

Behavioral **Biometrics**



International
Biometrics+Identity
Association

Overview

This paper explains how behavioral biometrics works, introduces some of the new technologies that make it possible, and looks at actual real-world applications of this powerful new tool.

Behavioral biometrics provides a new generation of user security solutions that identify individuals based on the unique way they interact with computer devices like smartphones, tablets or mouse-screen-and-keyboard.

By measuring everything from how the user holds the phone or how they swipe the screen, to which keyboard or gestural shortcuts they use, software algorithms build a unique user profile, which can then be used to confirm the user's identity on subsequent interactions.

Behavioral biometrics are currently deployed in online banking, e-commerce, payments, and high-security authentication markets.

- Because users can be enrolled in the background during a handful of normal interactions, behavioral biometrics is completely frictionless and doesn't slow, interrupt or otherwise interfere with the user experience.
- Because there are dozens and dozens of data points collected, and any combination of them can be used to identify a user, identification is accurate and precise and users cannot practicably be impersonated.
- Because authentication happens throughout the entire course of the transaction, behavioral biometrics provides powerful protection against insider threats and account takeover, as well as identity theft.

Behavioral biometrics does not replace the password or other legacy forms of identity authentication, but it does reduce the burden placed on them to protect sensitive data. Even the strongest password is only secure so long as it is secret. By offering an additional, continuous layer of identity assurance, behavioral biometrics prevents the password from being a single point of security failure.

Key Concepts & New Technologies

Human Behavioral Patterns

Human behavioral patterns consist of a variety of distinctive ‘semi-behaviors’ that make up an individual—they reflect your habits and micro-habits, and can be observed in any activity you undertake, such as speaking, typing and walking. Even when, to the naked eye, it might seem as though you behave just like the people around you, software can achieve what no human can—a unique profile comprised of a distinguishable combination of your behaviors.

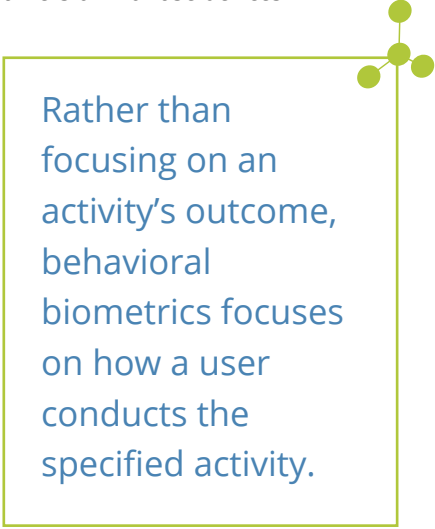
The patterns in your movements are formed not just by your physiology but also by social, psychological, and health factors, among others—helping to make them practically impossible to spoof or duplicate. If you are native language speaker, if you’re favoring an old elbow injury, or if you pause as you type certain words so that you can remind yourself how to spell them—all of these influence how your ‘semi-behaviors’ manifest in your interactions with computer devices.

Behavioral Biometrics

Behavioral biometrics is the measurement and recording of human behavioral patterns and their use to verify and authenticate an individual computer-user, either in real time or retrospectively. Rather than focusing on an activity’s outcome, behavioral biometrics focuses on how a user conducts the specified activity. Not whether the user-name and password are entered correctly, for instance, but how a user enters them: Are they typing quickly or slowly? Do they transition between the boxes with the mouse, or with the tab key?

Smart Sensors

Behavioral biometrics relies on increasingly ubiquitous, mobile computing devices like smartphones or tablets and wearables to capture data that will authenticate the user. Sensors have become smaller, as well as more configurable, efficient and connected in recent years. The rate of penetration of the consumer base continues to rise—more and more consumers own or use devices containing enhanced sensors. Devices like smartphones can be configured to passively capture behavioral data through the accelerometer and the gyroscope. That data can then be analyzed using advanced software algorithms in order to support identity authentication and fraud detection.



Rather than focusing on an activity’s outcome, behavioral biometrics focuses on how a user conducts the specified activity.

Machine Learning / Deep Learning

As sensors have become more prolific, the development of software algorithms that can analyze the vast fields of data they collect has also progressed by leaps and bounds. The role of artificial intelligence in behavioral biometrics is unique. As opposed to other fields such as image recognition and speech processing, in behavioral biometrics the AI is doing work that no human expert can do. The underlying event signals in which the computer-user’s behavioral data are encoded are not easily susceptible to human interpretation. Even a narrow AI can do much better than the most expert human.



... the ability to conduct continuous authentication using behavioral biometrics fills an important gap that's common in many current security programs.

Traditionally, behavioral biometrics involved extracting key signal features—such as the length of stride, cadence/speed of typing, or characteristic user flows through a user interface—which are then modeled for each user. This eventually yields a

characterization for all users, allowing individuals to be differentiated from each other. Recent developments in deep learning make this process more user-specific, allowing the AI to identify and model those features of each individual user's behavior that are most unique—that differentiate them best from among all the other users—which enables far better performance.

