

# BIOMETRICS

## Making The Right Impression

by Julian Ashbourn

### Introduction

It is time once again for our annual update on biometrics and to consider how the market is evolving. The selection of products we have for you this time are quite a mixed bunch and, indeed, show how the biometric market is beginning to mature.



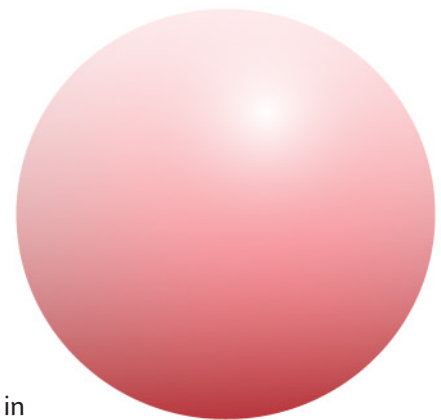
Fortunately, the penny is slowly dropping and integrators are spending less time looking for biometric applications (there is not really such a thing anyway) and more time seeking to integrate biometrics into existing processes where applicable. This is how it should have been all along. We can see this reflected also in the product mix, with solutions appearing which place the emphasis firmly on software, relegating biometric capture devices to commodity item status. This is quite reasonable and leads towards a potentially enhanced level of interoperability, something the biometric industry desperately needs.

In recent months, you will have noticed an increasing number of devices such as notebook computers and computer keyboards with integral biometric fingerprint readers, and some with smartcard readers as well, plus several variants of biometric mice. Given the forthcoming support for biometrics at operating system level, we are a small step away from using biometric verification as a regular method of access control to computers and networks. We mentioned fingerprint biometrics as this is the predominant technique at present as far as embedded biometrics in computer peripherals are concerned, but there are of course other techniques such as facial recognition, iris scanning, signature verification and voice verification, all of which lend themselves for use with computer and mobile communications devices (hand geometry may not be so easy to integrate at present).

Any device with an integral camera, microphone or writing tablet has the potential to incorporate biometric identity verification. Add to this phenomenon the fact that the cost of dedicated biometric devices has been steadily dropping, and it looks clear that we shall see a greater emphasis on this technology in coming months. However, capture devices are only part of the story; we also need well considered, secure and reliable software in order to implement a satisfactory biometric access control system. This is especially the case when we are dealing with large and complex networks. Several such software applications are starting to appear and we introduce you to a couple of examples within this update.

So, is that all there is to it? We load the software, plug in a capture device and off we go? Well, as a private user you may wish to try the technology this way, on an isolated workstation over which you have full control and responsibility, but for the corporate network we need to think a little more deeply. For example, one argument that vendors often use in their sales pitches is that biometrics have the potential to save you a fortune by eliminating helpdesk calls for forgotten passwords. This will of course only be the case if every user on the network never has a problem using their biometric device, an unlikely scenario. When they do have a problem using their biometric device, the helpdesk call is likely to be much longer and may not be resolved by remote action.

This brings us into the realms of training and biometric enrolment. Good quality enrolment procedures result in good quality biometric templates being created. Good quality templates result in



reliable identity verification, providing that users are reasonably consistent in the way they interact with the biometric device. Quality information and training will also ensure that users understand how the system is operating, how to give a good biometric live sample and the importance of operational consistency. But there are yet more variables to consider, some of which, like user psychology are not physical entities, which can be hot swapped in times of trouble. Then we have to consider whether our current groups of users and access rights need any modification, whether we implement single sign-on and other issues. On top of this, we need to consider maintenance and support of both software and hardware.

Phew! Is all this biometric fandango really worth it? Yes, it is. You see, biometrics offer the only practical way of really knowing who it is who accessed a given terminal, application or service. Extend this to commercial or inter-company transactions and the potential value of implementing such techniques becomes interesting indeed.

But surely we have passwords for this sort of thing? Yes, but passwords only tell us that someone at the other end knows the password. Ah yes, but what about certificates and PKI? Yes, that tells us that someone at the other end has access to the certificates. What about smartcards and certificates? Yes, that tells us that someone at the other end has access to both. Biometrics? Ah-ha, that tells us who it is at the other end.

