Invisible challenges: the next step in behavioural biometrics?

Avi Turgeman

Frances Zelazny

Avi Turgeman and Frances Zelazny, BioCatch

Since 2013, when Apple first introduced its Touch ID fingerprint technology on to smartphones, there has been a boom in the acceptance and adoption of biometric systems in a wide variety of applications. Biometrics had already become a staple within national and voter ID schemes, passports, visas, border control systems, frequent traveller programmes, law enforcement and other government systems. But only the convergence of biometrics on consumer mobile devices has enabled biometrics to enter mainstream commercial applications.

The financial sector has been the quickest to take advantage of this, streamlining the logon for consumers in online banking and web applications by offering Touch ID as a replacement for passwords and PINs. According to a 2015 Raddon Financial Group survey, 17% of iPhone 6 users reported using Touch ID to log on to a mobile device and a further 42% planned to do so in the future. Among all smartphone users, 42% of those using mobile banking preferred fingerprint identification[1].

The obvious driver for this is the need for faster and more convenient authentication across mobile banking and payments. And as more and more consumers move to digital platforms, the importance of physical biometrics as logon mechanisms will become even more pronounced. Yet at the same time, it is becoming well understood that the login process does not ensure ultimate security. In fact, according to the Federal Reserve's Consumers and Mobile Financial Services 2016 annual report, around 70% of users who did not use mobile banking or mobile payment services cited security as their main reason for holding back[2].

With all the continuing high profile hacks, the methods used by cybercriminals and fraudsters have become more simple and reliant on stolen credentials, yet on the other hand much more sophisticated. The fact is, via social engineering, malware and Remote Access Trojans (RATs), today's cybercriminals can and do bypass the login process completely, regardless of how secure and accurate it is.

Enter behavioural biometrics

Given all the fraud now coming from authenticated sessions, the key reason why behavioural biometrics are gaining particular prominence in banking is because they provide a form of continuous authentication without compromising the user experience. In its recent 'Ten Top Trends for Biometrics and Digital Identity' report, Acuity Market Intelligence predicted that behavioural biometrics would become mainstream in 2017[3]. Similarly, the Mercator Advisory Group reported in January: "Behavioural dynamics will play an increasingly important role in establishing trust factors for authenticating consumers' identity across every channel and for establishing persistent identity."[4] But with all the attention on this latest biometric modality come new questions about its accuracy, viability, scalability and adaptability to emerging threats. After all, dealing with fraud and security is often a cat-and-mouse game. The challenge is we don't know what the next threat will look like and where it will come from.

"Behavioural biometrics are gaining particular prominence in banking is because they provide a form of continuous authentication without compromising the user experience"

Behavioural biometrics analyse human-device interactions, which essentially fall into three main categories: cognitive factors such as eye-hand coordination, applicative behaviour patterns, usage preferences and device interaction patterns; physiological factors such as left/right handedness, press-size, hand tremors, arm size and muscle usage; and contextual factors such as transaction, navigation, device and network patterns.

The early class of behavioural biometrics looked at keyboard strokes, mouse movements and gesture analysis. But unlike physical biometrics, which are usually captured under static and controlled conditions (ie, place a finger on a scanner), with behavioural analysis in the real world there are much more dynamic aspects at play. Risks such as replay attacks, human interaction simulation and advanced malware injections must be taken into account.

But at the time of writing, there are not many practical ways to deal with these challenges. This can dampen enthusiasm for adopting behavioural biometrics, especially since reducing fraud cannot come at the cost of adding friction to the user experience. The ROI in this case is measured not simply in the ability to reduce overall fraud in real time, and the number of false accepts and false rejects. It also relates to the costs associated with escalations to cost centres because of failed authentications and false alarms.

New approach

To deal with these challenges, it's not enough to simply emulate a robotic attack, and therefore know the difference between robotic and human behaviour. What's needed are ways to improve the accuracy of behavioural biometrics, based on a clear understanding of how fraudsters behave online. One answer is 'invisible challenges', a new generation of fraud prevention tools. These aim to address the weakness of traditional approaches, which rely on malware libraries, two-factor authentication, device ID and other means that the sophisticated fraudsters of today have figured out how to circumvent.

Invisible challenges are a technique developed by former Israeli intelligence operatives that introduce tests into an online session that users subconsciously respond to without sensing any change in their experience. The response contains behavioural data that can be used to distinguish a real user from an imposter, human or non-human (robotic activity, malware, aggregator, etc).

It is important that each challenge and its corresponding deviation is tested to determine the threshold at which users notice a change in experience on the mobile or website. The following are examples of invisible challenges:

1. *Rotation of movement challenge:* Introducing a deviation in the mouse movement. Figure 1 shows a user reacting to the invisible challenge by making a small correction to a right-side deviation that would have made them miss their target without compensating. When given this challenge repeatedly, this user typically makes one small correction at 60-80 degrees (red hook) during the last 10% of the movement. But other people respond differently to the same challenge. In the screenshot to the right, a second user responds with multiple corrections (blue lines). They begin their correction during the last 20% of the movement. A robot would not compensate at all.

