CPU™

COMPUTER POWER USER

Stop The BAD GUYS

Digital Security: What's Available Today & What's Coming Tomorrow

May 2002
$5.95 U.S. $7.95 Canada

Columns

Anand Lal Shimpi
Alex "Sharky" Ross
Kyle Bennett
Chris Pirillo
Pete Loshin
Lisa Lopuck
Rob "CmdrTaco" Malda
Joan Wood
Alex St. John

Reviews

Q&A

With Xbox Technology Officer
Seamus Blackley

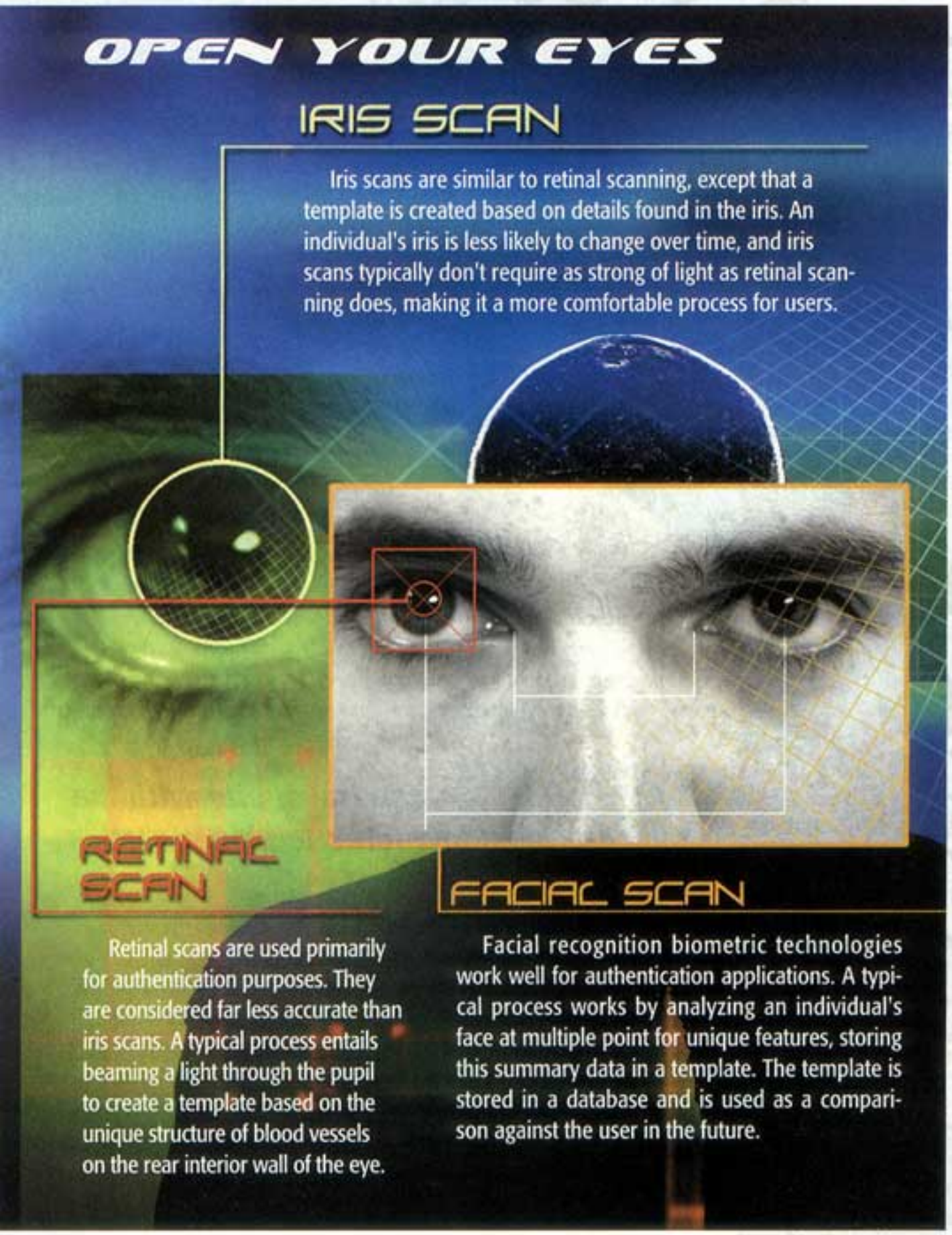
VISUAL BIOMETRICS

An Eye On How These Technologies Provide Security

Smile for the camera, please. Now blink your eyes. Say your name, please. Thank you. Next.

This isn't a scene from a Hollywood screen test. It's actually an enrollment procedure used in many visual biometric technologies for entering an individual into a database based on his or her unique visual characteristics. Enrollment is the first step in such biometric processes, creating a reference in the system for that individual.

The use of visually related biometrics for authentication and identification purposes is an exploding field. It's also a field that can be grouped into two primary sectors, including retina/iris recognition and facial recognition technologies.



Eyes Wide Open

Retinal scanning has been in use for years. Used almost exclusively for guarding access to facilities or areas where security is a concern, the technology works by using a specialized camera to look through the pupil at the blood vessels in the top layer of the retina, which consists of a nerve layer at the rear of the eye. The patterns of these blood vessels are unique to individuals, changing little during a lifetime, unlike fingerprints, which can change due to growth, scarring, and more.

Typically, a template that's less than 100 bytes in size is generated using these patterns, which are measured at more than 400 points. The small size of such templates lets standalone devices store large numbers of retina files without excessive storage demands or reliance on a central server.

The technology does have some drawbacks, however. A retinal scanning device can cost as much as $2,500, eliminating most home and retail uses. In addition, many people find the process of undergoing retinal scans more uncomfortable than other biometric input methods. For example, an individual might have to be within a half-inch of the scanning device, keep very still, and endure a strong light that illuminates the inside of the eye. As other biometric technologies advance and become easier to use, retinal scanning has retained many of these limitations.

