OneBeacon
TECHNOLOGY INSURANCE

A Member of OneBeacon Insurance Group®

Biometric Security: A Never Changing Approach to Security

Author: Norine McVann, Information Technology Risk Control

Published: October 2019

Executive Summary

Protecting and controlling access- whether to an office building or an operating system- is an ever evolving security challenge. With ongoing advancements in technology, the option to utilize biometric security controls is becoming more widely available. However, while these security techniques tend to be more secure than passwords or key cards, some biometric security methods have been criticized as invasive and even dehumanizing. Therefore, before committing to a method, stakeholders within any organization should thoroughly review biometric security methodology to better understand the positives and negatives and to make informed choices regarding security.

What is Biometric Security?

Biometric security uses an individual's physical characteristics (facial data or fingerprint) or behavioral characteristics (signature, gait, or key stroke pattern recognition) to automatically authenticate and provide access to a facility or system. Because this system of security evaluates an individual's body elements, biological or behavioral data for identity verification, it is the strongest and most foolproof physical security technique in use.[1]

Biometric security has practical applications in all aspects of security - from controlling access to a physical location such as an office building, airport or a sports arena to protecting critical electronic data and operating systems.

Biometric versus other authentication methods

Security authentication is measured in three ways:

- Something you know: a password, PIN, or personal information like where you were born.
- Something you have: a card key, smart card or token.
- Something you are: a biometric or an unchanging features or individual characteristics.[2]

Authenticating through something "known" or with a physical key or card are widely used methods. However they each carry significant drawbacks for security. We've all experienced forgetting a password or the confusion of having too many passwords. Many people, for convenience, write them all down leaving themselves vulnerable to having their passwords stolen. Passwords can also be easily guessed or determined through dictionary attacks, which is a process of gaining access into password protected servers or computers by systematically entering every word in the dictionary. Even though the majority of people know better in this digital age, some of the most common passwords continue to be "password", "12345678" and "iloveyou".[3]

Similarly, having a physical item, such as a card key or smart card, leaves security vulnerable to possible human error. These items can be lost, stolen, hacked or even simply loaned out to others by well intentioned, trusting individuals.

A Never Changing Approach to Security

Biometric authentication utilizes a unique part of the individual's behavior or biology and is therefore, always present. With this type of biometric security, there is nothing to remember, nothing to lose and overall it is more difficult to steal or copy.[4]

Three steps of Biometrics

Biometric systems work through a three step process:

- Enrollment: First, basic information about a person such as name or identification number is provided. The Biometric system then captures an image or recording of a person's specific trait that is being measured.
- Storage: The data collected is analyzed and stored onto a template which is then housed in a database. This data can be stored in a centralized database (e.g. storage of facial data for passports in use by Customs and Border Patrol) or on a local device (e.g. facial, iris or fingerprint data used to access a smart phone being stored solely on that smart phone).
- Comparison: The next time the biometric system is used, it compares the traits being presented against the template in the centralized or local device database to determine a match. It will either accept or reject who the person is claiming to be.[5]

Types of Biometric Techniques

There are a wide variety of techniques used to authenticate one or more individual physical characteristics. The unimodal or, single body trait, technique is most commonly used. This technique utilize a single trait, such as fingerprints, the retina or iris of the eye, hand geometry or facial recognition. Multimodal biometrics combines multiple biometric security techniques, such as voice and speech recognition, and provides an overall stronger authentication process.[6]

- Fingerprint recognition: The images of the ridges and valleys (minutiae) found on the surface of a person's finger tips can be captured using a scanning process. A mathematical representation (unique data set) of the person's finger print is created from the image. The hash of this unique data set is saved in the database, not the scanned image of the fingerprint.

  This is a one-way function, meaning that mathematically it is impossible to recreate the finger print image from this hashed data set. If the data is stolen or leaked, it cannot be reconverted to an image, and this eliminates the potential of someone recreating the finger print image from the underlying data.[7]

  However, finger print recognition is not completely foolproof. For example, capacitive scanners, which uses tiny capacitors just below the surface of the scanner to track the finger's friction ridges and valleys, can't always distinguish between a mold of a person's finger and the actual finger. An optical scanner, which uses an image sensor to capture the fingertip surface, could be spoofed by someone using a photo of another user's finger print.
- Retina recognition: This technique involves analyzing the layers and unique pattern of blood vessels situated in the back of the eye. This unique pattern can be scanned with the use of a low intensity light source through an optical coupler. Retinal scanning requires a person to look into a receptacle and focus on a given point. Drawbacks to this method include that it may not be very convenient for persons who wear glasses or are concerned about having contact with a reading device that is being used by a multitude of users.[8]
- Iris recognition: The features found in the iris of the eye, or the colored rings of tissue that surrounds the pupil, are unique to every person. Through the use of mathematical recognition techniques, the pattern can be captured and used for authentication. This technique does not require contact with a scanning/reading device, can operate at distance from the user, and requires only a glance. These features make it less intrusive and more convenient for users than the retinal recognition process.[9] However, the scanners require a person to stand in front of the device which is sensitive to movements and reflections such as eyelashes or lenses. An

untimely blink of an eye will obstruct the scanning device delaying the recognition process and requiring repeated attempts.

