كلية هندسة الحاسوب و المعلوماتية

أمن نظم المعلومات

Biometrics

هاشم الصباغ – سامح عرابي

Biometrics are rising as an advanced layer to many personal and enterprise security systems. With the unique identifiers of your biology and behavior, this may seem foolproof.

However, biometric identity has made many cautious about its use as standalone authentication.

Modern cybersecurity is focused on reducing the risks for this powerful security solution: traditional passwords have long been a point of weakness for security systems. Biometrics aims to answer this issue by linking proof-of-identity to our bodies and behavior patterns.

Modern cybersecurity is focused on reducing the risks for this powerful security solution: traditional passwords have long been a point of weakness for security systems. Biometrics aims to answer this issue by linking proof-of-identity to our bodies and behavior patterns.

- What is the meaning of biometric?
- What is biometric data?
- What is a biometric scanner?
- What are the risks of biometric security?
- How can we make biometrics more secure?

What is Biometrics?

For a quick biometrics definition: Biometrics are biological measurements — or physical characteristics — that can be used to identify individuals. For example, fingerprint mapping, facial recognition, and retina scans are all forms of biometric technology, but these are just the most recognized options.

Researchers claim the shape of an ear, the way someone sits and walks, unique body odors, the veins in one's hands, and even facial contortions are other unique identifiers. These traits further define biometrics.

Three Types of Biometrics Security

While they can have other applications, biometrics have been often used in security, and you can mostly label biometrics into three groups:

1. Biological biometrics
2. Morphological biometrics
3. Behavioral biometrics

Biological biometrics use traits at a genetic and molecular level. These may include features like DNA or your blood, which might be assessed through a sample of your body's fluids.
Morphological biometrics involve the structure of your body. More physical traits like your eye , fingerprint , or the shape of your face can be mapped for use with security scanners.
Behavioural biometrics are based on patterns unique to each person. How you walk , speak, or even type on a keyboard can be an indication of your identity if these patterns are tracked.

Biometric Security Works

Biometric identification has a growing role in our everyday security. Physical characteristics are relatively fixed and individualized - even in the case of twins. Each person's unique biometric identity can be used to replace or at least augment password systems for computers, phones, and restricted access rooms and buildings.
-Once biometric data is obtained and mapped, it is then saved to be matched with future attempts at access. Most of the time, this data is encrypted and stored within the device or in a remote server.

Biometrics scanners are hardware used to capture the biometrics for verification of identity. These scans match against the saved database to approve or deny access to the system.
In other words, biometric security means your body becomes the "key" to unlock your access.

Biometrics are largely used because of two major benefits:
Convenience of use: Biometrics are always with you and cannot be lost or forgotten.
Difficult to steal or impersonate: Biometrics can't be stolen like password or key can.

While these systems are not perfect, they offer tons of promise for the future of cybersecurity.

Examples of Biometric security

Here are some common examples of biometrics security:

- Voice Recognition
- Fingerprint Scanning
- Facial Recognition
- Iris Recognition
- Heart – Rate Sensors

-In practice, Biometric security has already seen effective use across many industries.
Advanced biometrics are used to protect sensitive documents and valuables. Citibank already uses voice recognition, and the British bank Halifax is testing devices that monitor heartbeat to verify Customers identities. Ford is even considering putting biometric sensors in cars.

-Biometrics are incorporated in e-Passports throughout the world. In the United States, e-passports have a chip that contains a digital photograph of one's face, fingerprint, or iris, as well as technology that prevents the chip from being read — and the data skimmed — by unauthorized data readers.

Are Biometric Scanners Safe? - Improvements and Concerns

Biometrics scanners are becoming increasingly sophisticated. You can even find biometrics on phone security systems. For example , the facial recognition technology on Apple's iPhone X projects 30,000 infrared dots onto a user's face to authenticate the user by pattern matching .

The chance of mistaken identity with the iPhone X biometrics is one in a million, according to Apple.

