A Practical Guide to Biometric Security Technology

Simon Liu and Mark Silverman

As organizations search for more secure authentication methods for user access, e-commerce, and other security applications, biometrics is gaining increasing attention. But should your company use biometrics? And, if so, which ones should you use and how do you choose them? There is no one best biometric technology. Different applications require different biometrics.

To select the right biometric for your situation, you will need to navigate through some complex vendor products and keep an eye on future developments in technology and standards. Your options have never been more diverse. After years of research and development, vendors now have several products to offer. Some are relatively immature, having only recently become commercially available, but even these can substantially improve your company's information security posture. We briefly describe some emerging biometric technologies to help guide your decision making.

WHAT IS A BIOMETRIC?

The security field uses three different types of authentication:

- Something you know—a password, PIN, or piece of personal information (such as your mother's maiden name);
- Something you have—a card key, smart card, or token (like a SecurID card); and/or
- Something you are—a biometric.

Of these, a biometric is the most secure and convenient authentication tool. It can't be borrowed, stolen, or forgotten, and forging one is practically impossible. (Replacement part surgery, by the way, is outside the scope of this article.)

Biometrics measure individuals' unique physical or behavioral characteristics to recognize or authenticate their identity. Common physical biometrics include fingerprints; hand or palm geometry; and retina, iris, or facial characteristics.

Behavioral characters include signature, voice (which also has a physical component), keystroke pattern, and gait. Of this class of biometrics, technologies for signature and voice are the most developed.

Figure 1 describes the process involved in using a biometric system for security.

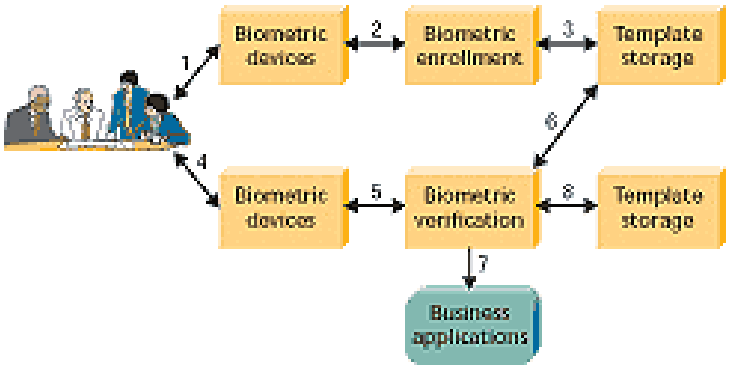

Figure 1. How a Biometric System Works.

(1) Capture the chosen biometric; (2) process the biometric and extract and enroll the biometric template; (3) store the template in a local repository, a central repository, or a portable token such as a smart card; (4) live-scan the chosen biometric; (5) process the biometric and extract the biometric template; (6) match the scanned biometric against stored templates; (7) provide a matching score to business applications; (8) record a secure audit trail with respect to system use.

Fingerprints

A fingerprint looks at the patterns found on a fingertip. There are a variety of approaches to fingerprint verification. Some emulate the traditional police method of matching minutiae; others use straight pattern-matching devices; and still others are a bit more unique, including things like moiréfringe patterns and ultrasonics. Some verification approaches can detect when a live finger is presented; some cannot.

A greater variety of fingerprint devices is available than for any other biometric. As the prices of these devices and processing costs fall, using fingerprints for user verification is gaining acceptance—despite the common-criminal stigma.

Fingerprint verification may be a good choice for in-house systems, where you can give users adequate explanation and training, and where the system operates in a controlled environment. It is not surprising that the workstation access application area seems to be based almost exclusively on fingerprints, due to the relatively low cost, small size, and ease of integration of fingerprint authentication devices.

Hand geometry

Hand geometry involves analyzing and measuring the shape of the hand. This biometric offers a good balance of performance characteristics and is relatively easy to use. It might be suitable where there are more users or where users access the system infrequently and are perhaps less disciplined in their approach to the system.

