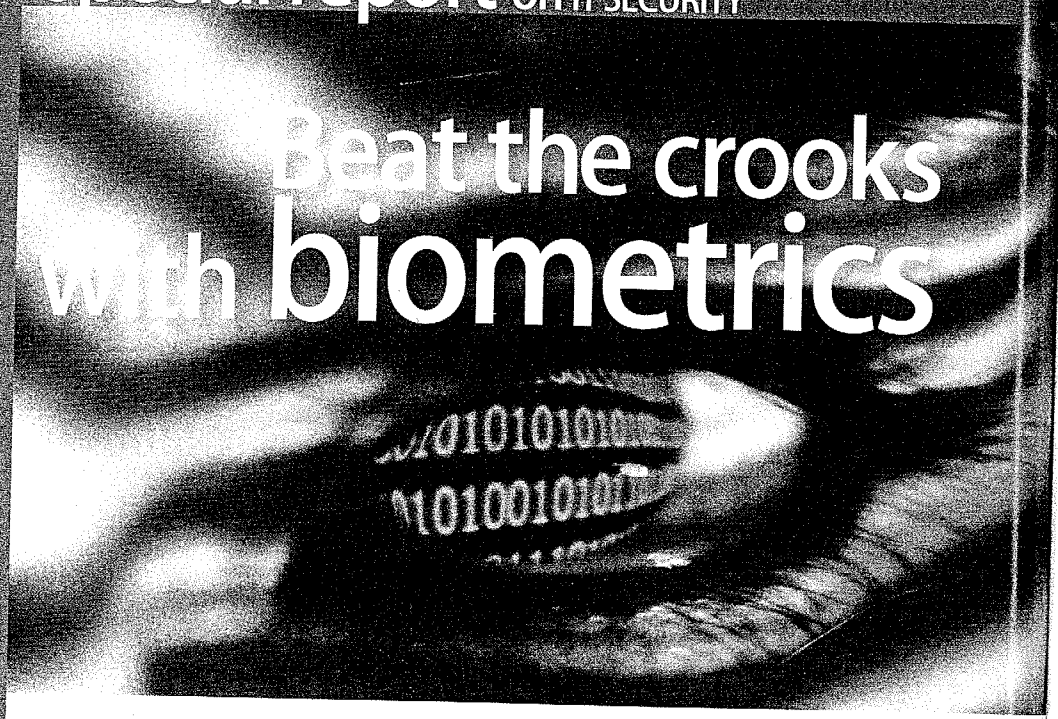


Beat the crooks with biometrics

Many companies have begun looking at biometrics as the ideal solution for securing IT access. With two-factor authentication methods already well established, the next step may be the introduction of multi-factor authentication

by Tim Best, Logica CMG

Identity technology already plays a bigger part in day-to-day life than many people realize. Used across a wide variety of applications, but none more so than security, the technology has quickly passed into common use and parlance. Fingerprint scanners can be added to laptops for next to nothing. Facial recognition systems are being deployed by organizations as varied as retail villages and football teams, and you can even compare iris scanner prices via the online price comparison site Kelkoo.

The reason the technology has come so far, so fast, is simple. The threats against the security and integrity of technology assets have grown in both size and scope at an alarming rate. The Web Application Security Consortium reports 41 hacking incidents last year, hitting some of the biggest names on the Internet. Spam is set to double in 2007 according to reports, and phishing has given rise to new SMS variations as the threats to IT security become more diverse and sophisticated. Cases of identity theft and fraud regularly hit the headlines. Social networking sites such as MySpace have opened up new avenues for social engineering and dangerous access to corporate networks. Consequently innovation itself – keeping one step ahead or even just keeping pace with the bad guys – has become a vital weapon.

