ARRAY Logo

icon

Identity verification over the Internet - A new approach

By Nick Collin
Independent Management Consultant
www.ncollin.demon.co.uk
nick@ncollin.demon.co.uk

Nick Collin is an independent management consultant, based in the UK, who specialises in banking technology, particularly e-commerce applications. He can be contacted by telephone on +171 833 8765.

Abstract

Verification of identity over the Internet is becoming a big headache. Passwords and PINs are almost impossible to remember and their security leaves a lot to be desired. Biometrics are expensive and can easily be compromised when used over the Internet. Smart cards are promising, but require passwords or biometrics to bind the card to the user. Applications such as Internet banking which may only be used occasionally are particularly vulnerable to these problems and this may be constraining widespread adoption. A new approach called Passfaces based on our remarkable ability to remember and recognise randomly assigned faces seems promising and is well worth checking out.

Identity verification – proving we are who we say we are – is an age-old problem. Passwords, PINs, signatures, and fingerprints are all solutions to the problem, but none are perfect. The explosive growth of electronic commerce – doing business over the Internet – has added a new urgency to the search for a better solution, and a small UK company called ID Arts with a product called Passfaces has come up with an intriguing new approach.

All methods of verifying identities depend on one of three things: "something we know" (such as passwords or PINs); "something we are" (such as fingerprints or signatures); or "something we have" (such as a smartcard or token).

Passwords, PINs and other "things which we know" are the most commonly used methods of user authentication for Internet applications such as on-line banking. Unfortunately, most people have great difficulty remembering passwords and PINs and this is bad news both for service providers and their customers. Firstly a service which is difficult to use is simply not likely to be successful. Secondly, because people find passwords and PINs so difficult to remember, most of us write them down somewhere, which compromises security. Thirdly, securely re-issuing passwords and PINs to customers who have forgotten them is a significant administrative overhead which costs money.

As the number of password protected services on the Internet proliferates, so the problem gets worse. A typical Internet user these days is expected to remember 20 or 30 passwords for accessing banks, Internet Service Providers, technical support sites, corporate intranets, and a variety of subscription services, many of which are only used occasionally.

Clearly, there has to be a better way.

One alternative is to use some form of biometric – "something we are". A great deal of research has been done to develop verification systems based on fingerprints, iris scanning, patterns of blood vessels in the retina or hand, voiceprints and the like. All these systems suffer from the disadvantage that special equipment is required. This costs money - to buy, to install and to maintain. There are other problems with biometrics. Users generally regard most methods as unpleasantly intrusive or as having criminal connotations. There is a lack of standards. By their very nature there will be a proportion of "false rejections" which will upset bona fide customers. But perhaps the biggest problem is that biometric data is inherently public and can be used to impersonate the real owner unless he or she is physically present. Once the biometric has been captured in digital form it can be copied and used fraudulently quite easily. And once compromised, a biometric cannot be changed! This is less of an issue on closed networks such as a departmental local area network, but for remote authentication over the Internet it becomes a serious threat. Biometric privacy is becoming a hot issue – the International Biometric Industry Association recently recommended a standardised set of "privacy principles" – but unless biometric data is always encrypted and its distribution very carefully controlled, it is difficult to envisage how it can safely be used for widespread identity verification over the Internet.

What about proof of identity based on "something we have"? There is little doubt that smartcards or other tokens which contain digital signatures will become increasingly common. Not only are these devices an extremely secure method for identification and verification, but they can also be used to digitally sign electronic documents, a prerequisite for many types of commercial transaction. But unfortunately, smartcards are easily stolen or lost – possession is not a guarantee of ownership. Consequently, most smartcards can only be used in association with a password, PIN, or biometric. In other words, we're back to where we started!

The ID Arts Passfaces solution is based on "something we know" but also has the characteristics of "something we are". It turns out that the human brain is amazingly good at recognising human faces - millions of years of evolution have seen to that. Passfaces exploits this innate ability. The way it works is as follows. We choose and memorise typically four "passfaces" from a library of anonymous photographs. In order to log on to a service, we are presented with, typically, four screens of nine faces, each containing one of our passfaces. We prove our identity by clicking on the faces we recognise. It's as simple as that. Note that we are not required to identify faces, which is difficult, just to recognise whether we've seen them before.

Passfaces has several advantages:

- Faces are much easier to remember than passwords or PINs. In fact they are very difficult to forget. In a recent trial conducted by ID Arts, 100% of users managed to gain access, even users who did not use the system for a month after enrolment.
- Faces are also very difficult to "write down" or to "give away" to other people. This improves security and reduces subscription fraud.
- No special equipment is required. Compared with biometrics, Passfaces is simple and inexpensive.
- The system is intuitive, fun to use, and a natural fit with the visual nature of the Internet.

The ID Arts stated mission is to establish Passfaces as the de facto standard alternative to passwords and PINs on the Internet. Why not test it out yourself on their website at www.id-arts.com?