Accuracy can be very high if desired, and flexible performance tuning and configuration can accommodate a wide range of applications. Organizations are using hand geometry readers in various scenarios, including time and attendance recording, where they have proved extremely popular. Ease of

integration into other systems and processes, coupled with ease of use, makes hand geometry an obvious first step for many biometric projects.

Retina

A retina-based biometric involves analyzing the layer of blood vessels situated at the back of the eye. An established technology, this technique involves using a low-intensity light source through an optical coupler to scan the unique patterns of the retina. Retinal scanning can be quite accurate but does require the user to look into a receptacle and focus on a given point. This is not particularly convenient if you wear glasses or are concerned about having close contact with the reading device. For these reasons, retinal scanning is not warmly accepted by all users, even though the technology itself can work well.

Iris

An iris-based biometric, on the other hand, involves analyzing features found in the colored ring of tissue that surrounds the pupil. Iris scanning, undoubtedly the less intrusive of the eye-related biometrics, uses a fairly conventional camera element and requires no close contact between the user and the reader. In addition, it has the potential for higher than average template-matching performance. Iris biometrics work with glasses in place and is one of the few devices that can work well in identification mode. Ease of use and system integration have not traditionally been strong points with iris scanning devices, but you can expect improvements in these areas as new products emerge.

Face

Face recognition analyzes facial characteristics. It requires a digital camera to develop a facial image of the user for authentication. This technique has attracted considerable interest, although many people don't completely understand its capabilities. Some vendors have made extravagant claims—which are very difficult, if not impossible, to substantiate in practice—for facial recognition devices. Because facial scanning needs an extra peripheral not customarily included with basic PCs, it is more of a niche market for network authentication. However, the casino industry has capitalized on this technology to create a facial database of scam artists for quick detection by security personnel.

Signature

Signature verification analyzes the way a user signs her name. Signing features such as speed, velocity, and pressure are as important as the finished signature's static shape. Signature verification enjoys a synergy with existing processes that other biometrics do not. People are used to signatures as a means of transaction-related identity verification, and most would see nothing unusual in extending this to encompass biometrics. Signature verification devices are reasonably accurate in operation and obviously lend themselves to applications where a signature is an accepted identifier. Surprisingly, relatively few significant signature applications have emerged compared with other biometric methodologies. But if your application fits, it is a technology worth considering.

Voice

Voice authentication is not based on voice recognition but on voice-to-print authentication, where complex technology transforms voice into text. Voice biometrics has the most potential for growth, because it requires no new hardware—most PCs already contain a microphone. However, poor quality and ambient noise can affect verification. In addition, the enrollment procedure has often been more complicated than with other biometrics, leading to the perception that voice verification is not user friendly. Therefore, voice authentication software needs improvement. One day, voice may become an additive technology to finger-scan technology. Because many people see finger scanning as a higher authentication form, voice biometrics will most likely be relegated to replacing or enhancing PINs, passwords, or account names.

USES FOR BIOMETRICS

Security systems use biometrics for two basic purposes: to verify or to identify users. Identification tends to be the more difficult of the two uses because a system must search a database of enrolled users to find a match (a one-to-many search). The biometric that a security system employs depends in part on what the system is protecting and what it is trying to protect against.

Physical access

For decades, many highly secure environments have used biometric technology for entry access. Today, the primary application of biometrics is in physical security: to control access to secure locations (rooms or buildings). Unlike photo identification cards, which a security guard must verify, biometrics permit unmanned access control. Biometric devices, typically hand geometry readers, are in office buildings, hospitals, casinos, health clubs, and even a Moose lodge. Biometrics are useful for high-volume access control. For example, biometrics controlled access of 65,000 people during the 1996 Olympic Games, and Disney World uses a fingerprint scanner to verify season-pass holders entering the theme park.

Engineers are developing several promising prototype biometric applications to support the International Air Transport Association's Simplifying Passenger Travel (SPT) initiatives. One such program is EyeTicket, which Charlotte/Douglas International Airport in North Carolina and Flughafen Frankfurt/Main Airport in Germany are evaluating. EyeTicket links a passenger's frequent-flyer number to an iris scan. After the passenger enrolls in the system, an unmanned kiosk performs ticketing and check-in (without luggage).