- Hand geometry: This technique uses the concept of measuring and recording length, width, thickness and surface area of an individual's hand while placed on a plate. Hand geometry systems use a camera to capture a silhouette image of the hand. The subject's hand is placed palm down on a plate and guided by five pegs that sense when the hand is in place. The image is evaluated and measured to create a template of the person's hand characteristics. Hand geometry recognition has been in use the longest, first marketed in the late 1980's and used at the 1996 Olympic Games to control and protect physical access to the Olympic Village.[10]
- Facial recognition: This technology measures and matches unique characteristics of the face, and is incredibly versatile with a wide range of potential applications. It has the potential to be integrated anywhere you can find a modern camera.

  Law enforcement agencies around the world use biometric software to scan faces in CCTV (Closed-circuit television) as well as to identify persons of interest in the field. Border Control uses this technique to verify the identity of travelers.

  Face recognition has the ability to gather demographic information and is an emerging technology for the retail industry to help in product marketing. There are those who oppose this technique because of the potential to "profile" and create discriminatory practices.[11]
- Voice and speech recognition: A voice print measures the sound a person makes while speaking, specifically the minutia of the voice. It is not wholly dependent on a spoken code. Speech recognition-- also called voice command-- uses a voice user interface (VUI) technology which allows users to interact and control technologies through speech. In other words, through the use of spoken words, computer software can recognize a voice and word sequence in tandem which can be integrated into security systems to allow or deny access to a restricted location or system. The combination of voice and speech recognition can be a powerful duo simultaneously providing both authentication and hands free interface.[12]

These are just some of the biometric security techniques that can be used to measure and analyze individual traits. There are many other traits, such as a person's manner of walking, moving or writing/typing which can also be measured and used for authentication.

Concerns with Biometrics

While utilizing a biometric system is proven to be safer than other methods of authentication, there are several concerns from both an organizational and individual perspective.

- Ease of use: Depending on the intended application, a quick user interface that does not require physical contact with a reader device is more likely to be well received and considered less intrusive. This is particularly true in applications where large numbers of people require access to venues that are open to the public.
- Storage security: It is crucial that the storage and retrieval of templates remain secure.. Although the traits captured during the enrollment process are analyzed and converted into mathematical measurements, privacy concerns still exits as these data systems are housing information on individual identities.[13]
- Human dignity and consent: Some critics believe that collecting biometric parameters is dehumanizing and reduces individuals to the sum of their parts - infringing on the body as a whole while ignoring their individuality.[14]

A Never Changing Approach to Security

It is also possible that data obtained during biometric enrollment may be used in ways the individual has not consented to. For example, most biometric features can disclose physiological and/or pathological medical conditions; fingerprints patterns are related to chromosomal disease; the iris could reveal genetic sex and; most behavioral biometrics can reveal neurological disease.

Privacy is, perhaps, the largest area of concern. There are three categories of privacy concerns:

- Unintentional functional scope: The authentication goes further than what is truly needed for authentication, and results in the identification of unintended health condition such as finding a tumor during a retinal scan or revealing a vascular disease based on vein patterns that are used in hand geometry scans.
- Unintentional application scope: The process correctly identifies a subject who in fact did not want to be identified. For example when a person's image is captured through a facial recognition process but who had never given explicit consent on the collection of his/her facial image.
- Covert identification: This is the use of the biometric data for purposes outside of the intended scope of identification and is used to exploit the person for personal or economic gain.[15] A person may want to remain anonymous and private but could be denied this privacy due to the use of biometric identification technology.

Conclusion

Biometric security technology is available in a wide range of options and techniques. When selecting the best biometric technology for a given application, there needs to be a balance in the technology that is selected and the appropriate privacy considerations.

By exploring the numerous options that are available, the ease of implementation and use and considering the barriers to acceptance, we can broaden our knowledge and hopefully be better positioned to choose wisely for our security needs.

Contact Us

To learn more about how OneBeacon Technology Insurance can help you manage online and other technology risks, please contact Dan Bauman, VP of Risk Control for OneBeacon Technology Insurance at dbauman@onebeacontech.com or 262-951-1455.

References

[1] Techopedia. Accessed June 2019. https://www.techopedia.com/definition/6203/biometric-security

[2] Liu, Simon and Silverman, Mark. (January/February 2001). "A Practical Guide to Biometric Security Technology." IEEE. Pages 27-32. Accessed June 2019. https://cedar.buffalo.edu/~govind/CSE717/papers/PracticalGuide.pdf

[3] (2009). "What is Biometrics?" Department of Computer Science and Engineering, Michigan State University. Accessed June 2019. http://biometrics.cse.msu.edu/info/index.html

[4] Ibid 2

[5] Wilson, Tracy V. "How Biometrics Work." How Stuff Works. Accessed June 2019. https://science.howstuffworks.com/biometrics.htm

[6] Ibid 3

[7] "What is Biometrics?" Accessed June 2019. http://www.bioelectronix.com/what_is_biometrics.html

[8] Accessed June 2019. https://en.wikipedia.org/wiki/Iris_recognition

[9] "Iris Recognition." Find Biometrics. Accessed June 2019. https://findbiometrics.com/solutions/iris-scanners-recognition/

[10] Mayhew, Stephen. "Explainer: Hand Geometry Recognition." Accessed June 2019. https://www.biometricupdate.com/201206/explainer-hand-geometry-recognition

[11] "Facial Recognition." Find Biometrics. Accessed June 2019. https://findbiometrics.com/solutions/facial-recognition/

[12] "Voice and Speech Recognition." Find Biometrics. Accessed June 2019. https://findbiometrics.com/solutions/voice-speech-recognition/

[13] Accessed June 2019. https://en.wikipedia.org/wiki/Biometrics

[14] Ibid 13

[15] Ibid 13