

BIOMETRICS

Remote Network Access

by Julian Ashbourn

Remote Network Access

In an 'e' world, remote access to corporate applications and data becomes increasingly valuable. For example, access to the corporate Intranet by employees wherever they might be -



important especially for mobile workers. Easy access to the network for home workers. Collaboration with business partners via extranets. Connectivity of PDA devices and wearable computers to host services. And so on.

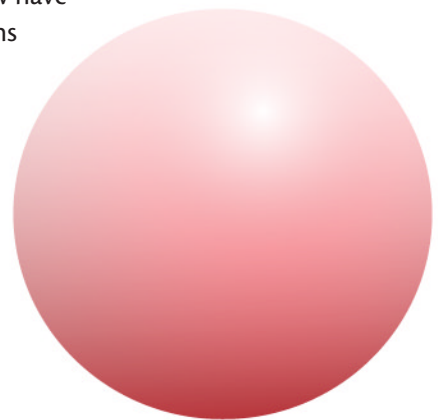
One obstacle to remote access has historically been the provision of acceptable security and ease of use at an equally acceptable cost. Many organizations currently use randomly generated 'one time passwords' via tokens, for certain users who need remote network access. However, this solution, whilst workable, is relatively expensive, not particularly user friendly, and doesn't guarantee the identity of the individual seeking access. If, for example, a notebook computer was stolen or lost between office and remote locations, there is a possibility that the token would be with the device - potentially compromising security.

We are all familiar with certain technological developments, which offer additional possibilities in this context, including the use of digital certificates for network transactions (PKI), virtual private networks (VPN), chip cards and biometrics. Furthermore, the cost of implementing these technologies has been falling, in some cases quite dramatically. The question though has been, are these technologies proven, and if so, how to put a suitable combination of such technologies together in a way that provides unquestioned business benefit in a practical, reliable, scalable and cost effective manner. may not be so easy to integrate at present).

Let us consider associated developments within the popular operating systems. Among the enhancements in Windows 2000 (client and server) for example, is improved support for virtual private networks (VPN) and enhanced authentication services (EAS). This suggests some interesting possibilities for future remote access across a variety of scenarios.

One idea that immediately springs to mind in this context is the combination of biometric identity verification, VPNs and the Internet. A biometric provides a high level of confidence as to the true identity of the user initiating a connection (something we don't have today). A VPN provides a secure communication link with data encryption and the use of certificates if required. The Internet provides a global maintained network, accessible at low cost via local area connection. If we put these elements together, we have the potential for user friendly, secure remote access at reasonable cost.

Imagine an in place VPN capability, using the Win 2000 client with Layer Two Tunneling Protocol (L2TP) over Internet Protocol Security (IPSec). For mobile remote access, clients would typically be accessing the Internet via an ISP account (perhaps negotiated globally, with an agreed service level) and initiating a secure VPN session. This would be subject to the usual back end arrangements for the VPN server (demilitarized zones / firewalls etc) and ongoing connectivity. Using computer level certificates, we now have a secure communications session between two known entities (the client device and the VPN server). What we don't know for sure is who is sitting at the other end making this connection.



Some advocate the use of chip cards in order to hold a private key away from the client device, but this token could still be used by anyone - thus adding cost and complexity, but not necessarily security. This is where biometrics comes in. Replacing the user password with a biometric ensures that only the bona fide approved user may initiate this connection. This approach, in addition to providing greatly enhanced security, also provides greatly enhanced convenience for the user. Imagine logging on to your PC with a single touch of an integral fingerprint reader. No multiple passwords to manage and forget (the system may still use passwords invisible to the user, if this helps with directory references etc.), no struggling with tokens and associated clumsy procedures, speedier logon and access to resources. There may also be an associated financial benefit in reduced levels of help desk calls for password maintenance.

Of course, we have been aware of the potential of biometrics for some time. However, it has often been considered that this is an expensive, immature or user-unfriendly technology. In fact, this is simply no longer the case. Many organizations are actively using biometrics now, with quite astonishing results - especially with regard to user acceptance, which, in the vast majority of cases is overwhelmingly positive.

Device costs have dropped dramatically in recent times, especially for fingerprint biometrics, which have almost become an OEM 'embedded solution'. We already have several computer keyboards with integral fingerprint readers, mice with integral fingerprint readers, peripheral PCMCIA cards with fingerprint readers, chip cards with on board fingerprint readers and other configurations. Very shortly, we shall see notebook PC manufacturers launch models with integral biometric readers. Similarly, PDA device manufacturers and mobile phone manufacturers are looking very closely at this possibility. Implementing biometrics in an enterprise network environment is also now well understood, and standards such as the Common Biometric Exchange File Format (CBEFF) and the Biometric Application Programming Interface (BIOApi) are well established.

Naturally, the technology isn't perfect (nothing is), but in terms of confidence levels as to user identity, it offers orders of magnitude improvements over passwords and tokens and is easily deployed. As devices become more commonplace (integrated or otherwise), this will appear an obvious way forward for conventional on site network access. For remote access across untrusted networks such as the Internet, and in conjunction with a secure communications session, it starts to look particularly interesting.

Integrating a biometric verification model (on the client) with a VPN environment would require a little thinking through, especially with regard to template enrolment and management, but is certainly feasible. It may be interesting to consider what business related benefits or enhancements could be realized with a low cost, secure means of communication across both trusted or untrusted networks. User connectivity from anywhere? Facilitating secure extranets for collaborative commerce? Additional customer services for users so equipped? Wireless connection for wearable computers when required? Secure messaging services for mobile personnel? Enhanced 'self service' facilities for office-based personnel?

As the modern world develops and more and more 'transactions' are on line (whether internal or external), the need to be sure of the identity of the person at the other end, and maintain secure communication during the session, will become increasingly important.

Source: Avanti
<http://homepage.ntlworld.com/avanti/remotearchive.htm>