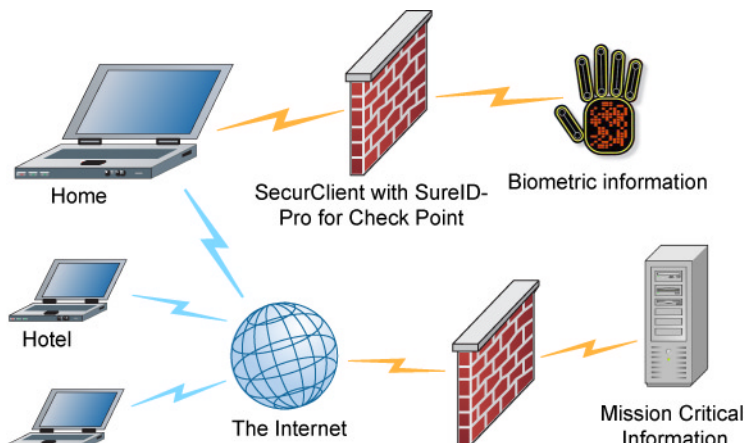
The time has come to think seriously about the ways in which biometric verification technology might enhance secure computing within your organization. The tools are available and have reached a level of acceptable maturity. Sure, biometrics are not a panacea for everything, but used intelligently they offer a range of possibilities that are simply not attainable by other means. Furthermore, you will be seeing more of them in public applications in coming months and years, creating a broader awareness among users in general.

If you are a systems or network administrator, it is time to bone up on this technology and understand the implications. A good starting point is the non-profit Avanti Biometric Resource site, which may be found at <http://homepage.ntlworld.com/avanti>, from which you can access many links to other organizations, government departments and suppliers, as well as a library of background information. The next step is to diligently read your copy of SC Magazine every month in order to keep up to date with developments as they unfold. With manufacturers such as Sony and Panasonic entering the field, as well as the global IT consultancies, we shall see some interesting developments coming down the line. Make no mistake, biometric verification technology is here to stay.

Source: SCMagazine 6/2002  
[http://www.scmagazine.com/scmagazine/2002\\_06/survey/survey.html](http://www.scmagazine.com/scmagazine/2002_06/survey/survey.html)



## SureID Case Study



SureID-Professional seamlessly integrates into Check Point's SecurRemote and SecurClient software enabling strong biometric authentication as part of your secure infrastructure. No additional server software or hardware is required and deployment is simple. Just plug-in your fingerprint reader, insert the SureID-Professional CD, follow the simple on-screen instructions, and you are operational within minutes. Because SureID-Professional is Check Point certified, you know that you have one of the most reliable, scalable, and secure solutions available. SureID-Professional does not replace the excellent security standards like IPSEC, IKE, and Digital Certificates provided by Check Point. SureID-Professional simply and reliably eliminates the weakest link in security, user authentication, by replacing authentication with strong biometric authentication.

### About Jason Roberts

Jason Roberts Associates continues to be a premiere SAP Supplemental Staffing and Consulting firm as well as a major provider of B2B, E-Commerce, CRM, Data Warehouse, Supply Chain and other ERP software package resources. We are responsible for delivering the most qualified Technology professionals to the world's top premier companies. Jason Roberts Associates earned the respect of the IT community by utilizing dynamic strategies to meet the challenges of SAP's fast-paced environment. Our success can be attributed to our ability to respond effectively to new customer needs and to seize market opportunities as they arise.

Jason Roberts has provided solutions to the Fortune 1000 including: American Standard, Andersen Consulting, Anheuser Busch, Aventis, Barnes and Noble.com, Bristol-Myers Squibb, Cap Gemini, Deloitte & Touche, Delphi Automotive, Discovery Channel, Ernst & Young LLP, Georgia Pacific, Gillette Company, Hewlett Packard, Monsanto Corporation, Northrup Grumman, Pricewaterhouse, Reebok International, SAP America, Siemens Business Services.

