State Of The Market: Biometric Security

If you're looking to replace or supplement login passwords with additional technology, there are many routes that you can take.

By Robert Schifreen

It's an accepted fact in IT security that there are three ways to authenticate someone and to prove that they are in fact who they claim to be. These are: something you know; something you have; something you are. Passwords fall into the first category, namely something you know, and of course the big trouble with something you know is that it's fairly easy to forget it or for someone else to get to know it too. Ask anyone who's manned a support desk on the day after a long Christmas break, and you'll appreciate just how easy it is to forget a password. One large bank of my acquaintance employs two people whose primary job is simply to reset forgotten passwords. Not only is this a huge waste of money but it's also a major security risk.

One way to circumvent the problems associated with something you know is to go with the idea of something you have. Smartcards and other physical tokens fall into this category. You can't forget a token, though you can of course forget to bring it into the office with you. And although tokens are relatively cheap to buy, the procedures and personnel required to issue them, reclaim them from ex-employees and so on is considerable. Nevertheless, hardware tokens in some form are proving very popular in high-security environments, especially where laptops containing confidential information are routinely taken out of the office.

Introducing Biometrics

Surprisingly, very little attention has been paid in the past to the third concept of authentication, namely something you are. This is the art of biometrics, ie checking a unique characteristic of the user such as a fingerprint, smell, voice, the way he signs his name, and so on. The concept is not a new one - the ancient Egyptians used characteristics such as scars and birthmarks to identify people many thousands of years ago.

Although biometrics does have its problems, not least the initial cost, it can provide an excellent way of removing the problems of forgotten passwords. However long someone is away from the office during the Christmas period, he's unlikely to forget to bring his finger when he returns. He can then simply place his finger on the reader to gain instant login to the company network without the need for a password. And in case you're wondering, there's usually a facility for an override master password and/or fingerprint to allow support staff to access machines in cases where a user is not physically present.

Categories

There are many features of a person that can be measured in order to generate a unique identity code. Fingerprints are obvious, and are certainly very popular with companies developing biometric solutions. Also popular is face recognition, in which algorithms similar to those used in fingerprint recognition are used to measure the distances between various components of the face. Recent developments in this area allow standard cameras to analyse a face in three dimensions rather than just two, which helps to improve accuracy if the subject doesn't always look straight into the camera either during the enrolment or recognition phase.

Handwriting analysis is another alternative, and specifically something known as signature dynamics. This uses a special pad (rather like a graphics tablet) or a special pen (rather like a pen-shaped mouse) to analyse the way that someone signs their name.

One interesting technology is the idea of using hand geometry. Instead of analysing the fingerprint, a camera above the hand measures the thickness, length, width etc of one or more fingers. However at least one vendor of such systems that I spoke to at a recent exhibition (see below) admitted that such systems are easier to fool.

The database of known fingerprints, faces, signatures etc with which comparisons are made is usually stored on a remote server. However another option is to store the data on a smartcard which the user carries with him. The authentication is then a process of checking that the user's current signature, face, fingerprint etc matches the version on the card which he carries. Although this adds an additional layer of security, it also adds to the cost and can lead to additional support problems.

Bear in mind too that storing faces or fingerprints in a single database may have legal implications, depending on the countries in which you operate and how you intend to store and transport the data. Data protection legislation in the UK, for example, prohibits the export of personal data to countries which don't have data protection legislation of the required standard. This makes it very difficult for UK subsidiaries of American companies to send customer data back to the US for processing, and might well scupper any attempts to create a single company-wide database of fingerprints and faces.

Beating The System

Passwords can be cracked. Unfortunately, biometrics isn't necessarily any harder to defeat. And a system with visible security such as a fingerprint reader attached is instantly going to alert people to the fact that it presumably contains highly confidential worthy of increased protection.

Systems that measure hand or face geometry can often be fooled by taking a silicone or wax cast. So long as it has the same measurements as the original it will often pass the test. Such casts are rarely able to defeat fingerprint readers, especially as the fingerprint readers normally check for heat, a pulse, skin conductivity and so on.

Voice recognition systems which always ask the same question, eg, "please say your name", are vulnerable to attack with nothing more complicated than a tape recorder. They get around this problem by randomly prompting the user to say a word that has not been asked for before.

One weakness with fingerprint readers is that anyone who places their finger on the reader will, unless the digit is completely free of oils, leave a visible fingerprint on the glass. If you've seen a crime movie you'll know that these can be lifted with the aid of some fine powder and adhesive tape, though transferring this onto something like an imitation rubber finger is far from trivial. Face recognition and iris (eye) scanning do not suffer from this particular drawback.

