Behavioral biometrics: The new 'certificate' in the AI ??era.

Behavioral biometrics is changing how security authentication works in the age of AI.

We are entering a major turning point in how online identity verification works. Previously, systems typically asked **you what you knew** —like a password, PIN, or security question. Then, technology advanced to asking **who you are** through Face ID or fingerprint recognition.

Now, the question is gradually shifting to: **How do you behave?**

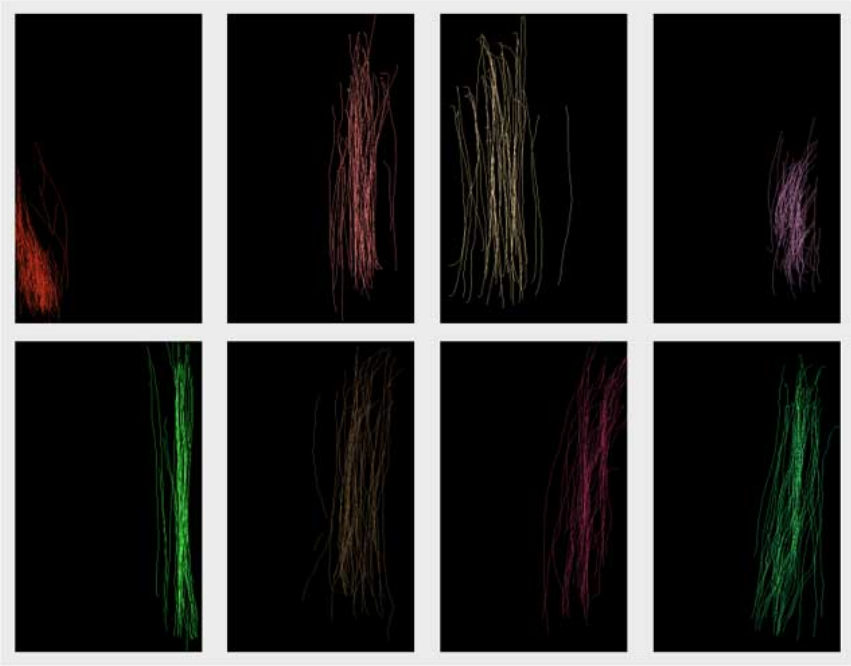
The development of generative AI and new attack technologies such as RATs (Remote Access Trojans) has helped cybercriminals scale their attacks and even bypass security methods once considered secure, such as Face ID or multi-factor authentication (MFA).

Therefore, **behavioral biometrics** is becoming the new layer of security. Many banks have begun implementing this technology to detect fraud based on how users interact with their devices.

How does behavioral biometrics work?

Every time you scroll, drag a slider, or tap your phone, your brain is making a series of tiny adjustments in real time. These adjustments happen in milliseconds and are almost unconscious.

Initially, behavioral biometrics was developed to distinguish humans from bots. But later, researchers realized that this technology could also differentiate **between individual users** .



Computational Motor Control Theory, a field that combines neuroscience, biomechanics, and computer science, has helped researchers better understand human behavior.

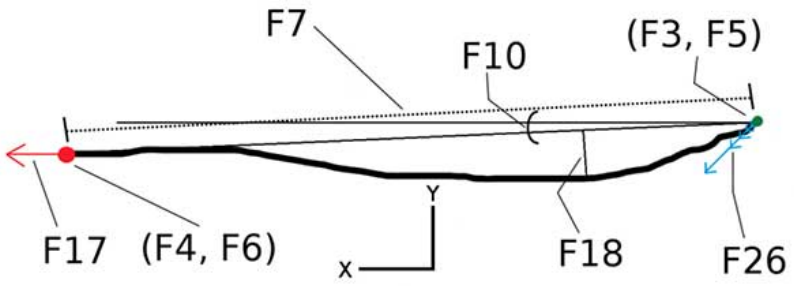
A 2012 study at the University of California, Berkeley—called Touchalytics—analyzed how 41 users scrolled their phone screens. The results showed that the system could accurately identify the user without error with just **11 scrolls .**

Digital behavior footprint

Berkeley's research identified more than 30 different behavioral traits, including actuation length, speed, direction of movement, curvature, time between acts, and even finger area when touching the screen.

For example, some people stop completely at the end of a scrolling motion. Others lift their hand while their finger is still moving. These subtle differences form each person's unique 'behavioral signature'.

Beyond just scrolling, factors such as keyboard typing rhythm, app navigation style, or phone holding technique can also help differentiate users.



The race for AI and security.

Certain individual behavioral cues can help detect fraud. For example, if the phone is flipped upside down during a transaction, that could be suspicious. Typing too quickly or mouse movements that are too straight can also trigger alerts.

However, modern behavioral biometric systems are not based on simple rules. Instead, AI combines multiple behavioral signals to build a unique model for each user.

These models can continuously authenticate users, even after successful login. This helps detect unusual behavior throughout the session.

Older adults are currently a vulnerable group to account hijacking attacks. An attack typically involves multiple steps, starting with phishing or social media manipulation.

Login information is then sold on black markets like Genesis Market. This data can be exchanged multiple times before being used to hack accounts.

Traditional security measures like OTP, MFA, or device verification are still effective, but new forms of attack are making these methods less effective.

Today, malware can:

1. Record keyboard input.
2. Stealing OTP codes
3. Remote device control
4. Block authentication messages

Deepfake tools are also being used to bypass facial authentication. One example is the ProKYC tool, which can fool even in-person verification systems.

Additionally, malware like BingoMod can impersonate legitimate applications to steal data and conduct financial transactions.

When a device is compromised, traditional security measures become almost ineffective. In this case, **user behavior becomes the only reliable authentication factor** .

Behavior is the future of authentication.

One positive aspect of behavioral biometrics is the improved user experience. When the system can authenticate continuously, users don't need to enter OTPs or verify multiple times.

If the user's behavior matches the saved profile, the session will continue normally. Otherwise, if an anomaly is detected, the system will request additional verification or block the transaction.

This shifts the authentication process from manual to passive. Users don't need to perform any additional actions, as the natural behavior itself becomes the authentication 'certificate'.

Behavioral biometrics is opening a new avenue in security. Instead of relying on passwords or traditional biometrics, the system will rely on how users interact with the device.

This represents a major shift from point-by-point authentication to continuous authentication, from a fragmented experience to a smoother and more secure one.

In the age of AI, **your behavior may be the most secure password** .

You finished reading the article "**Behavioral biometrics: The new 'certificate' in the AI ??era.**" edited by the **TipsMake** team. We hope this article has provided you with many useful tech tips and tricks. You can search for similar articles on tips and guides. Thank you for reading and for following us regularly.

© 2019 TipsMake.com