2. *Spinning wheel challenge*: Introducing a fluctuation in the way the selection wheel spins. A common user interaction element in mobile apps is the spinning selection wheel for dates, time, numbers, etc. This is often used when entering information such as a new destination account for money transactions. In this challenge, passive measures related to spinning the wheel are collected (speed, stopping strategy, corrections towards the end). Subtle fluctuations to the spinner are also introduced that can elicits different subconscious reactions. As shown in Figure 2, the challenge makes the wheel spin slowly (not kinetically). The first user compensates with a few long and continuous 'pushes' to spin the wheel, and adds two powerful strokes in the other direction for fine-tuning and final targeting. The second user on the other hand compensates by making many small and short 'pushes' to spin the wheel. Afterwards, this user adds several short, concentrated and powerful strokes in the same direction for final targeting.

3. *Disappearing mouse challenge:* Hiding the cursor. Users search for the cursor/mouse in very different and unique ways. Some use wide search patterns, others use small ones, some are horizontal while others are diagonal, and certain users always search counter-clockwise. Sometimes users move on a certain learning curve and their responses vary according to their location on the curve. All these can be captured as unique parameters. But typically this is not practical, because the time required for the user to provide enough relevant mouse movements to accurately authenticate themselves is too long. An invisible challenge unconsciously 'forces' the user to make various mouse movements in a very short time, allowing enough data to be captured from the user in only several hundred milliseconds. This makes it useful for detecting anomalies in user behaviour in near real time. Figure 3 shows 25 users, each with a slightly different search pattern for a missing cursor.

PIC 1

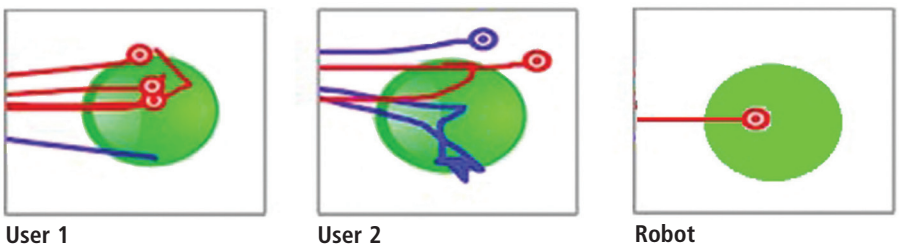

Figure 1: Rotation of movement challenge.

PIC 2

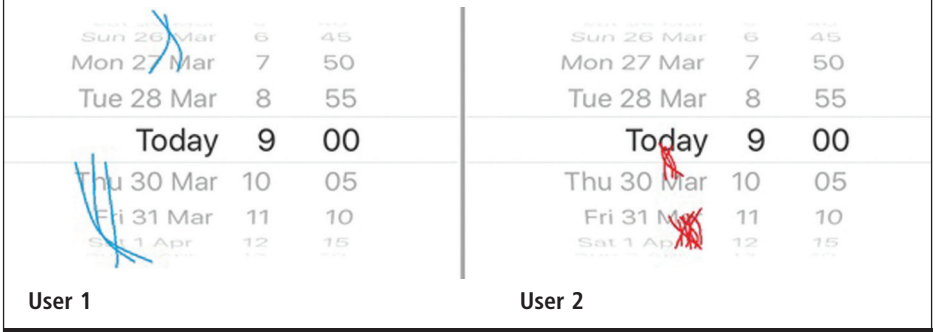

Figure 2: Spinning wheel challenge.

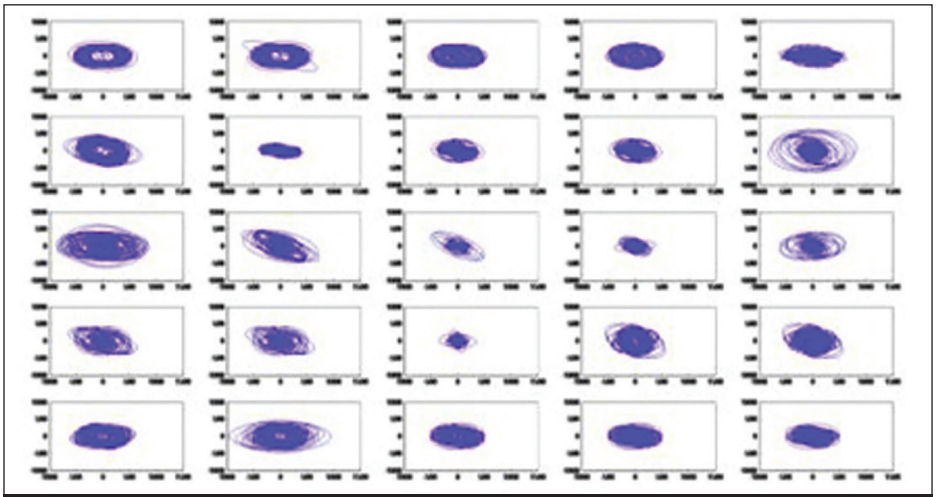

Figure 3: Disappearing mouse challenge.

Behavioural benefits

In the world of online transactions, it is vital to keep false positives and user friction to a minimum, while ensuring very accurate fraud alerts. In this respect, as a class of technologies behavioural biometrics offer advantages over other authentication modalities. They are passive, seamless, work in the background and do not require active enrolment. On the other hand, all these characteristics make it hard to achieve high levels of accuracy. Invisible challenges are designed to provide greater accuracy and other advantages over more traditional behavioural and fraud prevention approaches, as follows:

• Accuracy. Invisible challenges generate more data that cannot be captured in other ways. This data is intimate in the sense that it divulges cognitive and physiological parameters. In the world of machine learning and deep learning, the amount and quality of data is