What is biometrics? And why collecting biometric data is risky

Biometrics has the potential to make authentication dramatically faster, easier and more secure than traditional passwords, but companies need to be careful about the biometric data they collect.

By Maria Korolov

Contributing Writer, CSO

FEB 12, 2019 3:00 AM PT

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 cadence. 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 on the support line.

According to a recent Ping Identity survey, 92 percent of enterprises rank biometric authentication as an "effective" or "very effective" to secure identity data stored on premises, and 86 percent say it is effective for protecting data stored in a public cloud. Another survey, released last year by Spiceworks, reports that 62 percent of companies are already using biometric authentication, and another 24 percent plan to deploy it within the next two years.

However, companies need to be careful about how they roll out their biometric authentication systems to avoid infringing on employee or customer privacy or improperly exposing sensitive information. After all, while it's easy to issue a new password when the old one has been compromised, you can't issue someone a new eyeball.

According to the Spiceworks survey, 48 percent cite the risks of stolen biometric data as a top security risk with the technology. Other barriers to adoption include costs, cited by 67 percent of respondents, followed by reliability concerns at 59 percent.

For companies specifically using biometrics to secure IT infrastructure in cloud, SaaS, on-prem and hybrid environments, adoption rates are even lower, according to the Ping Identity survey. Only 28 percent of companies use biometrics on premises, and even fewer, 22 percent, use it for cloud applications.

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. Physical identifiers are, for the most part, immutable and device independent:

- **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. According to Spiceworks, fingerprint scanning is the most common type of biometric authentication in the enterprise, used by 57 percent of companies.

- **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.

- **Physiological recognition:** Facial recognition is the second most common type of authentication, according to Spiceworks, in place at 14 percent of companies. Other image-based authentication methods include hand geometry recognition, used by 5 percent of companies, iris or retinal scanning, palm vein recognition, and ear recognition.

- **Voice:** Voice-based digital assistants and telephone-based service portals are already using voice recognition to identify users and authenticate customers. According to Spiceworks, 2 percent of companies use voice recognition for authentication within the enterprise.

- **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. Last year, a $1,000 scanner hit the market that can do a DNA match in minutes -- and prices are likely to keep dropping.

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. And they can also be used in combination with other authentication methods, or, if the technology improves enough, as standalone security measures.

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. There is also a high potential for false positives and false negatives. 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.

Experts recommend that companies use multiple types of authentication simultaneously and escalate quickly if they see warning signs. For example, if the fingerprint is a match but the face isn't, or the account is being accessed from an unusual location at an unusual time, it might be time to switch to a backup authentication method or a second communication channel. This is particularly critical for financial transactions or password changes.

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 or, in the case of celebrities, by tabloid journalists. 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. Last year, a fitness app was discovered to be collecting information about user locations and exposing it in a way that revealed the location of secret U.S. military bases and patrol routes.

Any of these situations could potentially lead to significant public embarrassment for the company that collected the data, regulatory fines, or class-action lawsuits. 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.

How secure is biometric authentication data?

The security of the biometric authentication data is vitally important, even more than the security of passwords, since passwords can be easily changed if they are exposed. A fingerprint or retinal scan, however, is immutable. The release of this or other biometric information could put users at permanent risk and create significant legal exposure for the company that loses the data.

"In the event of a breach, it creates a Herculean challenge because physical attributions such as fingerprints cannot be replaced," says data security expert Kon Leong, CEO and co-founder at San Jose-based ZL Technologies. "Biometric data in the hands of a corrupt entity, perhaps a government, carries very frightening but real implications as well. "

At the end of the day, every company is responsible for its own security decisions. You can't outsource compliance, but you can reduce the cost of compliance, and the possible repercussions of a leak, by picking the right vendor. If a small or mid-sized company uses, say, Google’s or Apple's authentication technology and there's a security breach with Google or Apple, it's likely Google or Apple will get the blame.

In addition, companies that don’t keep credentials on file have some legal protections. For example, many retailers can avoid substantial compliance costs by keeping their systems "out of scope.” Payment information is encrypted right at the payment terminal and goes straight through to a payment processor. Raw payment card data never touches the company servers, reducing both compliance implications and potential security risks.