Use Cases

To date, behavioral biometrics technology has been deployed in four distinct types of applications: Continuous Authentication, Risk Based Authentication, Insider Threat Detection, and Fraud Detection and Prevention.

Continuous Authentication

The completely passive nature of the data capture in behavioral biometrics enables persistent, or continuous, authentication. By contrast, legacy authentication techniques are single-transaction based—identity is verified at a particular point in time, but not checked afterward. And they require a user to stop normal activity in order to accomplish an artificial task—entering a password, inserting a smart card, scanning a fingerprint. Continuous authentication provides assurance of an individual's identity over time, which is otherwise unavailable. Although confidence in that identity may naturally fluctuate, the

ability to conduct continuous authentication using behavioral biometrics fills an important gap that's common in many current security programs.

Behavioral biometrics applications of this kind continuously analyze a range of data generated by an individual using a computer device to access an account. Incoming data is compared with a previously stored profile in order to check for anomalies in behavior, and to generate a similarity score. If the score is above a predetermined threshold, the user's identity is considered verified, they are authorized and able to enjoy a full range of access or activities using the device. If the score falls below the predetermined threshold, the user's session is flagged so that security measures can take effect—for example, scaling back the user's access by logging them out, or restricting their ability to complete certain high-consequence actions such as a transfer of funds.

Behavioral biometrics solutions for enterprise security can be configured using a layered approach, depending on the location of the user and the confidentiality of the data they are accessing. Higher similarity scores can be required for instance for off-site logins. Typical deployments pair behavioral biometrics with PINs, card-access, and even security routines such as periodic forced password changes.

Risk-Based Authentication

Behavioral biometrics is also used to augment risk-based authentication for transactions conducted via web and mobile platforms. Specifically, a range of behavioral data generated by an individual using a device is analyzed in conjunction with the completion of a legacy single-transaction authentication method. For example, when a smartphone user accesses a banking app via



username/password entry, authentication mechanisms concurrently examine:

1. Behavioral qualities of the input data, such as typing speed or touchscreen interactions and their timing;
2. Supporting contextual factors of the current transaction, such as user device type, IP address, geolocation; and
3. The user's historical behavioral factors, such as the typical timing of user access, prior purchasing or access patterns, etc.

These data points are used to confirm that the person entering the username/password is in fact the authorized user, and not just someone who has stolen the authorized user's password. In such instances, behavioral biometrics doesn't provide unique, stand-alone identification, but rather layers onto existing ID techniques in order to enhance the certainty with which identity decisions can be made.


Insider Threat Detection

An insider threat is a danger to an organization that comes from malicious people with insider access, such as employees, former employees, contractors or business associates. Insiders have sensitive information concerning the organization's security practices, data and computer systems. Examples of insider threats include unauthorized exfiltration of sensitive data, vandalism and destruction of property, and even workplace violence.

A kind of biometric called User Behavior Analytics (UBA) can provide proactive defense against these threats by using big data and advanced algorithms to assess the risk of user behavior on the IT network. Leveraging security information event management (SIEM) data and network data, UBA technology overlays non-IT behavioral risk indicators as inputs and looks to detect patterns the organization has defined as insider-threat indicators.

Examples of non-IT risk indicators might include HR or compliance violations, demotion, having access to critical information, being at work outside of a normal pattern, increased complaints to supervisors regarding salary as well as isolation from coworkers. By combining employees' cyber footprints with non-IT behavioral indicators, organizations have a more complete picture of potential risks.

A study of insider cases by the US-CERT Insider Threat Center, a federally-funded research and development entity at Carnegie Mellon University, found that 27 percent of insiders had come to the attention of either a supervisor or coworker for some concerning behavior prior to the incident. Adding machine intelligence to monitoring of threatening behaviors can increase the chances of early detection and subsequent interdiction—before it is too late.



27% of insiders had come to the attention of either a supervisor or coworker for some concerning behavior prior to the incident.

Fraud Detection and Prevention

Fraud detection and prevention in consumer applications, financial services, and enterprise or government applications is the final primary use case for behavioral biometrics. In these deployments, behavioral biometrics applications are used for post-transaction forensic analysis to support fraud investigations, rather than to analyze identity data and conduct authentication in real time. For example, a financial services provider may use a behavioral biometrics application to examine months' worth of historical user data in order to better identify (1) what circumstances are flagged as potential fraud events, and (2) to validate the fidelity and utility of those alerts.



Behavioral biometrics are currently deployed in online banking, e-commerce, payments, and high-security authentication markets.

Utility & Benefits

Behavioral biometrics technology offers robust, risk-appropriate identity authentication and anti-fraud measures that are effortless for users and which require no special hardware or additional security steps.

