

Buyer's GUIDE



Are Biometrics The Answer?

Biometric authentication looks sexy, but before you start scanning, consider some of its negatives **By Mike Fratto**

The McGuffin in *Minority Report* is an eyeball. After our hero, John Anderton, is tagged as a murderer, his eye, removed from his body, is used to access a secure facility and network. It shows that biometrics can be fooled—one of the biggest drawbacks to this authentication technology.

Certain situations, however, lend themselves to the use of biometrics: If your helpdesk is suffering from too many requests for forgotten passwords (an estimated 40 percent of all helpdesk calls, according to Gartner), you might consider making the switch.

Strengths and Vulnerabilities

Biometric-security devices record a unique aspect of a person—such as a fingerprint—and use that record for comparison against later attempts to authenticate. Iris and retina scanners are the most reliable; fingerprints, face and handprint scanners follow close behind. These devices have a higher rate of reliability than voice or sig-



Fingerprint and iris scanners

nature scanners, but a lower rate of reliability compared with passwords or authentication tokens.

Environmental conditions can affect biometric-authentication devices. Fingerprint readers and iris scanners are small and make sense on the desktop but may not cut it in a shop environment rife with dust, humidity and other contaminants. Dirt, smudges and improperly placed fingers, hands or faces can cause a false read. Glasses, contact lenses, ambient or overhead lighting and awkward camera placement can significantly affect the usability of iris and retina scanners. Background

noises and changes in a person's voice because of illness or stress can cause errors with voice-recognition systems.

Additionally, all biometric devices have specific software and hardware requirements. Check that you can support the device and that the device works with your network software. Also determine if an external power source or USB port is required and available.

Fears and cultural- or religious-based beliefs may work against you as well. Survey your employees to determine how many will accept the idea. And try out the device to determine if your employees can accurately use it.

And, of course, security researchers have found ways to trick biometric devices. Fingerprints can be lifted off a glass surface, even from the fingerprint reader, using graphite powder and a piece of tape or a cube of gelatin. Iris scanners might be fooled with a high-resolution image of the user's eye. To counteract these tricks, newer devices look for "liveness" indicated by pulse or vascular movement.

Setting Thresholds

Biometric devices' acceptable-failure thresholds are based on a FAR (false acceptance rate) and an FRR (false rejection rate). The FAR shows the likelihood of a user



Biometric Checklist

Questions to ask before you buy:

- 1) Does the device suit the environment?
- 2) Is there a power source nearby?
- 3) Is the reader-to-PC interface supported on the PC?
- 4) Are authentication thresholds configurable?
- 5) Does the device provide the extra protection of 'liveness' testing?
- 6) Are there antireplay features to help thwart electronic resubmission of biometrics?

For details and prices on specific models, use our Interactive Buyer's Guide charts at www.nwc.com/1403/1403ibg1.html.

being incorrectly accepted; the FRR indicates how likely a biometric device will incorrectly reject a user.

If the administrator sets the threshold too low, the system will be more lenient in matching a submitted biometric to the user's template and subsequently will be more likely to accept an invalid user. Set the threshold too high, and you increase the likelihood that valid users will be rejected. To make ongoing management easier, make sure the thresholds can be configured and adjusted in house.

Enrollment & Integration

As with any authentication system, users must be enrolled first. Many biometric systems let users self-enroll. They authenticate to the local computer or to a directory and then enroll with the biometric. Unfortunately, if you are using biometrics to strengthen authentication but you rely on user names and passwords during the initial identification and authentication process, you haven't made any security gains. Monitored enrollment prevents this scenario but takes more time.

After enrollment, consider where the authentication information will be stored. Biometric systems that store data on the local machine can authenticate a user to that machine only. For larger deployments and for better management, look for a system that uses centralized storage. If the biometric software is deployed on all relevant systems, users can enroll once and have access everywhere.

For backup, multiple means of authentication should be recorded. Some devices let you enroll multiple biometrics—such as all the fingers on the right hand—for a single user. If something happens to one finger, a cut across the finger pad for example, the user can use another finger to authenticate without having to re-enroll.

In all cases, you will have to use hardware and software from a single biometric vendor: Interoperability is

Diminishing False Reads

Biometric devices are most commonly used for network logins, which could mean a huge number of users of varying competence levels. If a device is hard to use, the FRR will reflect that. Consider devices that include guides to help the user place a finger in the right spot or look in the correct direction. Another option, depending on the sensitivity of the material being accessed, is to use passwords, smartcards and other means of authentication in place of your biometric device if it fails. This will, at the very least, counter those helpdesk calls asking, "How do I make this thing work?"

Industry Orgs

The BioAPI Consortium (www.bioapi.org), comprising government and industry leaders, released version 1.0 of the BioAPI Specification in March 2000; version 1.1 of the specification and reference implementation came out in March 2001.

OTHER INDUSTRY ORGANIZATIONS:

» **The Biometric Consortium** (www.biometrics.org) serves as the U.S. government's focal point for research, development, testing, evaluation and application of biometric-based personal identification/verification technology.

» **The BioSec Alliance** (www.biosec.com) is a multivendor initiative founded by BioNetrix in 1999 to promote enterprise authentication solutions.

» **The International Biometric Industry Association** (www.ibia.org) is a trade association founded in 1998 to look after the interests of the biometric industry.

From Gartner's July 19, 2002, technology overview, "Biometric Authentication: Perspective"

nonexistent in biometric authentication, despite the BioAPI Consortium's rallying to provide a standardized API for biometric integration. Authentication-management applications, such as Novell's NMAS and Secure Computing's SafeWord PremierAccess, which tie together biometric and nonbiometric authentication strategies for directory logins, are available, however.

Application integration is still based on individual partnerships, so it is important to ensure the device you choose supports your applications or that the vendor is willing to develop the integration for you. Integration usually takes place on the desktop or server using a Unix PAM (Pluggable Authentication Module), a Windows GINA (Graphical Identification and Authentication) or a Novell eDirectory LCM (Login Client Module). As long as a user name-password pair is cached, your login credentials are used to log in to other applications. If your applications require a separate login, expect to do some developing.

Biometrics alone shouldn't be used for access to highly confidential data unless you've thoroughly tested the technology. If your goal is strong authentication, more proven technologies—hardware and software tokens and passwords—work well. And despite a recent decrease in the cost of biometric devices, these old standbys are usually a better deal. But if your goal is ease of use and reasonably strong authentication, biometric technology might be for you. **NWC**

Mike Fratto is a senior technology editor based in NETWORK COMPUTING's Syracuse University Real-World Labs®. Write to him at mfratto@nwc.com. Post a comment or question on this story at www.nwc.com/go/ask.html.