AdNovum

From binary yes/no to continuous authentication

The rules of online identity verification change when you combine a dynamic risk assessment and machine learning solutions. Behavioral biometrics as the missing link to achieve a cognitive security layer.

By Ingo Deutschmann

As humans, we are taught that we are the weakest link when it comes to IT security. Many attempts have been made to remove the human factor from the security equation, but no one has succeeded. If we look at the security we're used to in our devices and services, it is based on thinking from the 1970s, where a binary yes or no at login made more sense. In our always-on culture, that kind of thinking is no longer adequate. Equally, adding extra steps can be a good way to boost security, but also gets in the way of user experience. It is ironic, then, that the human factor, the so-called "weakest link", can be the solution to the security challenge, simply by humans behaving normally.

Big data machine learning biometrics

To find the beginning of the story we need to travel all the way to the Arctic Circle in northern Sweden to Luleå University of Technology. In 2006, an undergraduate behavioral biometrics project, with help from the university's innovation team, resulted in three students founding the spin-off BehavioSec. The idea was uncomplicated while the technology, the algorithm were not. Would normal end user interaction with a device or keyboard be enough to verify the identity of a human being? Are we that unique?

Behavioral biometrics

Human gestures can be repeated in ways that may look similar to the naked eye, however, when they are measured by a behavioral algorithm, they look totally distinct. The way a person holds, swipes, or types on a screen or keyboard is a source of data for user authentication and verification.

Behavioral biometrics technology doesn't measure just one gesture, but a whole range of data inputs, with a high level of accuracy and precision, and can do so throughout a user session. This new capability to be able to continuously authenticate an end user, not just at login, is intriguing to a wide range of organizations, as they see a solution that can protect against account takeover, identity theft, and even internal fraud.

The power of choice

The modern end user of today has high expectations on user friendliness, and they know that they are in a power position to get what they want. Whenever end users are offered a choice they will act with brutal decisiveness: One BehavioSec client operates

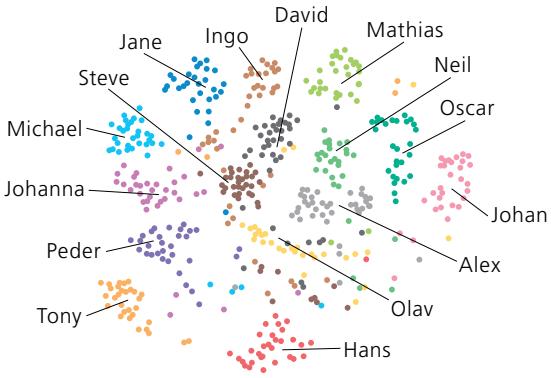
About Ingo Deutschmann

A security professional with more than 15 years of experience in development, consulting and product services, Ingo Deutschmann is Business Development Director DACH at BehavioSec. With his former background as General Manager Germany at Gemplus, he will add to the team his knowledge in security software development as well as his experience from the Swedish start-up company Celo Communications and German DEH GmbH, where he was responsible for R&D operations. Ingo was codeveloper of the hardware antivirus solution ExVira. He is a mathematician from the University of Jena, and holds worldwide patents for a smart card reader.

as an identity provider for banks with a combined user base of 7 million. When they started offering strong authentication with a mobile app supported by our behavioral biometrics technology, they saw an exponential growth in usage from 3–4 transactions a month to 20–25.

This highlights the potential for user experience successes, and how the disruption of financial services is already in progress.

Pre analysis



BehavioSec analysis

The BehavioSec scatter plots above before and after BehavioSec algorithm analysis. To the left: clusters of processed end user data from 15 people typing one same password where each dot represents one session. The end user behavior profile cluster is the result of the transformation of 22 dimensions that are simplified into 2 dimensions.

Risk-based authentication

Product, customer and end user experience teams are continuously working to decrease friction, in order to meet the high expectations of busy, multitasking users. Adaptive, dynamic, layered security helps you to create authentication processes that align with these expectations.

Fewer than 30% of us log out of our accounts when we're finished using a service. Our mobile apps are especially vulnerable, even more so now that social media services also act as identity providers and will soon be entering the payments space. Security needs aren't all the same, even within these individual services. For example, checking your bank balance is not as risky as carrying out a large transfer or changing account details.

Get the right level of security, at the right time

BehavioSec analyzes every session from start to finish, continuously profiling behavioral patterns. The system creates a profile match score based on a range of factors, by comparing it to stored results. Is this person typing as they normally do? Are they in a recognized location, using their usual device? This is monitored throughout the session, so that security is an ongoing process, not just a step.

From yes or no to "if-this-then-that"

As a user interacts during a session, the similarity score is fed into your risk engine, and your security or fraud team determines what happens next. If the score is high, the system allows the user through. If it's not high enough, that's when you can add further steps, using the other layers in your system. If the score is very low, your system can log the user out completely.

If it is not you, then who?

BehavioSec has already proven to successfully verify that it is the right person requesting access. The holy grail of fraud prevention is to be able to transform end user behavior to narrow down the group of known users who are the prime suspect for a potential fraud. This is accomplished by efficient machine learning capabilities and applying artificial intelligence to user profiles. Our user profile's level of sophistication enables BehavioSec to find the needle in the haystack. Consequently, more session intelligence will increase the chances for it to be a customer-friendly and secure user journey. By transforming existing user interaction behavior into an additional layer of security you have created a cognitive security solution that will considerably improve the security posture. ■

Imprint

Publisher:
AdNovum Informatik AG
Corporate Communication
Roentgenstrasse 22, 8005 Zurich
Phone +41 44 272 6111
E-mail info@adnovum.ch
Subscription: www.adnovum.ch/notitia
www.adnovum.ch
Responsibility and editing:
Andrea Duttwiler
Feedback: notitia@adnovum.ch
Design and realization:
Comuniq, Zurich
Photography:
akg, Berlin, Gerry Nitsch, Zurich, Fabian Unternährer, Berne
Printed on Balance Pure