Biometrics Boosts Identity Assurance

August 2020

Adam Shane, PSP MSEE
Systems Integration Manager

Advances in biometrics—the use of physical or behavioral characteristics to digitally verify personal identity—are being used with increasing frequency in a variety of applications to help keep facilities and information secure.

Today, various applications capture and use a slew of distinctive human characteristics (also called "modalities"), including fingerprints, palm-vein patterns, facial features, or iris or retina traits, to authenticate a person's identity. Other applications use behavioral characteristics, such as the way an individual walks, talks or types, to verify identity.

Authenticating Biometrics

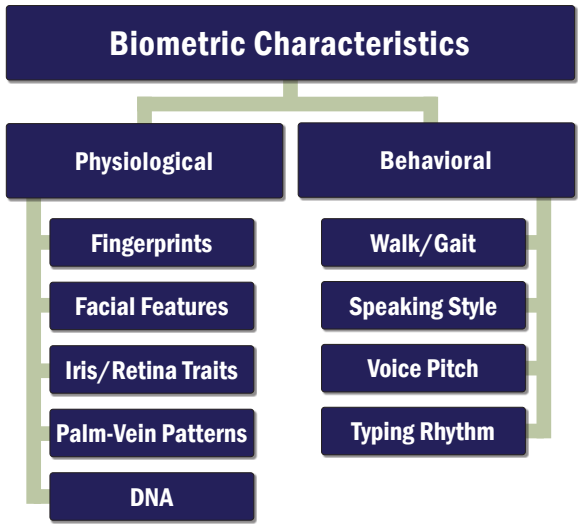
Biometric authentication is used in several different ways . The most common is multi-factor authentication, using biometrics in conjunction with an access token and PIN or password, for example, to gain access to a facility or computer system. Biometrics also are used to identify a specific user from a population of known persons, relying on a bank of previously obtained and vetted information and characteristics.

> **"To be effective, biometrics must be: consistent, persistent, measurable, and unique to the individual..."**

To be effective, biometrics must be: consistent, persistent, measurable, and unique to the individual. Consistency ensures that the device capturing biometric information does so consistently from one presentation to another. Persistence means that the biometric information does not change over time. Measurable refers to the ability to capture the biometric information during the

initial "enrollment" period, convert it to a digital format suitable for a computer-matching algorithm, and store the resultant data. Uniqueness means that the biometrics collected are unique to each individual.

No biometric system is perfect, however, and several factors can impact its performance, namely its ability to match a biometric sample with the information previously captured at enrollment. In general, performance can be evaluated by looking at: 1) the failure-to-enroll rate, which measures the system's ability to "register" a person using supplied information; 2) the false-rejection rate, which measures inappropriate rejections; and 3) the false-acceptance rate, which measures erroneous identity confirmations. Performance benchmarks for each of these factors are determined by the specific application of the biometric system.



Biometrics are not Infallible

It also is important to remember that, while biometrics provide greater identity assurance than a simple password or key card, they are not infallible. Recent studies have confirmed that DNA, for example, considered to be one of the most accurate biometric measurements, is not unique to an individual if he or she has had a bone marrow transplant. (The transplant, in fact, gives the transplant recipient two distinct sets of DNA in their blood and saliva.) Biometrics is not an exact science and relies heavily on empirical evidence to gauge its success. As a result, when designing a biometric system, it is prudent to consider the following:

Multi-factor authentication (MFA) employs several different identity "challenges," including possession of a token (such as a key card), knowledge of a secret (such as a password), a biometric (such as a physical characteristic), and the location of the request—all in an effort to provide the highest level of assurance of the claimed identity.

Masks can defeat facial recognition; contact lenses can defeat iris recognition; or latex molds can defeat fingerprint matching. As a result, the level of security a biometric system affords is determined by both error rates and the system's ability to detect and reject fakes.

When used to pick a person out of a vast database, the biometric matching algorithm must demonstrate a high level of accuracy and performance based on the size of the population. If a biometric matching system used at an airport, for example, has a real-world false acceptance rate of 1 in 1000, scanning a population of 50,000 would result in 50 false acceptances, on average. While this acceptance rate may be reasonable for a frequent-flier airport lounge, it would not be an acceptable rate for access to airport areas that demand more security. It is, therefore, vital to assess your specific security needs when evaluating biometric systems and their rates of performance.

Protecting Personally Identifiable Information

Care also should be taken to protect the registered biometric information, much of which is sensitive personally identifiable information (PII). If a user name and password are stolen, for example, they're easily changed to reinstate security. If highly unique biometric information is stolen, however, it cannot be changed, and the damage can be irreparable. As a result, PII data should be well and proactively protected, including the use of encryption when data is stored and transmitted.

"Care should also be taken to protect the registered biometric information, much of which is sensitive personally identifiable information (PII)."

Biometric authentication has a certain cachet, and presents seemingly boundless opportunities to boost security. The technology is not perfect, but it is improving, and requires careful planning and implementation to ensure that its practical, day-to-day use fulfills the facility owner's requirements.

Adam Shane, PSP, MSEE
Systems Integration Manager
ashane@burns-group.com
www.burns-group.com