Iris scanning is another biometric method gaining popularity in a hurry. For biometric measurements, the iris (the colored portion of the eye surrounding the pupil) provides 266 unique points of reference within what is known as the trabecular meshwork. Like retinas, human irises are a constant biometric from before birth to death, barring external damage or degenerative disease. Unlike retinal scanning, however, devices can scan an iris from as far as three feet away, eliminating the discomfort associated with some retinal devices. In addition, a clear camera view of the iris typically doesn't require strong auxiliary lighting.

In a typical process, a scanning device acquires an image of the iris. Algorithms then divide the image into finely spaced concentric rings, which are further divided into hundreds of subsections called phasors. The phasors are then examined and their contents cataloged. Extremely complex mathematics help create a template based on this data.

Iridian Technologies (www.iriscan.com) refers to this template as an IrisCode, which contains the location of the contents within the phasors and the phasors' location within the iris. An IrisCode (512 bytes) isn't as compact as a 96-byte retina template. However, continuing improvements and decreasing costs of computing power and data storage should eventually make the files very manageable.

Many applications use iris recognition technology (see pg. 54), including tor protect a home user's PC—check out Panasonic's Authenticam ($239; wwwpanasonic.com/medical_industrial/iri.asp), which is powered by embedded software from Iridian—and ultra-sensitive government facilities guarded by high-end products, such as Iridian's IrisAccess 2200.

Tom Tallerico, a research engineer at the Department of Energy's Brookhaven National Laboratory (www.bnl.gov), has extensive experience working with biometrics. Part of his job entails deciding on the best means of providing access to secure areas at Brookhaven, such as the Relativistic Heavy Ion Collider research facility. Having worked with a variety of access-control technologies—including retinal scanning, hand geometry recognition, and iris scanning—Tallerico says users prefer the non-intrusive, no-contact-required operation of iris scanning compared to other biometric platforms.

