AUTHENTICATION

Behavioral Biometrics: Hype or Hope?

Redacted Version

More than **9 billion credentials have been stolen since 2013** and according to the **Verizon 2017 Data Breach Investigations Report**, 81% of confirmed data breaches involved weak or stolen passwords. With biometrics delivering on the promise of a more convenient and secure logon experience, what does the next evolution in behavioral biometrics hold?

Aren't my fingerprints enough?

To address the problem of credential misuse, more and more businesses are moving toward multi-factor authentication (MFA), which require more than one method of authentication from independent categories of credentials. In fact, the MFA Market accounted for $4.05 billion in 2015 and is expected to reach $13.59 billion by 2022. MFA has proven to be an obstacle for all but the most sophisticated hackers, as it can make stolen credentials difficult to use.

One popular method used in MFA is biometric authentication, which makes use of unique physical attributes, such as fingerprint minutia stored in credential databases as biometric templates. As with any stored credential, templates are subject to attack. Technology like **biometric tokenization** can obfuscate bulk database templates and help mitigate this problem.

In June 2015, a hack of the Office of Personnel Management exposed 21.5 million records including fingerprint files for 5.6 million of them. Clearly, MFA is now a new frontier for hackers.

What are behavioral biometrics?

Since static biometric authentication factors can be stolen, new technology is evolving – behavioral biometrics. This method leverages dynamic data points based on unique interactions with a device. With the support of artificial intelligence (AI), behavioral biometric solutions adjust profiles continuously as users interact with a device. For example, a mobile phone could create a profile based on how you hold the phone, scroll, apply typing pressure, respond to pop-ups and other unique, dynamic data points that can't be duplicated by another individual.

Behavioral biometrics is poised to take off

In the 1970s, biometrics took off with speech recognition and signature verification. The technology has come a long way since then, with other trends setting the stage for a behavioral biometrics revolution:

- **Data Management:** Data science continues to see huge advances in the synthesis and processing of massive amounts of complex data, with the ability to analyze how all the data points relate to one another and pinpoint behavioral anomalies.
- **Artificial Intelligence:** The growing field of AI gives computers the ability to learn without being explicitly programmed. This leads to authentication solutions that can verify a user's identity throughout an authenticated session, and not just at the point of login, for greater security.
- **Frictionless User Experience:** Many successful apps, such as Uber and Pinterest, have focused on creating a smoother, less disruptive user experience (UX) to gain competitive advantage. We can see seamless authentication as a natural outgrowth of this rising technology.

What's to come?

Behavioral biometric authentication is still relatively new, but recent success stories are fueling the hype. For example, **Mastercard** has introduced a next-generation biometric card with a fingerprint reader for point-of-sale purchases. The **Department of Defense** is experimenting with authentication that analyzes a user's keystrokes.

This goes to show that with today's cyber threat landscape forward-thinking businesses are looking toward the next advances in cybersecurity, such as the biometric identity management and composite authentication.