The US Immigration and Naturalization Service's Passenger Accelerated Service System uses hand geometry to identify and process preenrolled, low-risk frequent travelers through an automated immigration system. Currently deployed in nine international airports, including Washington Dulles International, this system uses an unmanned kiosk to perform citizenship-verification functions.

Virtual access

For a long time, biometric-based network and computer access were areas often discussed but rarely implemented. Recently, however, the unit price of biometric devices has fallen dramatically, and several designs aimed squarely at this application are on the market. Analysts see virtual access as the application that will provide the critical mass to move biometrics for network and computer access from the realm of science-fiction devices to regular system components. At the same time, user demands for virtual access will raise public awareness of the security risks and lower resistance to the use of biometrics.

Physical lock-downs can protect hardware, and passwords are currently the most popular way to protect data on a network. Biometrics, however, can increase a company's ability to protect its data by implementing a more secure key than a password. Using biometrics also allows a hierarchical structure of data protection, making the data even more secure: Passwords supply a minimal level of access to network data; biometrics, the next level. You can even layer biometric technologies to enhance security levels.

E-commerce applications

E-commerce developers are exploring the use of biometrics and smart cards to more accurately verify a trading party's identity. For example, many banks are interested in this combination to better authenticate customers and ensure non-repudiation of online banking, trading, and purchasing transactions. Point-of-sales (POS) system vendors are working on the cardholder verification method, which would enlist smart cards and biometrics to replace signature verification. MasterCard estimates that adding smart-card-based biometric authentication to a POS credit card payment will decrease fraud by 80 percent.

Some are using biometrics to obtain secure services over the telephone through voice authentication. Developed by Nuance Communications, voice authentication systems are currently deployed nationwide by both the Home Shopping Network and Charles Schwab. The latter's marketing catch phrase is "No PIN to remember, no PIN to forget."

Covert surveillance

One of the more challenging research areas involves using biometrics for covert surveillance. Using facial and body recognition technologies, researchers hope to use biometrics to automatically identify known suspects entering buildings or traversing crowded security areas such as airports. The use of biometrics for covert identification as opposed to authentication must overcome technical challenges such as simultaneously identifying multiple subjects in a crowd and working with uncooperative subjects. In these situations, devices cannot count on consistency in pose, viewing angle, or distance from the detector.

THE FUTURE OF BIOMETRICS

Although companies are using biometrics for authentication in a variety of situations, the industry is still evolving and emerging. To both guide and support the growth of biometrics, the Biometric Consortium formed in December 1995. The recent Biometric Consortium annual conference highlighted two important areas.

Standardization

The biometrics industry includes more than 150 separate hardware and software vendors, each with their own proprietary interfaces, algorithms, and data structures. Standards are emerging to provide a common software interface, to allow sharing of biometric templates, and to permit effective comparison and evaluation of different biometric technologies.

The BioAPI standard released at the conference, defines a common method for interfacing with a given biometric application. BioAPI is an open-systems standard developed by a consortium of more than 60 vendors and government agencies. Written in C, it consists of a set of function calls to perform basic actions common to all biometric technologies, such as

- Enroll user,
- Verify asserted identity (authentication), and
- Discover identity.

Not surprising, Microsoft, the original founder of the BioAPI Consortium, dropped out and developed its own BAPI biometric interface standard.

Another draft standard is the Common Biometric Exchange File Format, which defines a common means of exchanging and storing templates collected from a variety of biometric devices. The Biometric

Consortium has also presented a proposal for the Common Fingerprint Minutia Exchange format, which attempts to provide a level of interoperability for fingerprint technology vendors.

