Security Concern

Biometrics security isn't one-size-fits-all

Andrew Jamieson

We "give away" our biometric data all the time, in photos, as DNA, to other systems. It's basically public data.

Anyone could be taking a picture of your ear or eye right now, or looking it up on social media, so biometric markers can be vulnerable to exposure if not managed properly.

Biometrics have rapidly expanded into consumer applications like the financial market for customer authentication to payment services and withdrawing cash from ATMs in high-fraud markets. More so, by 2020 nearly all smart devices including mobile phones, tablets and wearables will have some form of biometric security enablement.

While the above seems to justify the adoption of biometrics in the banking industry, it is essential to understand the impediments to broader adoption. Many technologies that would be enabled by biometrics are still vulnerable to spoofs and hacking.

For example, mobile apps continue to pose serious security risks due to vulnerabilities that may exist within their software. Such vulnerabilities may be exploited to steal information, control a user's device, exploit hardware resources, or result in unexpected app or device behavior.

It's not all about the device

A lot of the media, and some academic, attention is paid to the "falsification of the biometric trait", such as replicating a fingerprint, using a mask to fool a facial recognition system, or a video to confuse an iris pattern matching process. However, after the capture, this trait is transformed into a digitized data, and so we must also be concerned with how this digitized data is protected?

If one can make a 'copy' of this digital data, it may be possible to pose as the person from which it was originally provided. Although there is a strong history and culture of physical and logical security for PINs and card data, it is not the same for biometric data.

It is because biometric data can often be easily cloned, for use in 'presentation attacks' (e.g.; cloning the data input), that biometric data should be used in conjunction with a second factor for higher security. Additionally, biometric systems targeting higher security should include mechanisms to prevent presentation attacks such as "liveness detection". This liveness detection is critical for preserving trust in the integrity of biometrics authentication, increasing consumer acceptance and industry adoption.

The benefit of robust biometrics in the authentication process is from the ability to mitigate the potential for attacks being truly scalable. Fraudsters want to find a way of committing fraud, and to repeat it again and again. By introducing additional layers of authentication, such as a hybrid approach that combines technology and human verification, it's far more difficult for that to happen.

Layer by layer

Instead of relying on a one-size-fits-all solution, any widely deployed security mechanism needs to consider a layered based approach to identification, which harnesses the power of both physiological and behavioral biometrics, to create a secure and user-friendly online experience, whilst also addressing users concerns and potential security flaws.

Technological advances now mean the behavior of the user also can be used as a means of identification by learning and processing a multitude of different data points - from the way a user swipes their phone to their individual key strokes. These behavioral biometrics create a way to develop a usable risk profile and act as part of a more trustworthy identification process, with the ability to detect anomalies, where bot and replay attacks can be easily spotted. Using this much more amenable approach to biometrics also means that users can opt out of sharing highly personal information and data, insulating both the user and the enterprise against the risks posed by data breaches.

However, such new technologies are also fraught with concerns around the ability to perform 'hidden' tracking of users - as we learn more about ways to identify us as individuals, it becomes harder and harder for us to remain anonymous in all aspects of our digital lives.

Biometrics can undoubtedly be an easy and convenient way to identify a customer and, when used properly, can be secure as well. One must realize, however, that biometrics is not a remedy for all problems.

Biometrics can undoubtedly be an easy and convenient way to identify a customer and, when used properly, can be secure as well. One must realize, however, that biometrics is not a remedy for all problems.

Understanding how any specific biometric authentication process works, when to use it and when not to use it, is essential. In an increasingly digital world, businesses need to square the circle of strong security and identification processes, whilst not inhibiting the user journey. By combining the unique identification markers offered by biometrics, we can create a secure, robust, layered identification process, by utilizing the most unique data points and markers possible - the users themselves.

(Andrew Jamieson is director of security & technology for the identity management & security unit, UL)