About Face

Facial recognition is also leading the pack of sexy technologies transitioning into mainstream reality. As with most biometrics apps, many vendors are getting their hands wet in this field, using various proprietary algorithms and techniques in their products. However, there are essentially four primary groups that make up the underlying foundation of the various technologies.

The crudest of the four is probably AFP (Automatic Face Processing), which looks at a facial image, finds key features, and measures distances and angles between them. For example, a system might measure how far it is from the tip of the nose to the right corner of the mouth or where the eyes are in relation to other facial features. By comparing these parameters to the measurements taken of an individual, software can decide if a match is warranted.

Another facial recognition technology is eigenfaces, developed by MIT (www-white.media.mit.edu/vismod/demos/facerec/basic.html). In this process, an individual's face is compared to a database of 128 "global faces," pulling similar features, such as eyes, ears, a nose, and a mouth, from different global faces to compile a virtual composite, or eigenface. Each global face and each feature—eigeneye, eigenear, and so on—is numbered. The software notes the global face each feature was compiled from and compiles a numerical face template. As with most biometric applications, the template is used for future authentication or for verifying a person is who he claims to be or for determining a person's identity from a pool of many possibilities.

Neural Network Mapping technology looks at each feature in the enrolled face and the face of the individual seeking verification. An algorithm decides if the two features match and assigns that feature either a match or no-match designation. A goal of Neural Network Mapping is to adapt and learn in an intelligent fashion which features provide the most reliable verification or authentication possibilities for a certain face, thus improving the reliability of future operations.

The fourth technology, and the one probably used most widely, is Feature Analysis. LFA (Local Feature Analysis) is a version of this technology that Visionics (www.visionics.com) favors. Visionics produces FaceIt, a popular facial recognition product. The company recently announced a merger with Identix (www.identix.com), another major presence in the biometrics world. LFA works on the assumption that you can construct any facial image using an "irreducible set of building elements." The template that's produced, called a faceprint, is constructed by arranging these building blocks into an image that matches the face of the person being enrolled and then recording which block went where. The resulting file is just 84 bytes, which permits very fast manipulation during actual use.

Eigenface is one form of facial recognition technology in use at MIT. The process compares a user's face to 128 "global faces" in a database to make a composite out of comparable features.

Put Your Best Face Forth

Facial recognition products are showing up everywhere, for authentication and identification purposes on still image and live video surveillance systems. Casinos use the technology to watch for known professional gamblers. Law enforcement agencies use it as a sentinel for known criminals. IBM's snap-on UltraPort II camera ($99; www.pc.ibm.com/us/thinkpad/index.html) for the company's X, T, and A series ThinkPad notebooks bundles Visionics' FaceIt software, which unlocks the screen saver when an authorized face appears in the field of view of the computer's camera.

Visually based biometric technologies, particularly iris scan and facial recognition, are constantly being deployed in new locations. So the next time you have that nagging feeling someone is watching you, smile for the camera. And try not to blink.

FINGERPRINT & HAND RECOGNITION

Get A Feel For These Biometric Technologies

If you've ever had the distinct pleasure of being loaded into the back of a cruiser and hauled to the county lockup, you remember with pride having your fingers pressed into ink and rolled across a 10-print card. (Even if your record is squeaky clean, you've at least seen Sipowicz haul some poor slob into the precinct for the treatment, right?). Well, that inkpad/paper card ritual is giving way in many departments to glass and silicon in the form of biometric fingerprint technology.

Law enforcement is just one area where biometric methods are being used for identification and verification purposes, but it may be the most visible. Bryan Hall, Lee County Jail administrator in Tupelo, Miss., says that jail uses Identix's TouchPrint 2000 (www.identix.com) to input suspects' fingerprints into a database. TouchPrint acquires prints via an optical scanning process. No ink. No mess. Little fuss.