Biometric assurance—confidence that a biometric device can achieve the intended level of security—is another active research area. Current metrics for comparing biometric technologies, such as the crossover error rate and the average enrollment time, are limited because they lack a standard test bed on which to base their values. Several groups, including the US Department of Defense's Biometrics Management Office, are developing standard testing methodologies. Much of this work is occurring within the contextual framework of the Common Criteria, a model that the international security community developed to standardize evaluation and comparison of all security products (Kimberly Caplan, "Building an International Security Standard," IT Professional, Mar.-Apr. 1999).

Hybrid technology uses

One of the more interesting uses of biometrics involves combining biometrics with smart cards and public-key infrastructure (PKI). A major problem with biometrics is how and where to store the user's template. Because the template represents the user's personal characters, its storage introduces privacy concerns. Furthermore, storing the template in a centralized database leaves that template subject to attack and compromise. On the other hand, storing the template on a smart card enhances individual privacy and increases protection from attack, because individual users control their own templates.

Vendors enhance security by placing more biometric functions directly on the smart card. Some vendors have built a fingerprint sensor directly into the smart card reader, which in turn passes the biometric to the smart card for verification. At least one vendor, Biometric Associates, has designed a smart card that contains a fingerprint sensor directly on the card. This is a stronger secure architecture because cardholders must authenticate themselves directly to the card.

PKI uses public- and private-key cryptography for user identification and authentication. It has some advantages over biometrics: It is mathematically more secure, and it can be used across the Internet. The main drawback of PKI is the management of the user's private key. To be secure, the private key must be protected from compromise; to be useful, the private key must be portable. The solution to these problems is to store the private key on a smart card and protect it with a biometric.

In the Smart Access common government ID card program, the US General Services Administration is exploring this marriage of biometrics, smart cards, and PKI technology. The government of Finland is also considering using these technologies in deploying the Finnish National Electronic ID card.

SELECTING A BIOMETRIC TECHNOLOGY

Biometric technology is one area that no segment of the IT industry can afford to ignore. Biometrics provide security benefits across the spectrum, from IT vendors to end users, and from security system developers to security system users. All these industry sectors must evaluate the costs and benefits of implementing such security measures.

Different technologies may be appropriate for different applications, depending on perceived user profiles, the need to interface with other systems or databases, environmental conditions, and a host of other application-specific parameters (see **Table 1**).

Table 1. Comparison of Biometrics

Characteristic	Fingerprints	Hand Geometry	Retina	Iris	Face	Signature	Voice
Ease of Use	High	High	Low	Medium	Medium	High	High
Error incidence	Dryness, dirt, age	Hand injury, age	Glasses	Poor Lighting	Lighting, age, glasses, hair	Changing signatures	Noise, colds, weather
Accuracy	High	High	Very High	Very High	High	High	High
Cost	*	*	*	*	*	*	*
User acceptance	Medium	Medium	Medium	Medium	Medium	Medium	High
Required security level	High	Medium	High	Very High	Medium	Medium	Medium
Long-term stability	High	Medium	High	High	Medium	Medium	Medium

***The large number of factors involved makes a simple cost comparison impractical.**

Ease of use

Some biometric devices are not user friendly. For example, users without proper training may experience difficulty aligning their head with a device for enrolling and matching facial templates.

Error incidence

Two primary causes of errors affect biometric data: time and environmental conditions. Biometrics may change as an individual ages. Environmental conditions may either alter the biometric directly (for example, if a finger is cut and scarred) or interfere with the data collection (for instance, background noise when using a voice biometric).

Accuracy

Vendors often use two different methods to rate biometric accuracy: false-acceptance rate or false-rejection rate. Both methods focus on the system's ability to allow limited entry to authorized users. However, these measures can vary significantly, depending on how you adjust the sensitivity of the mechanism that matches the biometric. For example, you can require a tighter match between the measurements of hand geometry and the user's template (increase the sensitivity). This will probably decrease the false-acceptance rate, but at the same time can increase the false-rejection rate. So be careful to understand how vendors arrive at quoted values of FAR and FRR.