Securing online banking

This security imperative has been compounded by developing business cases for investing in identity technology. A great example can be found within the retail banking industry – here securing an online, easy to use identity for a customer is crucial as it forms the very bedrock of successful online banking. Online banking offers far lower business costs, but an insecure and difficult to use electronic 'identity' will send a customer straight back to a branch, losing the savings and tarnishing the reputation of the bank.

Therefore the deployment of identity technology must take into account ease of use and customer experience – issues traditionally outside of the security realm. New thinking has so far yielded the use of tokens with random, single-use log-in numbers, biometric access, and even the use of mobile phones as an authentication layer.

It is worth noting that this increased set of processes is being built from the "end-user back" – that is finding ways in which the established behavior of the end user can be used to make things more secure, rather than attempting to change that behavior itself with new technology. This has led to the re-evaluation of the identity technologies most likely to be suitable for securing physical access to assets or logical access to data itself.

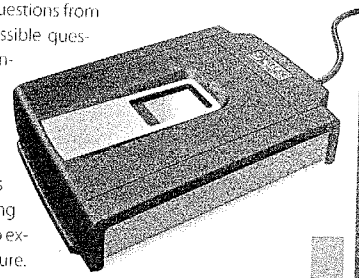
Multi-modal biometrics

One of the biggest new developments is multi-modal biometrics – using more than one factor or modality to establish or verify an identity. This may be done in a variety of ways: combining two biometrics, such as a fingerprint and iris scan, taking multiple readings of a single modality, such as scanning a fingerprint many times, or in some cases combining biometric and non-biometric elements such as biographic information or passcodes or tokens.

Two-factor authentication methods offer an increased level of security, combining something that the person is with something that they possess. Crucially they often involve no additional burden on the end user, reinforcing security by improving the "back office" elements of the security chain. In addition, combined biometric/biographic processes may (though this has yet to be fully researched) offer a more cost-effective alternative than having to equip organizations with multiple examples of biometric scanning equipment, especially in lower risk situations.

Multi-factor authentication

The natural extension of a two-factor authentication is to move toward multi-factor authentication (MFA). This throws open many possibilities for increasing the security of IT assets and data. Verification of identity could be made by a biometric combined with a token and a password or any combination of any multiple of these options - two questions from a list of five possible questions, plus a fingerprint, for example, would deliver a much stronger solution for access without requiring huge changes to existing infrastructure.



Multi-factor authentication can be carried out using a biometric with a token and password or any combination of any multiple of these

The central principle here is to link something the person is with something they have and something they know. By having multiple instances of one of these "somethings" from which a random selection is made (especially the 'something they know' category) an element of unpredictability is introduced that can frustrate attempts to impersonate the identity of the person with genuine rights to access the information or IT facilities.

This innovation has been guided by an established principle – deploying the right level of identity technology based upon the level of threat posed to the asset being secured.

Multi-modal biometrics offer greater confidence in verifying ID without disrupting established frameworks

As the crimes of identity theft and fraud have increased, multi-modal biometrics offer increased confidence in establishing and verifying identity without causing disruption to established frameworks – it is simply an additional layer within established processes.

However it is not just the identity technology itself that can be considered new. Its very application is changing as well. As the previous retail banking example shows, many organizations are now considering extending their IT to their customers. Allowing this "logical" access to private, often sensitive data outside of the "castle walls" of an organization is a huge undertaking. Organizations cannot guarantee the security of end user devices, nor can they ensure users are adequately trained. Furthermore the plethora of laptops, PDAs and mobile phones that may be used to access data mean a consistent, platform-independent methodology of establishing and verifying identity is crucial.

With these new methods of access, the vanguards of identity technology use are expanding at an incredible rate. Rather than attempting to educate potentially millions of users to use passwords that need to be increasingly complex to beat the crooks, many companies are looking the intuitive nature of secure biometrics to provide the next generation of secure access.

By redefining identity technology around the end user, instead of trying to alter users' behavior, the security offered in the face of diverse and sophisticated threats is increasing without compromising on the usability of the solutions themselves. ■