"I love it," Hall says. "We used to have to send in ink cards [to a state agency], and sometimes we got back as much as 70% as rejects. With this system, the rejects are around zero."

Lee County has been using the system for about two years. Hall says prints are typically stored in the computer systems of the law enforcement agency that captured them. They are also routed to a central state agency, and most prints from suspected felons are sent to the FBI. Once prints are acquired, authorities can search for matches in various databases and compare latent prints gathered at crime scenes.

Tools Of The Trade

There are essentially three primary technologies used in electronic fingerprint recognition. Optical scanning is the most common, followed by silicon-based scanning and then ultrasound. In optical scanning, a finger or thumb is placed on a small, flat glass or plastic plate. A light in the scanner illuminates the bottom of the finger, and a CCD captures an image of the print.

Silicon-based scanning, a method rapidly growing in use, generally entails a silicon surface acting as part of a capacitor, while the surface of the finger acts as another part. The silicon is divided into a tightly packed grid of rows and columns, with as many as 200 increments per centimeter. The device captures the nuances of the ridges and spaces on a finger with exceptional detail. Silicon sensors are showing up in a variety of computer peripherals, including Siemens' ID Mouse ($99 to $119; www.siemensidmouse.com). Such sensors eliminate the need for using PINs and passwords for verification and identification purposes. Simply touch the pad and you gain access to a system.

Some experts are touting ultrasound methods as the fingerprint scanning technology of the future. Ultrasound methods bombard a fingertip with acoustic waves, measuring the impedance of the finger in extremely fine detail to yield images with great resolution. Ultrasound also has a better ability to see through dirt on fingers or smudges on plates, which can cause poor readings in other recognition methods.

During the acquisition of prints, images undergo various phases of digital cleanup and sharpening. Various vendors—and there are a lot of them—have their own proprietary algorithms to handle the analysis, comparison, and verification of fingerprints. Although manual processing of fingerprint images is possible on most systems, the cleanup that takes place during the acquisition phase is internal to the system and transparent to the operator.

Book Em', Danno

The method in which electronic fingerprints are processed depends largely on the intended use. The methods generally fall into one of two large camps: AFIS (Automated Fingerprint Identification System) and non-AFIS. AFIS is the method law enforcement agencies use to acquire, process, store, and match fingerprints. Because of evidentiary needs, AFIS prints move through the system as intact images.

Non-AFIS fingerprints—referred to as finger-scans by the International Biometric Group (www.biometricgroup.com)—are handled differently after the acquisition stage, primarily in an effort to break free from the criminal stigma attached to fingerprinting. A few products work by creating vector-based maps of the ridges on a fingerprint. Most finger-scan systems, however, index prints based on unique features called minutiae.

Minutiae deal with characteristics of the ridges on a fingerprint, with ridge endings being the termination points. A ridge can divide into two ridges, known as a bifurcation. Other minutiae are known as crossover points, islands, deltas, and dots. You may also hear other characteristics used for comparisons referred to as whorls, loops, and arches.

In many systems, software algorithms find minutiae and mark their locations in reference to a map-like grid that uses x- and y-axes. Some systems mark the location of a minutiae point in relation to a fingerprint's core. Other systems set a 0,0 grid home at the bottom-left corner of a print. The information compiled for each minutiae point typically includes distance and direction from 0,0, as well as the angle at which the feature resides on the fingertip. Once a minutiae map is formed, it's stored as a template (anywhere from 200 bytes to 1,000 bytes in size). Compared to image files, authorities can search these templates at extremely high speeds. Privacy is also less of a concern here because the image is discarded and can't be reconstructed from the template.

Simply put, electronic fingerprints are well suited for both the authentication and identification of a person from a database containing scores of prints. For example, incorporating fingerprint identification hardware and software into a device, such as a mouse or keyboard, is far more effective than requiring the use of a PIN or ID card to verify the identity of employees with access to certain computers in highly secure work environments. A common identification example is the matching of latent prints from a crime scene to those in a criminal database.