If a company needs to collect authentication information and keep it on its own servers, best-practice security measures should be applied. That includes encryption both for data at rest and data in transit. New technologies are available for runtime encryption, which keeps the data in encrypted form even while it is being used.

Encryption is not an absolute guarantee of security, of course, if the applications or users that are authorized to access the data are themselves compromised. However, there are a couple of ways that companies can avoid keeping even encrypted authentication data on their servers.

Local or device-based authentication

The most common example of a local authentication mechanism is the hardware security module in a smartphone. User information — such as a fingerprint scan, facial image or a voice print — is stored inside the module. When authentication is required, biometric information is collected by the fingerprint reader, camera or microphone and sent to the module where it's compared to the original. The module tells the phone whether or not the new information is a match to what it already had stored.

With this system, the raw biometric information is never accessible to any software or system outside the module, including the phone's own operating system. On the iPhone, this is called the secure enclave and is available on every phone with an Apple A7 chip or newer. The first phone with this technology was the iPhone 5S, released in 2013. Similar technology is also available on Android phones. Samsung, for example, started rolling out the ARM TrustZone trusted execution environment with the Samsung S3 smartphone.

Today, smartphone hardware security modules are used to provide security for Apple Pay, Google Pay and Samsung Pay as well as to authenticate third-party applications. PayPal, for example, can use a phone's biometric sensor for authentication without PayPal ever seeing the actual biometric data itself. Square Cash, Venmo, Dropbox and many banking apps and password management apps leverage this authentication mechanism as well.

Enterprises can also use smartphone-based biometric readers whenever their users or customers have access to smartphones, without ever having to collect and store any identifying biometric information on their own servers. Similar technology is available for other types of devices, such as smart cards, smart door locks, or fingerprint scanners for PCs.

According to Spiceworks, phone-based fingerprint recognition is the most common biometric authentication mechanism in use today. Thirty-four percent of companies use Apple's Touch ID fingerprint sensor. In addition, 14 percent of companies use Apple Face ID and 7 percent use Android Face Unlock.

Smartphone-based authentication offers significant usability benefits. First, users tend to be immediately aware if they have misplaced or lost their smartphone and will take immediate steps to find or replace it. If, however, they misplace a badge that they only use to access a building during the off-hours, they might not notice for a while that it is missing.

Smartphone manufacturers are also in the middle of an arms race to make their technology better and easier to use. No other industry — or individual company — can match the scale of mobile investment or the usability and security testing that phones receive.

Finally, phone authentication offers users maximum flexibility. They can opt for phones with face ID, fingerprint scanners or voice recognition, or some other new technology that hasn't been invented yet but will dominate the market tomorrow. However, using a third-party mechanism like consumer smartphones puts the authentication process outside enterprise control.

Another downside to device-based authentication, in general, is that the identity information is limited to that one device. If people use a fingerprint to unlock their smartphone, they can't then also use that same fingerprint to unlock their office door without separately authorizing the door lock, or to unlock their computer without separately authorizing their PC's fingerprint scanner.

Companies that need to authenticate users or customers on multiple devices in multiple locations need to either have some kind of centralized mechanism to store the authentication credentials or leverage a device that the user carries with them at all times. For example, companies can put the authentication mechanism inside a smart badge that employees wear around the office. They can also use a smartphone to authenticate the employee, then communicate the identity confirmation to other devices and systems via Bluetooth, NFC, WiFi or the internet.

Tokenization or encryption

Another approach to allowing new devices to recognize existing authorized users is tokenization, one-way encryption, or hashing functions. Say, for example, retinal, voice or fingerprint identification is used to recognize and authenticate employees wherever they might go within a company, but the company doesn't want to have the image or audio files stored on servers where hackers or malicious employees might misuse them.

Instead, the company would use a device that, say, scans a person's face or fingerprint, converts that image into a unique code, then sends that code to the central server for authentication. Any device that uses the same conversion method would then be able to recognize the employee, and the raw identification data is never available on any system. The downside to this approach is that the company is then locked into a single proprietary authentication mechanism.