Because FAR and FRR are interdependent, it is more meaningful to plot them against each other, as shown in **Figure 2**. Each point on the plot represents a hypothetical system's performance at various sensitivity settings. With such a plot, you can compare these rates to determine the crossover error rate. The lower the CER, the more accurate the system.

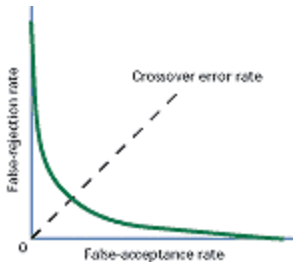

Figure 2. Crossover error rate attempts to combine two measures of biometric accuracy.

Generally, physical biometrics are more accurate than behavioral biometrics.

Cost

Cost components include

- Biometric capture hardware;
- Back-end processing power to maintain the database;
- Research and testing of the biometric system;
- Installation, including implementation team salaries;
- Mounting, installation, connection, and user system integration costs;
- User education, often conducted through marketing campaigns;
- Exception processing, or handling users who cannot submit readable images because of missing appendages or unreadable prints;
- Productivity losses due to the implementation learning curve; and
- System Maintenance.

User acceptance

Generally speaking, the less intrusive the biometric, the more readily it is accepted. However, certain user groups—some religious and civil-liberties groups—have rejected biometric technologies because of privacy concerns.

Required security level

Organizations should determine the level of security needed for the specific application: low, moderate, or high. This decision will greatly impact which biometric is most appropriate. Generally, behavioral biometrics are sufficient for low-to-moderate security applications; physical biometrics, for high-security applications.

Long-term stability

Organizations should consider a biometric's stability, including maturity of the technology, degree of standardization, level of vendor and government support, market share, and other support factors. Mature and standardized technologies usually have stronger stability.

Biometric technology has been around for decades but has mainly been for highly secretive environments with extreme security measures. The technologies behind biometrics are still emerging. This article gives a snapshot of the dynamics under way in this emerging biometric market, and we hope it will help you consider all the possible alternatives when acquiring new biometric technologies.

Simon Liu is director of computer and communications systems at the National Library of Medicine. He is also an adjunct professor at Johns Hopkins University. Contact him at simon_liu@nlm.nih.gov .

Mark Silverman is a technical advisor at the Center of Information Technology, National Institutes of Health. Contact him at mls@nih.gov .

Resources

- *The Biometric Consortium*: Serves as the US government's focal point for research, development, test, evaluation, and application of biometric-based personal identification and verification technologies.
- *Association for Biometrics:* Aims to promote the awareness and development of biometrics-related technologies. It provides an international forum for research and development, system design and integration, application development, market development, and other issues.
- *Avanti*: A reference site for biometrics, Avanti contains considerable amount of background information about biometrics, their use in everyday business situations and how to deploy them.
- *Biometrics: Journal of the International Biometric Society*: Published quarterly, *Biometrics* aims to promote and extend the use of mathematical and statistical methods in various disciplines. It describes and exemplifies developments in these methods and their application for experimenters and those primarily concerned with data analysis.
- *International Biometric Industry Association*: A trade association founded in September 1998 in Washington, D.C., to advance, advocate, defend, and support the biometric industry's collective international interests. Governed by and for biometric developers, manufacturers, and integrators, IBIA aims to serve all biometric technologies in all applications.

GLOSSARY

Crossover error rate (CER)—a comparison metric for different biometric devices and technologies; the error rate at which FAR equals FRR. The lower the CER, the more accurate and reliable the biometric device.

Enrollment—the initial process of collecting biometric data from a user and then storing it in a template for later comparison.

False-acceptance rate (FAR)—the percentage of imposters incorrectly matched to a valid user's biometric.

False-rejection rate (FRR)—the percentage of incorrectly rejected valid users.

Identification—the process by which the biometric system identifies a person by performing a one-to-many (1:*n*) search against the entire enrolled population.

Template—a mathematical representation of biometric data. A template can vary in size from 9 bytes for hand geometry to several thousand bytes for facial recognition.

Verification—the authentication process by which the biometric system matches a captured biometric against the person's stored template (1:1).