Products

At the end of 2001, the annual Biometrics exhibition took place in London. The remainder of this article looks at some of the products that were on show, and includes links to Web sites from where you can obtain further information and, in some cases, evaluation versions of software.

"Systems that measure hand or face geometry can often be fooled by taking a silicone or wax cast. So long as it has the same measurements as the original it will often pass the test."

BioPassport

The BioLogin module replaces the login procedure on Windows 2000 and XP, and supports face and / or fingerprint recognition. The face recognition software uses a standard Webcam rather than requiring any specialist hardware. More details are at **http://www.identalink.com**. Because the product hooks into the standard Windows authentication API it also works with all password-protected applications.

The company also produces an add-in for Outlook which allows biometric security to be applied to email encryption.

Aurora

Aurora makes face recognition products for shift workers to clock on and off, and also for secure login to networks and servers. Details are at **http://auroracs.co.uk**. The company also produces something called VisNet, which is a Windows application for keeping track of visitors to a site. This isn't biometric-based, but manages the printing of badges, keeping a database of who visits whom and when, and so

on. The product can also produce barcoded badges in advance, so visitors simply collect their badge and pass through a scanner rather than having to queue upon arrival.

Cognitec

Cognitec's FaceVACS allows you to secure a workstation against unauthorised logins using face recognition. The program works with a standard Webcam and you can download the software for around US$70 from the company's site at **http://www.cognitec-ag.de**. The program supports all versions of Windows from 98 to XP and can work in conjunction with a password for additional security. There's also an SDK if you want to extend the features of the software.

Tridentity

Tridentity uses 3D modelling software to build up what the company claims is a more reliable and secure model of a face. The program claims to measure 200 separate features of the user's face in order to provide maximum reliability and security. Details are at **http://www.neurodynamics.com**.

Guardware

Guardware produces fingerprint recognition systems for system logins and for controlling doors into secure areas. The company also produces a fingerprint reader and smartcard slot which fits into a standard 5.25 inch drive bay. Although this may be useful in some instances, bear in mind that allowing physical access to a computer is generally considered a bad idea and is this only really of use for users' own workstations and certainly not for servers. Details are at **http://www.guardware.com**. Guardware also claims that its fingerprint reader is especially good at differentiating between real and fake fingers.

Smart Pen

At **http://www.smartpen.net** you'll find details of the Smart Pen for authenticating via signature dynamics. This pen doesn't need a special pressure-sensitive pad; it contains ink as well as the electronics and can thus be used on paper just like a normal pen. It's available in wired and wireless versions and takes standard ink refills.

Visionics

Visionics (**http://www.visionics.com**) makes a face recognition software package, and also markets an SDK that allows you to develop enhancements in C++, Visual Basic or Delphi. The company also markets software for picking out faces in crowds, such as looking for known troublemakers.

SentriNET

SentriNET, from Informer Systems, is a fingerprint-based authentication system for networks, workstations and applications. It's based on the Cherry keyboard mentioned above and runs under Windows (98 and above) as well as NetWare. The company also produces software to allow NetWare NDS to accept fingerprint templates. Details are at **http://www.informer.co.uk**.

"Cognitec's FaceVACS allows you to secure a workstation against unauthorised logins using face recognition. The program works with a standard Webcam and you can download the software for around US$70."

SentryCom

SentryCom produces a biometric product that uses voice recognition to control login to Windows networks, VPNs and so on. The product includes random real-time prompting to circumvent tape-recorder attacks. Information is at **http://www.sentry-com.co.il**.

