Biometrics: An Overview of the Technology, Challenges and Control Considerations

By Michael P. Down, OCNP, and Richard J. Sands, CISSP, OCNP

Biometrics is an authentication mechanism that relies on the automated identification or verification of an individual based on unique physiological or behavioral characteristics. Physiological characteristics refer to inherited traits that are formed in the early embryonic stages of human development. Typical physiological features measured include an individual's fingerprints, face, retina, iris and hand. Behavioral characteristics are not inherited, but learned. Typical behavioral features that can be measured include voice patterns, handwriting and keystroke dynamics.

Biometrics as a concept has been around for thousands of years. History details that potters from East Asia signed their pottery by placing their fingerprint in the clay as it cured. In addition, traders from Egypt were identified by physical traits, such as height, weight, eye color, hair color and other physical features. During the 19th century, criminologists used fingerprints to help identify habitual criminals. It was not until the 1970s that biometrics as an automated technology first appeared. The first commercial applications for automated biometrics were used to control physical access to buildings. This trend has continued with the increasing need to reduce fraud and limit physical and logical security breaches.

Global events have amplified the need to increase the level of security awareness and the urgency to implement a secure environment. Also, improvements in computing performance coupled with a reduction in biometric solution implementation costs have made a strong case for the mainstream use of biometric technologies. Another factor in favor of this authentication method is its basis on "something you are" as compared to a password, which is "something you know and might forget," or tokens, which are "something you have and might lose."

Biometric technologies offer two means to determine an individual's identity: verification and identification. Verification confirms or denies a person's claimed identity by asking, "Is this person whom he/she claims to be?" Identification, also known as recognition, attempts to establish a person's identity by asking, "Who is the person?" Verification is a one-to-one comparison of the biometric sample with the reference template on file. A reference template is the enrolled and encoded biometric sample of record for a user. Identification makes a one-to-many comparison to determine a user's identity. It checks a biometric sample against all the reference templates on file. If any of the templates on file match the biometric sample, there is a good probability the individual has been identified.

Biometric Technologies

Many different types of unique physiological or behavioral characteristics exist for humans. Some of the more traditional uses of these biometric methods for identification or verification include:

- Fingerprint recognition—Fingerprint recognition systems rely on the biometric device's ability to distinguish the unique impressions of ridges and valleys made by an individual's finger.
- Hand geometry—Hand geometry solutions take more than 90 dimensional measurements to record an accurate spatial representation of an individual's hand.
- Retina scanning—Retinal scanning involves an electronic scan of the retina, the innermost layer of the wall of the eyeball.
- Iris scanning—Iris scanning uses a camera mounted between three and 10 feet away from the person to take a high-definition photograph of the individual's eyes. It then analyzes 266 different points of data from the trabecular meshwork of the iris.
- Facial recognition—Facial recognition attempts to identify a subject based on facial characteristics such as eye socket position, space between cheekbones, etc.
- Signature dynamics—Dynamic signature verification not only compares the signature itself, but also marks changes in speed, pressure and timing that occur during signing.
- Keystroke dynamics—Keystroke dynamics technology measures dwell time (the length of time a person holds down each key) as well as flight time (the time it takes to move between keys). Taken over the course of several login sessions, these two metrics produce a measurement of rhythm unique to each user.
- Voice recognition—Voice recognition biometrics digitize a profile of a person's speech into a template voiceprint and stores it as a table of binary numbers. During authentication, the spoken passphrase is compared to the previously stored template.

Other technologies that are emerging or that are being studied include vein patterns, facial thermography, DNA, sweat pores, hand grip, fingernail bed, body odor, ear shape, gait, skin luminescence, brain wave pattern, footprint recognition and foot dynamics.

Biometric technologies can be combined to provide enhanced security. This combined use of two or more biometric technologies in one application is called a multimodal biometric system. A multimodal system allows for an even greater level of assurance of a proper match in verification and identification systems. Multimodal systems

help overcome limitations of single biometric solutions, such as when a user does not have a quality biometric sample to present to the system (e.g., an individual with a cold attempts to authenticate to a voice recognition system) and to reduce the ability for the system to be tricked fraudulently.

