BIOMETRICS

FEBRUARY 2020 **ITSAP.00.019**

Biometrics refers to the measurement and use of your unique body characteristics (e.g. fingerprints, retinas, facial structure, speech, or vein patterns). For example, you can use your fingerprint as a form of authentication to unlock your mobile device. If using your biometrics for authentication, we recommend using them with a password or PIN for an added layer of protection (i.e. multi-factor authentication). Biometrics come with advantages and disadvantages, as well as security vulnerabilities that are outlined in this document.

Some examples of how biometrics are captured include:

- A fingerprint scanner measures electrical currents or emits ultrasounds that reflect the pattern of your fingerprint
- A facial recognition system takes a photo of your face and compares it to known images of yourself
- An iris recognition system takes an image of your eye, using infrared light, and compares it to documentation of your identifiable iris
- A vein pattern recognition system emits infrared light through a scanner to create an image of the veins inside your hand
- A speaker recognition system analyzes a combination of the acoustics in your voice with additional individual characteristics (e.g. accent, rhythm, vocabulary)

WHERE ARE BIOMETRICS USEFUL?

Biometrics are a convenient form of authentication. Rather than always having to input passphrases or passwords, you have your biometrics readily available.

Organizations can use biometrics in different ways, such as the following examples:

- Managing access to building facilities (e.g. server rooms)
- Unlocking IT assets and devices
- Making payments through a smartphone

HOW DO I ENROLL IN BIOMETRICS?

The first time you use biometrics on your device, you register your unique characteristic through an enrollment process. For example, with a fingerprint scanner, you need to scan your fingerprint multiple times so that the device can analyze and store an encoded hash of your individual biometric. The encoded hash represents your fingerprint in an encrypted code, which is very difficult for attackers to decrypt. The image of your fingerprint is never saved.

Before using a biometric system (e.g. mobile device), we recommend researching it to ensure its security procedures meet your organization's requirements.

AWARENESS SERIES

WHAT ARE SOME THREATS SPECIFIC TO BIOMETRICS?

Although your biometrics are unique to you, threat actors can mimic, copy, or impersonate your biometrics to fool systems, such as in the following examples:

- Copying your fingerprint (e.g. MasterKey synthetic fingerprint)
- Using a photo from your social media profile to trick a facial recognition system
- Capturing an image of your iris to trick an iris recognition system (e.g. contact lenses using printed image of your iris)
- Recording your voice or using voice morphing to trick a speaker recognition system (e.g. extracting your voice to overlay the attacker's voice)

Social media-specific threats are increasing. Your social media accounts give threat actors easy access to the photos and videos that you share publicly. Keep in mind that what you post can be used to mimic your biometrics.

WHAT ARE SOME ISSUES WITH BIOMETRIC SYSTEMS?

Biometric systems can malfunction and mistakenly deny (i.e. false negative) or allow (i.e. false positive) access to a system or device.

A **false negative** is when the biometric system does not recognize the authentic individual and blocks their access. A false negative could threaten your organization. For example, if a server infrastructure is down and authorized personnel are blocked from accessing the infrastructure, your organization loses access until the false negative is fixed or someone can successfully gain access.

A **false positive** is when a biometric system incorrectly matches an individual to someone else's credentials. If an unauthorized individual receives a false positive, your organization and the person whose credentials are being used are at risk. For example, if your smartphone grants access to someone else through incorrect facial recognition, your personal information could be compromised.

False negatives and positives can occur. We recommend using a password or pin, in combination with a biometric factor (i.e. multi-factor authentication), for an additional security layer.

HOW SECURE ARE NEWER STRUCTURES?

Recent technological advancements have improved the security measures that you can use to defend your biometrics against common cyber attacks. Some new features and technologies include the following examples:

- Facial recognition systems now rely on methods that use infrared dots to create a 3D map of a user's face (e.g. a photograph of you taken from your social media account is unlikely to match).
- Palm vein scanning is a considerably secure method of biometrics authentication. Veins are not as readily visible as your face or your fingerprints. It is more difficult for an attacker to steal your vein patterns.

WHAT PRIVACY CONCERNS ARE ASSOCIATED WITH BIOMETRICS?

Although biometrics can be a convenient authentication method, they are also a form of personal information. If your organization wants to use biometrics as a method of multi-factor authentication, you must ensure that this data is collected, handled, and used according to legal and regulatory requirements (e.g. *Privacy Act, Personal Information Protection and Electronic Documents Act*). As an example, you must get consent from employees to collect and use their biometrics.

WHAT CAN YOU DO TO STAY SAFE?

We recommend that you use biometrics with another authentication method (e.g. passphrases). MFA provides a stronger level of security. If one form of authentication is compromised, you still have a back up method that continues to protect your devices and accounts from being accessed.

Unlike other methods of authentication (e.g. passwords and smartcards), biometrics cannot be guessed or stolen. However, if mimicked or copied, a specific biometric (e.g. your right-hand index fingerprint) cannot be issued again as a password or pin would be. Another form of biometric (e.g. another finger's print) must be enrolled and used as a replacement to prevent threat actors from accessing systems and devices.

Need help or have questions? Want to stay up to date and find out more on all things cyber security?
Visit the Cyber Centre website at **cyber.gc.ca**