FaceGate

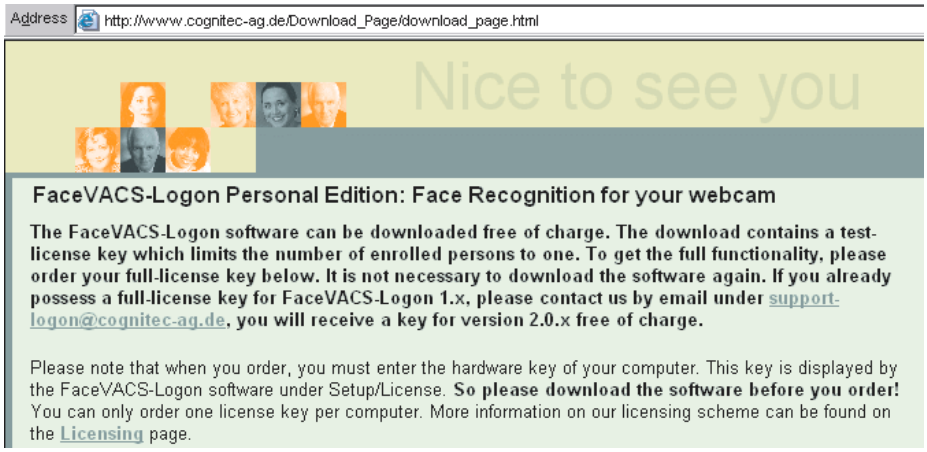
FaceGate (**http://www.bio4.co.uk**) produces face recognition technology for controlling Windows, SQL Server, intranet and extranet logins, and also has similar software for portable computers including those running Windows CE and PalmOS.

Omron

Omron produces a face recognition unit built into an electronic door lock, to control physical access to secure areas. The company has a site at **http://www.society.omron.com** which contains more information.

Cherry

Cherry is a well-known producer of PC keyboards. The company also produces



models with built-in smartcard and/or fingerprint readers. Various companies bundle these keyboards with the necessary software for controlling system logins. The company's Web site is **http://www.cherry.de**.

Conclusion

The trouble with passwords is that they're a compromise between price and performance. Although passwords can be cracked, forgotten or stolen, they are an incredibly cheap authentication method to set up. But better alternatives do exist, and if you are having specific problems with the concept of passwords then you would do well to consider investigating the idea of biometrics, at least on a handful of machines in the first instance.

While there are many biometric devices and technologies, fingerprinting is a mature technology and has been by far the most popular in the past. However the heightened fight against terrorism since last September has increased the pace of development of facial recognition systems, especially for picking out known troublemakers in a crowd. This, plus the proliferation of webcams on home and office PCs, may mean that face recognition may overtake fingerprint technology in terms of both set-up costs and ubiquity. Any organisation considering the use of biometrics would do well to investigate both technologies before making a final decision.

Another use for face recognition technology which is rapidly becoming widespread is its use by police forces to assist in the cataloguing of image libraries seized from suspected child pornographers. The technology can quickly analyse large numbers of image files to detect faces which appear more than once in a suspect's library, or to find faces which appear in the libraries of multiple suspects.

But it would seem that fingerprint recognition is the accepted technology for authenticating users of computer systems such as network logins. Face recognition seems to be more popular for controlling door looks for access to secure rooms and also for workers to clock on and off a shift.

Vendors tend to make major claims in terms of how accurate their systems are. This is obviously crucial. You need to be sure that impostors won't be admitted into your systems, but equally you need to be confident that legitimate users won't be locked out for no good reason. This is one reason why you need to test out different systems in your own environment, to be sure that you're getting the solution that is right for you. For example, noisy environments such as call centres or large open-plan offices are not suitable for voice recognition, while dirty, oily environments might not be suitable for fingerprints. Also, many companies admit that their fingerprint readers are more reliable with white skin than on non-white hands, so this may be relevant too.

Finally, bear in mind that whatever you save in terms of not having to reset users' passwords might well be spent in buying biometric hardware. Even in quantity, the necessary hardware and software won't cost less than around US$100 per PC.

"Whatever you save in terms of not having to reset users' passwords might well be spent in buying biometric hardware. Even in quantity, the necessary hardware and software won't cost less than around US$100 per PC."

PCNA

New Reviews from Tech Support Alert

Anti-Trojan Software Reviews

A detailed review of six of the best anti trojan software programs. Two products were impressive with a clear gap between these and other contenders in their ability to detect and remove dangerous modern trojans.

Inkjet Printer Cartridge Suppliers

Everyone gets inundated by hundreds of ads for inkjet printer cartridges, all claiming to be the cheapest or best. But which vendor do you believe? Our editors decided to put them to the test by anonymously buying printer cartridges and testing them in our office inkjet printers. Many suppliers disappointed but we came up with several web sites that offer good quality cheap inkjet cartridges with impressive customer service.

Windows Backup Software

In this review we looked at 18 different backup software products for home or SOHO use. In the end we could only recommend six though only two were good enough to get our “Editor’s Choice” award

The 46 Best Freeware Programs

There are many free utilities that perform as well or better than expensive commercial products. Our Editor Ian Richards picks out his selection of the very best freeware programs and he comes up with some real gems.