Talk To The Hand

Although biometric fingerprint technology is in fairly wide use, it's not the only game in town. Hand geometry biometrics is also growing, mainly as a verification method. A typical process involves providing a person, such as an employee, with an ID card or PIN. Software takes dozens of precise measurements of the employee's hand, including for width, length, thickness, and surface area. From the measurements, the software creates a template.

Let's say an employee needs access to an area of a building. The user swipes an ID card or enters a PIN at the entry point. Software matches the ID or PIN to a corresponding profile in a database, which also contains the hand geometry template. The employee places his hand palm down in a device, which performs extremely quick measurements of the hand to create a profile that is compared against the template in the database. If they match, you're in. Some devices—including some at Disney entry points for season pass holders—measure two fingers instead of the entire hand.

A high-profile example of hand geometry technology is INSPASS (Immigration and Naturalization Service Passenger Accelerated Service System), in place at some major airports (see www.ins.usdoj.gov/graphics/howdoi/inspass.htm for more information) to let frequent travelers bypass immigration lines. Another major project is known as Basel, which will use Recognition Systems' HandReader technology (www.recogsys.com/index.shtml) at access points in Israel. Basel is expected to use hand geometry and facial recognition technology.

ANATOMY OF A FINGER-SCAN

Below are some of the usual steps taken in a typical process for acquiring a fingerprint using a non-AFIS (Automated Fingerprint Identification System) method.

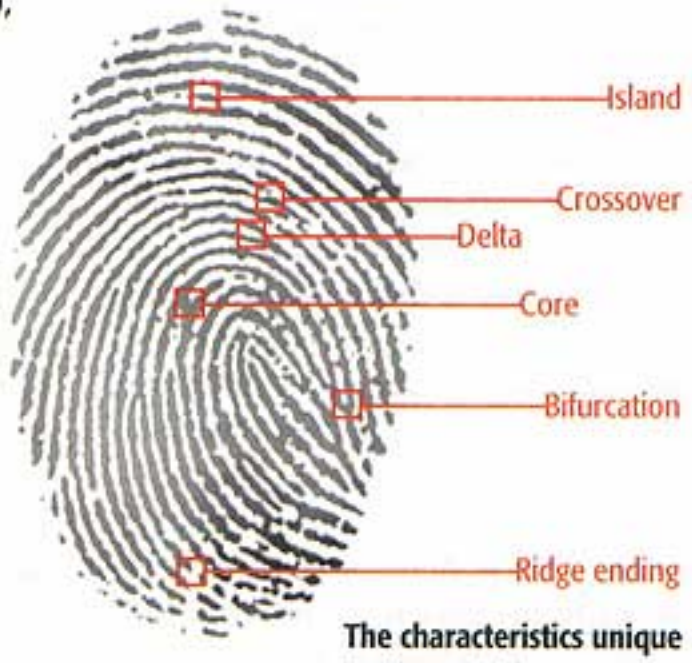
To start, a fingerprint is scanned into a system using a device that typically utilizes an optical scanning, silicon-based, or ultrasound technology.

After the print is acquired, software marks minutiae, which are unique characteristics of a print, including ridge endings, bifurcations (ridge divisions), crossover points, islands, deltas, and more. Algorithms are then used to locate these minutiae.

Once minutiae are identified and stored, the image is discarded, leaving behind a minutiae map that's saved as a template and one that corresponds to the person from whom the print was taken. The template can then be referenced later for various identification and verification purposes.

Fingerprint

Fingerprint with minutiae marks.



The characteristics unique to fingerprints.

Because the similarity of hand geometries among some people is more common than in other biometrics, the technology isn't typically used in identification systems. However, hand geometry is reliable enough for verification tasks because a reading from a user must match the template encoded on an accompanying ID card or PIN.

