The art of authentication – What route do you choose?

Biometrics: physical attributes vs. behavioural patterns – the privacy debate

By Robert Capps

Vice President of Business Development at NuData Security

Account takeovers are increasingly affecting a growing population of online user accounts due to a confluence of threats, such as weak consumer password practices, frequent mass data breaches and brute force attacks against web properties.

The scope, scale and frequency of these online attacks against user accounts has demonstrated time and again that companies can no longer rely upon authentication methods based on static elements that can and will be stolen, traded and sold to the highest bidder in underground markets.

These trends have recently led organisations to consider the use of human biometric characteristics to supplement standard, but weak, single factor authentication schemes that have historically relied on a shared secret, such as a password, to validate that the rightful owner of an online account is the one who is accessing it. As these organisations investigate advanced authentication methods, they face an environment where the term "biometrics" has become an industry buzzword that encompasses a number of human second-factor solutions from "selfie"-based facial recognition, to fingerprint and iris scans, behavioural patterns, voice – even the human heartbeat.

As such technology is increasingly proposed and used in online and offline transactions; the use of biometric factors is rapidly becoming an area of concern from a data privacy and security perspective.

When most people who do not live and breathe online security hear the word "biometrics", they immediately think of Tom Cruise in Mission Impossible, using physical attributes such fingerprints, handprints, retinal scans, voice print and facial recognition to secure access to some highly protected asset or location. For some reason, they don't generally link the use of these elements to facilitate a secure login to an e-commerce, banking or social media website.

While the use of these physical biometric factors has been a boon for physical security, where the person to be authenticated is physically presenting themselves for enrolment and subsequent authentication, many factors quickly lose effectiveness in an online world, where the user is physically enrolling and authenticating themselves through a consumer grade device that they own and control.

There are several factors companies must consider before relying on physical biometric technology to authenticate users in an online environment. The first consideration is that using only one physical biometric data point to authenticate a user at the time of login is essentially the same as adding a static second password – albeit one that can never be changed if compromised.

Perhaps the most significant issue with relying on physical biometrics for online authentication is that they can be captured, and in some cases, reused.

Let's take a fingerprint as an example – use of such a physical biometric attribute is akin to when an employee was caught writing a password on a Post-It note, but instead of it being pasted on their computer screen, they simply leave a copy behind everywhere they go. Humans leave behind biometric traces with every glass they pick up, every piece of gum they discard and every camera that records their image.

Unlike passwords or credit card numbers, a person's physical biometric attributes can never be changed, resulting in privacy and identity concerns if a high-quality reproduction of a biometric element were to be obtained by a malicious actor. In September 2015, 5.6 million fingerprints were stolen from the Office of Personnel Management (OPM). From a security perspective, there are several possible use cases where compromised biometric data, like that of the OPM, can be used to access accounts without the user being present. Using the infamous gummy bear attack against a newly released product with embedded fingerprint scanning, for example, was a variation on a well-known physical hack for

in-person fingerprint scanners dating back to 2002.

Alarmingly, as authentication of high value transactions is increasingly moving to multi-factor authentication using some form of physical biometric, there is a real potential for criminals to shift their focus to obtain the biometric identifier, with violence. For this reason alone, many companies are steering well clear of utilising physical.

With this in mind, not all biometric factors have the same risk of impersonation or lack of effectiveness when used to authenticate online interactions.

A much less invasive, and more consumer friendly technique, leverages signals generated by the way in which a human interacts with the world around them. When taken in aggregate, such behavioural signals are highly effective at identifying repeat good users, are self-enrolling, and are tolerant of changes in the patterns presented as a user's behaviour naturally changes over their lifetime.

For an example of how behavioural data is useful in identifying a legitimate account holder, think about how you use your smart phone to interact with a website or application. Do you realise that you have a unique way of holding your mobile device that's different from other people, if only slightly? Does your phone tilt a little to the left? Do you normally hold your phone in portrait or landscape mode? Do you use your index fingers or thumbs to type? How hard do you press on the screen when you hit each key?

This method, dubbed "behavioural biometrics", aggregates hundreds of these human and interaction signals, creating a unique signature for each authentic user.

Using these subtle signals and unique signatures, organisations can easily identify when the account owner is not the one attempting to authenticate, even if the correct login and password is used in conjunction with the authentic account holder's computer or mobile device.

Unlike physical biometrics, behavioural signals that make up a behavioural biometric profile cannot be stolen, duplicated, or reused - so they have no value to criminals. In the event that a high fidelity copy of an authentic user interaction was made, the mere attempt to replay the past interaction would, in itself, be an anomaly that is out of pattern for any human user.

Collecting behavioural biometric data is non-invasive to the consumer, as they do not have to enter, enrol in, or provide any additional information to a website or application. They simply keep doing what they are used to doing, interacting with the sites and services as they always have. As human and interaction signals are collected, instead of physical biometric characteristics, it is far more privacy-friendly than some physical biometrics.

As organisations consider layering additional authentication technology and methods to secure their users' accounts, they must select methods that reduce friction for their good users, reduce risk to the organisation or the consumer, and are sensitive to the privacy concerns of their users–all the while making the reuse of compromised authentication and identity information nearly impossible.

With appropriate protections in place, online businesses can continue as usual, and with great confidence–even in the face of frequent data breaches and poor consumer security habits.

NuData Security predicts fraudulent transactions by identifying good users from bad, based on their online behaviour. By tracking over 18 billion behaviours anually, NuData harnesses the power of behavioural and statistical analysis, enabling its clients to predict fraud with 99% accuracy.

For more information, please visit
www.nudatasecurity.com

NU DataSecurity