Understanding Biometric Systems' Performance Measures

Performance measures are used to create baselines to help organizations evaluate products. The performance of a biometric system is based on measures such as false rejection rate, false acceptance rate, crossover rate, verification time and failure to enroll rate. Following is a brief description of these performance measures.

False rejection rate (FRR), also commonly referred to as a type I error, measures the percentage of times an individual who should be positively accepted is rejected—in other words, how many times the "good guys" cannot gain access. If users who should be granted access are repeatedly rejected, they will not have access to the protected application or location to perform their assigned duties. Biometrics vendors strive to have a low FRR.

False acceptance rate (FAR), also commonly referred to as a type II error, measures the percentage of times an individual who should be rejected is positively matched by the biometric system—how many times the "bad guys" beat the system. If an attacker gains access to a protected application or location, the security of the system has been breached. Biometrics vendors strive to have a low FAR.

Crossover rate, also referred to as the equal error rate (EER), is the point on a graph where the lines representing the FAR and FRR intersect. A lower crossover rate indicates a system with a good level of sensitivity and generally means the system will perform well.

Verification time is the average time taken for the actual matching process to occur.

Failure to enroll rate (FTER) is used to determine the rate of failed enrollment attempts. Factors such as quality of the enrollment equipment, ease of enrollment, environment surrounding enrollment and quality of the user's biometric influence the FTER.

It should be noted that vendors typically market products using measures based on laboratory tests in ideal situations. However, practical applications of these products show different statistical results and change the actual performance baseline. These differences are caused by factors such as user familiarity, network speeds, environmental effects and product design. Organizations and standards groups, such as the National Biometric Test Center, INCITS M1 and the ISO SC37 Biometrics group are working to provide real-world statistics on biometric systems so consumers have a better guide to a biometrics solution's true performance. As more effective standards become available, published performance measures will become more reliable, but organizations should still consider performing independent testing. These independent tests should be executed within the organization's own environment and user population guidelines to provide the best understanding of actual performance in the installed system.

Business Drivers of Biometrics

Increased Security and Convenience

Biometrics technology is designed to provide a greater degree of security than traditional authentication techniques since the biometric credentials are difficult to steal, lose, forget or compromise. Biometrics may be leveraged as a complementary form of authentication to increase security for a critical resource. In addition, biometrics systems are designed to improve the verifiability of IT audit trails and user accountability because the technology provides a higher level of confidence in the identity verification process.

Convenience is another goal. Unlike traditional authentication methods, a biometric is based on a user characteristic that is not easily lost or forgotten. For that reason, users would not have to remember as many passwords or worry about misplacing authentication tokens.

Enterprise Applicability

Biometric systems can be applied to areas across the enterprise requiring logical or physical access solutions. Biometric authentication readers for workstations can be integrated with desktop applications for logical authentication to provide a stronger alternative to a username and password. Biometric devices can also be used to control physical access to buildings, safes or rooms.

Biometric authentication integration efforts are becoming easier with the vendor adoption of industry standards, such as Biometric Application Programming Interface (BioAPI) and the Common Biometric Exchange File Format (CBEFF). The BioAPI is designed to provide a cross-platform interface that simplifies development and standardizes programmatic interaction with biometric devices. The CBEFF was developed to facilitate improved interoperability between biometrics systems and simplify hardware and software integration.

Privacy Impacts of Biometrics

The storage of the biometric is a digital representation that could be stolen, lost or otherwise compromised. Unauthorized access to biometric storage devices could present numerous issues, not the least of which is privacy. Misuse of a biometric is a serious issue, given that the biometric itself cannot be changed and once compromised continues to be an issue for the life of the donor. Even when used as intended, the biometric control results in the capture of personal information, such as fingerprints, iris scans, palm geometry, etc.