Although fingerprint and hand geometry technologies continue to rapidly improve, fingerprint methods in particular is still not quite as easy to use as vendors would have us believe. The primary bottleneck is in the acquisition stage, where inconsistent operator skill, dirt, scars, and other factors often make it hard to acquire a quality print.

Still, these methods beat having your finger plopped in ink—especially if looking at five to 10.

VOICE & MOVEMENT

Biometrics That Listen & Watch What You Say

As vendors of biometric applications continue their quests for the perfect authentication and identification products—be they voice or facial recognition, fingerprint or iris/retinal scanning, or hand geometry methods—individual biometrics have inherent strengths and weaknesses. One weakness is the difficulty some users have participating in particular processes. For example, someone with severe arthritis may not be able to reliably flatten a finger on a fingerprint scanner. In addition, many people are uncomfortable having a strong light beamed in their eyes, a requirement in some retinal scanning processes.

In addition to user difficulty, reliability of various methods is a primary concern. There's little to no room for error in a biometric solution that grants Johnny Laser access to a top-secret government facility housing a missile defense system.

In terms of comfort, the biometric of voice verification may be the least intrusive biometric platform in use, requiring nothing more of a user than speaking into a microphone. Voice verification differs from voice recognition in that it matches a voice to a particular user, as opposed to using a computer to translate spoken words into digital text.

A Distinct Voice

Veritel (www.veritelcorp.com) is one company offering a line of voice verification products. According to the company, the products analyze unique vocal features, such as cadence, pitch, tone, harmonics, and the shape of a user's larynx, to create a voiceprint as unique to a person as his or her fingerprints. During an enrollment process, the user is prompted to speak a certain phrase. At first glance, a graphical representation of that spoken phrase looks similar to those of other users. Upon closer examination of small areas of the speech file, however, differences are noticeable. It's these distinct patterns that represent the acoustic nuances unique to the vocal tract of one individual.

One obvious problem with voice verification is that a person's voice doesn't always sound the same. A person sounds different when they have a cold or are otherwise ill. Many people sound different in the precoffee hours. Some vendors claim their technologies take these factors into account, but we've also seen disclaimers that read something such as "If a verification attempt fails, try the verification again." Some might surmise this as being a tactical admission that the system may not be dependable enough for crucial situations.

Another potential shortcoming is the possibility of using a recording from an authorized user to grant access to the wrong person into a secure area. Some vendors insist this isn't possible because algorithms are able to decipher the difference between a human voice and an acoustic speaker in a playback device. This may be true in most circumstances, but digital recording and playback technology are making their own advances. In light of this, some users are reluctant to bet the farm based on vendor assertions.

One way in which such risks are being mitigated is multimodal biometric technology. In this approach, authentication relies on a combination of more than one biometric measurement. BioID (www.bioid.com) is one company that uses a multimodal approach. To enroll in a typical BioID-enabled setting, the user looks into a camera and speaks his or her name several times. Three separate reference files are then created for future comparison and verification.

The first reference file is a voiceprint. The second a facial template, such as those used in facial recognition applications. The third is an analysis of how the user's lips move when he speaks his name. The lip recognition component locates the mouth by searching the image for a contrasting section of pixels in the approximate shape of a mouth. Once this portion of the image is detected, it is isolated and a set of vectors is drawn around the outline of the lips. The movements of these vectors in relation to a virtual grid are recorded, reduced to numerical values, and stored as a template.

After enrollment, requesting access to information or a location entails the user looking into the camera and speaking his name. All three parameters are compared, and access is granted or denied. The obvious benefit of a multimodal approach is that the chance of falsely confirming the wrong user on all three of these biometric measurements is miniscule.

You can experience this technology firsthand by downloading a demo version of BioID SOHO at www.bioid.com/cgi-bin/download_demo.pl. The package replaces your Windows logon procedure with the three-part verification technology described above. A camera and microphone are required to use the software.