Biometrics

Definition

Biometric authentication uses physical or behavioral human characteristics to digitally identify a person to grant access to systems, devices or data. Examples of these biometric identifiers are fingerprints, facial patterns, voice or typing. Each of these identifiers is considered unique to the individual, and they may be used in combination to ensure greater accuracy of identification.

Because biometrics can provide a reasonable level of confidence in authenticating a person with less friction for the user, it has the potential to dramatically improve enterprise security. Computers and devices can unlock automatically when they detect the fingerprints of an approved user. Server room doors can swing open when they recognize the faces of trusted system administrators. Help desk systems might automatically pull up all relevant information when they recognize an employee's voice.

Types of biometrics

A biometric identifier is one that is related to intrinsic human characteristics. They fall roughly into two categories: physical identifiers and behavioral identifiers.

Fingerprints: Fingerprint scanners have become ubiquitous in recent years due to their widespread deployment on smartphones. Any device that can be touched, such as a phone screen, computer mouse or touchpad, or a door panel, has the potential to become an easy and convenient fingerprint scanner.

Photo and video: If a device is equipped with a camera, it can easily be used for authentication. Facial recognition and retinal scans are two common approaches.

Voice: Voice-based digital assistants and telephone-based service portals are already using voice recognition to identify users and authenticate customers.

Signature: Digital signature scanners are already in widespread use at retail checkouts and in banks and are a good choice for situations where users and customers are already expecting to have to sign their names.

DNA: Today, DNA scans are used primarily in law enforcement to identify suspects -- and in the movies. In practice, DNA sequencing has been too slow for widespread use. This is starting to change.

Behavioral identifiers are a newer approach and are typically being used in conjunction with another method because of lower reliability. However, as technology improves, these behavioral identifiers may increase in prominence. Unlike physical identifiers, which are limited to a certain fixed set of human characteristics, the only limits to behavioral identifiers is the human imagination.

Today, this approach is often used to distinguish between a human and a robot. That can help a company filter out spam or detect attempts to brute-force a login and password. As technology improves, the systems are likely to get better at accurately identifying individuals, but less effective at distinguishing between humans and robots. Here are some common approaches:

Typing patterns: Everybody has a different typing style. The speed at which they type, the length of time it takes to go from one letter to another, the degree of impact on the keyboard.

Physical movements: The way that someone walks is unique to an individual and can be used to authenticate employees in a building, or as a secondary layer of authentication for particularly sensitive locations.

Navigation patterns: Mouse movements and finger movements on trackpads or touch-sensitive screens are unique to individuals and relatively easy to detect with software, no additional hardware required.

Engagement patterns: We all interact with technology in different ways. How we open and use apps, how low we allow our battery to get, the locations and times of day we're most likely to use our devices, the way we navigate websites, how we tilt our phones when we hold them, or even how often we check our social media accounts are all potentially unique behavioral characteristics. These behavior patterns can be used to distinguish people from bots, until the bots get better at imitating humans.

How reliable is biometric authentication?

- Authentication credentials such as fingerprint scans or voice recordings can leak from devices, from company servers or from the software used to analyze them.
- A facial recognition system might not recognize a user wearing makeup or glasses, or one who is sick or tired.
- Voices also vary.
- People sound different when they first wake up, or when they try to use their phone in a crowded public setting, or when they're angry or impatient.
- Recognition systems can be fooled with masks, photos and voice recordings, with copies of fingerprints, or tricked by trusted family members or housemates when the legitimate user is asleep.

What are the privacy risks of biometric authentication?

- Some users might not want companies collecting data about, say, the time of day and the locations where they typically use their phones. If this information gets out, it could potentially be used by stalkers.
- Some users might not want their family members or spouses to know where they are all the time.

- The information could also be abused by repressive government regimes or criminal prosecutors overstepping boundaries.
- Foreign powers might use the information in an attempt to influence public opinion.
- Unethical marketers and advertisers might do likewise.
- Any of these situations could potentially lead to significant public embarrassment for the company that collected the data.
- If DNA scans become widespread, they give rise to a whole new area of privacy concerns such including exposure of medical conditions and family relationships.