Communications Security Establishment
Centre de la sécurité des télécommunications

CLASSIFICATION

CANADIAN CENTRE FOR CYBER SECURITY

Biometrics

February 2024

ITSAP.00.019

Biometrics refers to the measurement and use of your unique body characteristics or behaviours, like fingerprints, retinas, facial structure, vein patterns, speech or gait for security or authentication. If using your biometrics for authentication, we recommend using them with additional authentication factors, such as a password or personal identification number (PIN) for an added layer of protection. This is known as multi-factor authentication (MFA). Biometrics come with advantages and disadvantages, as well as security vulnerabilities that are outlined in this document.

How are biometrics captured?

Biometrics can be captured in a number of ways. Some of the main examples include:

- Fingerprint scanners measure electrical currents or emit ultrasounds that reflect the pattern of your fingerprint
- Facial recognition systems take a photo of your face and compare it to known images of you
- Iris recognition systems take an image of your eye using infrared light and compare it to documentation of your iris
- Vein pattern recognition systems emit infrared light through a scanner to create an image of the veins inside your hand
- Speaker recognition systems analyze a combination of the acoustics in your voice with additional individual characteristics, like accent, rhythm, or vocabulary
- A gait recognition system uses cameras to monitor and analyze your movements (such as the stride and cadence of your walk) to verify your identity

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:

- managing access to building facilities, like 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. An 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 on your device, we recommend researching it to ensure its security procedures meet your organization's requirements.

AWARENESS SERIES

Cat. No. D97-1/00-019-2023E-PDF
ISBN 978-0-660-68191-7

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:

- copying your fingerprint with a master key 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 using contact lenses with a printed image of your iris
- recording your voice or using voice morphing to trick a speaker recognition system by laying your voice over 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 or allow access to a system or device. This is known as a false negative or a false positive.

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, for an additional security layer.

How secure are newer structures?

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

- Newer facial recognition systems now rely on methods that use infrared dots to create a 3D map of a user's face. A picture taken from your social media account is unlikely to match.
- Palm vein scanning is a considerably secure method of biometric authentication. Veins are not as readily visible as your face or your fingerprints, making it more difficult for an attacker to steal your vein patterns.
- Movement-based liveness checks are used on some newer devices to ensure it is a real person being scanned.

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 MFA, you must ensure that this data is collected, handled, and used according to legal and regulatory requirements, such as the *Privacy Act and the Personal Information Protection and Electronic Documents Act* (PIPEDA). You must also 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, like a password or PIN. 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, like passwords or smartcards, biometrics can't be guessed or stolen. However, if mimicked or copied, a specific biometric like your index fingerprint cannot be issued again as a password or pin would be. Another form of biometric, like another fingerprint or retina scan, must be enrolled and used as a replacement to prevent threat actors from accessing systems and devices.

Learn more

- Best practices for passphrases and passwords (ITSAP.30.032)
- Secure your accounts and devices with multi-factor authentication (ITSAP.30.030)