is surely important in ATM security, and so the leap from laboratory to the High Street needs to be taken with great care.

About the author

Stephen Wilson is a leading international authority on identity management and information security. He founded the Lockstep Group in 2004 to provide independent security advice, and to develop new smartcard solutions for web security and privacy. Contact swilson@lockstep.com.au.

[2] See http://www.biometricgroup.com/reports/public/reports/CBT6_report.htm.

