Comment and analysis

Expert views on the latest developments

This month: Angela Sasse on the vulnerability of biometric security

"Biometrics are not a security panacea that will single-handedly wipe out all terrorism and crime"

Work is about to start on the 2012 Olympic Park in London – probably the first building site in Britain to use biometric screening. Each morning, builders turning up for work will have their faces and a hand scanned to make sure only authorised employees can walk through the security barriers. And it's not just the Olympic site – biometric tests are springing up everywhere. The UK Home Office operates mandatory fingerprint checking of all visa applicants as "a first line of defence against illegal immigration". In the US, biometric equipment has been installed at 116 airports, 15 sea ports and 154 land ports of entry. And in the future, the UK Identity and Passport Service will capture the face and fingerprints of anyone applying for a passport or identity card.

The use of biometric systems – the most common being face, fingerprint, hand and iris recognition – has many ardent supporters, who argue that biometrics significantly improve security. Their unique selling point is that they provide a 'strong proof of identity' – whether a person is who they claim to be. With old-style passports, a person looking to enter the country illegally could use a passport of anyone who looked roughly the same. With a biometric passport, a border officer can verify that the fingerprint on the passport matches the fingerprint of the person presenting it. That, surely, is a good thing. But biometrics are not a security panacea that will single-handedly wipe out all illegal immigration, terrorism, organised crime, and benefit fraud.

Fingerprint readers can be deceived

Biometrics have vociferous critics, invasion of privacy being the most common objection. BAA planned to fingerprint all passengers (some four million a year) using Heathrow's new Terminal 5, but had to hold off when the Information Commissioner's Office – roused into action by privacy campaigners – announced that this might constitute a breach of the Data Protection Act. Other biometric schemes are likely to provoke similar protests in the future.

Of even greater concern is the fact that biometric tests do not guarantee security as some of their advocates make out. A key problem is that, to detect a terrorist or criminal, you have to know they are one. If you don't know Carlos the Jackal is a terrorist, and he turns up with a biometric passport that matches his fingerprint, he'll go undetected. Even if Carlos the Jackal is known to be a terrorist, he might obtain a passport that matches his fingerprint under the name 'John Smith'.

Biometrics can also be spoofed. Carlos the Jackal might kidnap John Smith, take his passport, and make a silicone copy of his fingerprint. In the movie *Gattaca*, Ethan Hawke's character uses this technique to assume the identity of the character played by Jude Law; in the real world, it has been shown that fingerprint systems can indeed be fooled by someone putting a silicone layer with someone else's fingerprint over their own. Most famously, a Japanese computing professor melted down Gummi Bears to make a fake fingerprint that successfully fooled a high-end scanner. And the Chaos Computer Club in Germany recently included a silicone 'sticky finger' in its magazine with the fingerprint of the German Home Secretary, Wolfgang Schaeuble. They had lifted the print from a glass. Schaeuble was unimpressed, arguing he had "nothing to hide, after all", but the point is clear: any systems – say, a perimeter access control system – that simply check that the fingerprint presented matches one in the database are vulnerable to this sort of attack.

The problems don't end there. The match between the registered biometric and the one presented for checking can only ever be an approximate one. There are many reasons why a legitimate user's biometric might not be recognised as a match: lighting conditions can affect face and iris capture, a finger may be placed in a slightly different position, the reader may be too dirty to distinguish ridges.

Putting biometric readers everywhere will not improve security – the bad guys will find a way round them and many ordinary people will be inconvenienced. Any security system has to be carefully matched to the security threat, and needs to be able to work well enough for real people in the real world.

Professor Angela Sasse is a UCL security specialist and was an advisor to the national ID card enquiry

ALAMY X2, REUTERS, REX, AP/PA PHOTOS