Individuals do not always have the choice to opt out of using biometrics because of policy requirements even if they are aware of the biometric use. Users may be required to use biometrics as a job requirement or to gain access to related systems or services. Some users may reject its use solely on the basis of the "Big Brother" principle, while others truly believe that the information may be misused to track their activities, falsify transactions or for other unauthorized purposes.

The adoption of biometrics systems is growing and will almost assuredly continue to gain momentum. Organizations must accept biometrics and determine the best approach to ensure that they are used appropriately, that the information

stored is adequately secured and that data collected on the user remain private. Data collection, storage methods and the consent of the persons from whom the data are being collected are key factors that must be closely examined during an audit or review. Legal considerations also must be clearly reviewed to determine the propriety of the collection process, storage and use, and the possible contingencies posed by the use of biometrics within an organization.

Control Considerations and Management Risks for Biometrics

Biometrics technologies present unique risks and need to be managed to allow an organization to achieve an acceptable return on its investment. The organization (management and auditors) should consider the following controls when evaluating, designing, implementing, maintaining and auditing biometric systems:

- Misuse of biometric data from social and business viewpoints—The adoption of privacy laws throughout the world requires an immediate determination of the applicable laws with regard to biometric data use. In the US, for example, laws such as the Health Insurance Portability and Accountability Act (HIPAA) contain important privacy restrictions.
- False negatives and positives—Organizations should consider the impact to the organization, from operational and reputational viewpoints, presented by the misuse of biometric controls. False negatives could hinder productivity, because valid individuals are prevented from accessing the system. False positives can present an opportunity for unauthorized access to the data and systems protected by the biometric control.
- Physical and logical controls over access to biometric data—The location of biometric storage is a key point in the consideration of controls. The organization should ensure that the underlying digital representation of the biometric is controlled as standing data during transmission, regardless of whether it is stored centrally, in single computers, or on a smart card or other device.
- Security of the computers hosting the application and databases—The organization should review access controls and configuration settings of the underlying computers and networks hosting and providing the communication channels for the biometrics controls in use. The organization should also ensure that the computers, network lines and equipment, and other equipment used in the authentication process have been secured and are being monitored on an ongoing basis to ensure their security.
- Audit trails—Proper audits trails are essential in ensuring proper use, maintenance and control of biometric systems. Audit trails should exist for all transactions used in the biometric process and should provide a mechanism to trace system users and their activity. Audit trail logs should be backed up and secured offsite to ensure their security and availability.
- Certification of software and hardware by vendor(s)—The vendor should properly test the software and hardware used by the biometric authentication process to ensure that it meets required standards. The organization should determine if steps have been taken to ensure that the vendor has supplied evidence and/or a certification of the software and hardware abilities.
- Auditor's role in selecting the system—The organization must determine that the system has been thoroughly reviewed to ensure compatibility with the existing network and legacy applications. The auditor can help by understanding the intended use of the system to determine that the biometric system chosen will comply with standards required for external systems with which it may interface.

Barriers to Future Growth

A successfully implemented biometrics application can help organizations address complex authentication issues. While it seems natural to expect that biometrics should be booming, in reality, only a few businesses and government agencies are testing or have deployed biometrics. Skeptics say the technology is still too expensive, is not foolproof, can be hard to integrate with other systems and requires employees to change the way they work. The following are some of the challenges organizations face trying to incorporate biometrics into their business processes:

- Technology is not foolproof—Interest probably will not start growing until biometrics systems overcome technical problems related to the reliability of the biometrics application.
- Cost of deployment—Deploying biometric readers on every door leading into a building or every PC on a network can be an expensive proposition. Hardware and software costs may not be the only consideration—the organization must bear in mind the associated complexity involved in enrolling new users and administering usage training.
- Accuracy—Verification and positive identification systems may allow unauthorized users to access facilities or resources as a result of incorrect matches. In a negative identification system, the result of a false match may be to deny access.
- Resistance to change—As with many technologies, some users would rather not change the way they do things. For example, some users have the perception that using a username and password to log onto a system is faster than using a fingerprint scanner. This perception may arise from frustration related to the FRR, a performance measure that tracks the percentage of times an individual who should be positively accepted is rejected.