The **LG V30** smartphone combines facial and voice recognition with fingerprint scanning and keeps the data on the phone for greater security. CrucialTec , a sensor manufacturer, links a heart – rate sensor to its fingerprint scanners for two – step authentication. This helps ensure that cloned fingerprints can't be used to access its systems.

The challenge is that biometric scanners, including facial recognition systems, can be tricked. Researchers at the University of North Carolina at chapel hill downloaded photos of 20 volunteers from social media and used them to construct 3-D models of their faces. The researchers successfully breached four of the five security systems the tested.

Examples of fingerprint cloning are everywhere. One example from the Black Hat cybersecurity conference demonstrated that a fingerprint can be cloned reliably in about 40 minutes with $10 worth of material, simply by making a fingerprint impression in molding plastic or candle wax.

Germany's Chaos Computer Club spoofed the iPhone's TouchID fingerprint reader within two days of its release. The group simply photographed a fingerprint on a glass surface and used it to unlock the iPhone 5s.

Biometrics – Identity & Privacy Concerns

Biometric authentication is convenient, but privacy advocates fear that biometric security erodes personal privacy. The concern is that personal data could be collected easily and without consent.

Facial recognition is a part of everyday life in Chinese cities, where it's used for routine purchases, and London is famously dotted with CCTV cameras. Now, New York, Chicago, and Moscow are linking CCTV cameras in their cities to facial recognition databases to help local police fight crime. Ramping up the technology, Carnegie Mellon University is developing a camera that can scan the irises of people in crowds from a distance of 10 meters.

In 2018, facial recognition was introduced in Dubai airport, where travelers are photographed by 80 cameras as they pass through a tunnel in a virtual aquarium.

Facial recognition cameras are also at work in other airports throughout the world, including those in Helsinki, Amsterdam, Minneapolis-St. Paul, and Tampa. All that data must be stored somewhere, fueling fears of constant surveillance and misuse of data.

Biometrics Data Security Concerns

A more immediate problem is that databases of personal information are targets for hackers. For example, when the **U.S. Office of Personnel Management was hacked in 2015**, cybercriminals made off with the fingerprints of 5.6 million government employees, leaving them vulnerable to identity theft.

Storing biometric data on a device – like the iPhone's TouchID or Face ID – is considered safer than storing it with a service provider, even when the data is encrypted.

That risk is similar to that of a password database, in which hackers may breach the system and steal data that's not effectively secured. The ramifications, however, are significantly different. If a password is compromised, it can be changed. Biometric data, in contract, remains the same forever.

Ways to Protect Biometric Identity

With the risks to privacy and safety, additional protections must be used in biometric systems.

Unauthorized access becomes more difficult when systems require multiple means of authentication, such as life detection (like blinking) and matching encoded samples to users within encrypted domains.

Some security systems also include additional features, such as age, gender, and height, in biometric data to thwart hackers.
India's Unique ID Authority of India Aadhaar program is a good example. Initiated in 2009, the multi-step authentication program incorporates iris scans, fingerprints from all 10 fingers, and facial recognition.
This information is linked to a unique identification card that is issued to each of India's 1.2 billion residents. Soon, this card will be mandatory for anyone accessing social services in India.
Biometrics make a good replacement for usernames as part of a two-factor authentication strategy. That incorporates:

- Something you are (Biometrics)
- Something you have (like a hardware token) or something you know (like a password)

Two-factor authentication makes a powerful combination, especially as IoT devices proliferate. By layering the protection, secured internet devices become less vulnerable to data breaches.
In addition, using a password manager to store any traditional passwords can give you an additional safeguard.

Takeaways on Biometrics

In summary, biometrics remains a growing way to verify identity for cybersecurity systems.

The combined protection of your physical or behavioral signatures with other authentications gives some of the strongest known security. At the moment, it is at a minimum better than using a character-based password as a standalone verification