- Flexibility—A virtually limitless array of behavioral biometric features are available for analysis, and selected features can be easily tailored to specific use case needs.
- Convenience—Behavioral biometrics analyzes the characteristic behaviors of a device user, without disrupting the user experience.
- Efficiency—For identity authentication, behavioral biometrics are applied in real time and operate concurrently with legacy authentication mechanisms such as password entry. For fraud detection, retrospective biometric behavioral analysis substantially reduces the time needed to identify and differentiate fraud from legitimate user behavior.
- Security—Behavioral biometrics are intrinsic characteristics that are extremely difficult for humans to discern and practically impossible to replicate, particularly when multiple behavioral features are examined concurrently.

Accuracy/Performance Considerations

Behavioral biometric technology gathers user data continuously, rather than during a single, fixed-length instance like a sign on with a token or scanning a fingerprint. As a result, it can achieve high performance, and provide a high degree of identity fidelity over time.

However, it is important to remember that the technology is designed to work in very specific scenarios. The range of accuracy demonstrated by current commercial implementations of behavioral biometrics depends on the quality and volume of data available for capture and analysis, as well as unique requirements dictated by the specific use case or application. Consequently, it remains difficult to broadly characterize the performance of behavioral biometrics across diverse market verticals.

Behavioral biometrics are currently deployed in online banking, e-commerce, payments, and high-security authentication markets.

Additional verticals in which this technology is expected to be deployed in the near future include e-learning—especially exam integrity solutions—and enterprise security solutions. Increased adoption is also anticipated among online service providers that are negatively impacted by account-sharing fraud.

To provide a general example of performance, consider an implementation of behavioral biometrics deployed in an online banking context: the use of behavioral data collected throughout the entirety of an online banking session—combining the results of each individual transaction (e.g., customer login, one time password, fund transfers, endorsement)—validated users with 99.7 percent accuracy.

Additional reporting on accuracy and performance can be found in the Additional Reading section.

Privacy

Privacy constitutes a leading concern for new identity technologies, including behavioral biometrics. Some view all biometrics as privacy-invasive. But there is a case to be made that behavioral biometrics are inherently privacy friendly. While the data your smartphone, for instance, collects about the way you use it can, over time and in aggregate, be used to confirm your identity, none of the underlying data points could individually be used to identify you. Your street address is still yours even severed

from other data like your name or zipcode. The way you wield your mouse cannot be used to find you. Moreover, behavioral biometrics relies on data that device or network operators are generally already collecting under standard privacy documentation.

It is worth noting that behavioral biometrics are agnostic of personally identifiable information or PII. I don't need to know anything about you to be sure it's you—I just know it's the same you that signed on last time. This actually creates the possibility for fully anonymous account identity authentication: All I know about you is that it's same you that signed on last time.

Looking beyond these innate characteristics, behavioral biometrics providers are also pursuing innovative approaches for addressing privacy concerns. Some examples include:

1. Educating users on the security benefits available to them through verifying their identity with behavioral biometrics;
2. Transparently informing users about how their data is being modeled and used; and
3. Enabling users to revoke, at-will, a usage license for their behavioral biometric data.

While privacy issues vary greatly from use-case to use-case, behavioral biometrics can provide tremendous benefit, at little-to-no cost in privacy, for both customers and users.

Outlook

Currently, behavioral biometrics are deployed as an additional layer to enhance identity authentication and fraud detection systems.

The future performance of behavioral biometrics, however, is limited only by the capabilities of the sensors available to collect behavior data, and the AI capabilities available to analyze it.

As the ubiquity and sensitivity of devices that collect behavioral data grows, and as the accuracy with which AI can analyze the data increases, behavioral biometrics have the potential to become a widespread, user-friendly, high-performance identity authentication technology.

Additional Reading

Defense Advanced Research Projects Agency (DARPA) – Active Authentication Program: Program Page: <http://www.darpa.mil/program/active-authentication>
Open Catalog Publications: <http://opencatalog.darpa.mil/AA.html>

BehavioSec, *BehavioWeb: A Case Study of BehavioWeb in a Real World E-banking Environment* <https://www.behaviosec.com/wp-content/.../BehavioSec-CaseStudy-DanskeBank.pdf>

BehavioSec, *Lifting the lid on Digital Behaviour: The Discrepancy between our Online and Offline Selves* <https://www.behaviosec.com/resources/>

BehavioSec, *Accuracy Report for Native Mobile Application* <https://www.behaviosec.com/resources/>

Novetta, *Improving Authentication Mechanisms for Enterprise Information Systems* https://www.novetta.com/wp-content/uploads/2015/03/NOV_Active_Authentication_Overview.pdf

Leidos Corporation, *User Behavior Analytics: The Key to Detecting Insider Attacks*, <https://cyber.leidos.com/products/insider-threat-detection>

TwoSense, Inc., *Mobile Authentication using Device Motion Characteristics*, <https://www.twosen.se/resources.html>

Identity Matters



International
Biometrics+Identity
Association

1090 Vermont Avenue, NW • 6th Floor
Washington, DC 20005

202.789.4452 x1309
IBIA.org