Conclusion

Biometrics is poised to take off, but before this transformation can occur, obstacles such as overall cost, lack of globally accepted standards, interoperability, reliability and user perceptions must be overcome. Drivers such as governmental and commercial mandates to improve security and privacy, enterprise application integration, and the ongoing reduction in the cost of hardware will help overcome some of the barriers related to the widespread implementation of biometrics technology.

References

"BioAPI Consortium," 23 September 2003, *www.bioapi.org*

Bosner, Kevin; "How Facial Recognition Systems Work," *How Stuff Works*, 24 September 2003, *www.computer.howstuffworks.com/facial-recognition2.htm*

Hong, Lin; "Automatic Personal Identification Using Fingerprints," Ph.D. Thesis, 1998, *biometrics.cse.msu.edu/lin_thesis.pdf*

Jain, Anil. K.; L. Hong; and S. Pankanti; "Biometrics: Promising Frontiers for Emerging Identification Market," *Comm. ACM*, p. 91-98, February 2000, *www.cse.msu.edu/cgi-user/web/tech/document?ID=436*

Monrose, Fabian; Aviel D. Rubin; "Keystroke Dynamics as a Biometric for Authentication," *Future Generation Computer Systems*, The Netherlands, 1999, p. 351-359, *www.avirubin.com/fgcs.pdf*

National Institute of Standards and Technology. "Common Biometric Exchange File Format (CBEFF)," 24 September 2003, *www.itl.nist.gov/div895/isis/bc/cbeff/*

Prabhakar, Salil; S. Pankanti; A. K. Jain; "Biometric Recognition: Security & Privacy Concerns," *IEEE Security & Privacy Magazine*, volume 1, no. 2, 2003

Ross, Arun; "A Prototype Hand Geometry-based Verification System," *M.S. Project Report*, 1999, *biometrics.cse.msu.edu/RossHand_MS99.pdf*

"Understanding Signature Verification," Find Biometrics: Complete Identification Verification Source, 24 September 2003, *www.findbiometrics.com/Pages/signature%20 articles/signature_1.html*

US General Accounting Office, "Technology Assessment: Using Biometrics for Border Security," GAO-03-174, November 2002

Editor's Note:

The IT Governance Institute publication, *Risk and Control of Biometric Technologies: A Security, Audit and Control Primer*, is posted for ISACA members at *www.isaca.org/biometric*. This publication is intended to assist private and public sector senior management—CEOs, CFOs, CIOs, department/division heads worldwide, members of ISACA, and other IT audit, security and control professionals—in their understanding, use and control of biometrics technology. It provides:

- Business drivers associated with biometrics
- Current and future demand for biometrics technology
- Role and components of a biometrics system
- Processes involved in using a biometrics system for security
- Risks associated with biometrics
- Security and audit considerations for protecting biometrics systems
- Self-assessment questionnaire

Michael Down, OCNP
is a consultant with PricewaterhouseCoopers, specializing in the design and implementation of large-scale identity management solutions. His other accomplishments include the development of an enterprise security strategy.

Richard Sands, CISSP, OCNP
is a manager with PricewaterhouseCoopers and has more than 10 years' experience in information technology. He specializes in IT security, focusing on design, implementation and review of large-scale identity management solutions. Richard is a member of the Puget Sound Chapter of ISACA.

Information Systems Control Journal, formerly the IS Audit & Control Journal, is published by the *Information Systems Audit and Control Association*, Inc.. Membership in the association, a voluntary organization of persons interested in information systems (IS) auditing, control and security, entitles one to receive an annual subscription to the *Information Systems Control Journal*.