Secure Coding.
Practical steps to defend your web apps.

Copyright SANS Institute
Author Retains Full Rights

This paper is from the SANS Software Security site. Reposting is not permitted without express written permission.

Interested in learning more?
Check out the list of upcoming events offering "Defending Web Applications Security Essentials (DEV522)" at http://software-security.sans.org/events/
Let's begin with a question for enterprise security teams and system administrators: How do you know your users are truly your users? Are strong passwords and simple authentication mechanisms protecting your organization? The rate of fraud and cybercrime continues to grow significantly every year at astronomical rates. In July 2018, the FBI announced that funds stolen because of Business E-mail Compromise (BEC) scams—a scam typically based on account takeover and user impersonation—had totaled more than $12.5 billion over an approximate five-year period.1 With this much money walking out the door, it may be time to consider how your users are being authenticated and verified.

The easiest answer for many has been multi-factor authentication (MFA). It’s true that MFA can be used to significantly reduce the attack surface; however, that depends upon correct implementation and usage. Unfortunately, some organizations implement MFA but do not enforce it. High-ranking members of the organization may insist on not having MFA because they deem it an inconvenience. We are seeing that older defense mechanisms, such as tokens, simply aren’t working anymore.

In response to ineffective or “inconvenient” multifactor mechanisms, SANS worked with BehavioSec to understand how they are using behavioral biometrics to defeat advanced automated and manual attacks. In this paper, we'll define behavioral biometrics, examine what it can mean for your organization and explain how BehavioSec can implement it within your authentication processes. We also spent some time reviewing BehavioSec’s product and will discuss a case study where the system was able to detect—and block—automated and remote-access account takeovers.

Overall, we found BehavioSec's implementation and use of behavioral biometrics to be extremely effective in validating user activity while providing a seamless authentication experience. Its product can move seamlessly between user platforms, something we found unique and necessary in today's ever-mobile workforce. We can see how arming organizations with behavioral biometrics as part of their authentication mechanisms could shift the advantage to the information security team and allow the organization to mitigate attacks such as account takeover and detect good vs. bad users.

**Behavioral Biometrics**

Before we launch into BehavioSec’s product, we first wanted to understand what behavioral biometrics is and whether it can be utilized to effectively secure your users. The concept of behavioral biometrics centers around profiling the data about your users, instead of collecting data from your users. Let’s clear the air on one thing: When we say data about your users, this is not the collection of sensitive documents or data from their systems.

Behavioral biometrics instead focuses on analyzing and building profiles of the behavior of your users. These behaviors can include, but are not limited to:

- How they type, the keys that they press and how they press them
- How they move the mouse
- How quickly they answer questions that they should know
- How slowly they answer questions that they shouldn’t know
- How they swipe left to right on a mobile platform or utilize other gestures

This data can be used to design an algorithm that details a legitimate user. However, it’s important to note that these data points cannot be captured just once and then used as permanent authentication mechanisms. After all, user behavior can and does change. The tools must be able to adapt. Therefore, the second required element of behavioral biometrics is that it continues to be honed as more data about the user is observed. It must also be adaptable; users may sometimes access the same resource via different platforms. All of this is legitimate activity, and the tool must be able to account for behavioral variances that different platforms can introduce.
The collection of this data allows for each user to have a custom profile, or algorithm, that distinctly identifies who they are. This step allows your organization to say, with confidence, that the user who logged in is the true user. Think of it as user baselining—this collection and profiling activity occurs in the background without impacting users. And when you have a baseline of what’s good, it becomes trivial to identify what’s bad.

We tend to think that this is where the future of authentication must go. Some authentication mechanisms currently in place take advantage of potentially hard-to-spoof qualities, such as facial recognition or fingerprint scanners. But each of these solutions has an issue: They are dependent upon additional action by the user. Furthermore, every ounce of friction that is created by the authentication measure increases the risk of being abandoned by the users completely. What we found, and what we like, about behavioral biometrics is that it is designed entirely around profiling users for their individual human idiosyncrasies, which are almost impossible to spoof and replicate.

This is where the power of behavioral biometrics lies—having the capability to automatically detect when an account is being used by a legitimate user or an imposter, and all the legitimate user must do is be themselves.

**BehavioSec**

Enter BehavioSec, an organization that has figured out how to utilize and seamlessly integrate behavioral biometrics into user authentication. We had the chance to test BehavioSec’s authentication integration, and we learned how BehavioSec integrates with your platforms to build user profiles. BehavioSec’s understanding of defense mechanisms is based on stages of attacker activity and/or account takeover. Figure 1 provides details on these three stages.

**BehavioSec’s Behavior Biometric Model**

In our testing and analysis of the tool, we found that BehavioSec develops and relies on three unique behavioral biometric models. Let’s look at each briefly:

**Behavioral Score**

The behavioral score is the first score BehavioSec develops when a user interacts with the authentication system. This score is developed by monitoring much of the data we described previously: how a user does what they do and with what frequency they do it. This behavioral score is kept from user to user, from session to session, and is refined based on all that the user does.
Confidence Score

The aptly named confidence score illustrates the level of confidence that BehavioSec is witnessing activity from a legitimate user. The confidence score is a crucial element to evaluating user risk because it allows for decisions to be made on user authentication depending on confidence level. The behavioral and confidence scores illustrate one of BehavioSec’s strong points: the capability to continue refining its user algorithm as the user interacts with the system time and again.

Risk Factor(s)

The risk factor is BehavioSec’s way of describing observations about user activity. We will discuss data enrichment in our next section, but the risk factor considers not only the user activity, but also the other observables—such as whether the user is accessing a resource remotely, the user has changed IPs, or other potentially suspicious changes in activity.

Bringing It All Together

Armed with these three metrics, BehavioSec can assess whether your users are who they say they are. Figure 2 shows an example of how BehavioSec analyzes a user approaching a website and entering their password.

Let’s look at how BehavioSec is uniquely examining each piece of the puzzle:

- Notice that the tool first identifies use of the mouse, which is hard to replicate.
- The tool then examines how the user enters data into username and password fields. Again, the way the user types, whether he or she tabs or clicks between fields, etc., are all traits unique to the user, and hard for attackers to replicate.
- Each step is evaluated and scored accordingly in the background while the user is accessing a website. Because BehavioSec is examining and scoring behavior as it is happening, it can make snap decisions about access legitimacy.

Now, let’s examine the second half of BehavioSec’s analysis and see if the user threw any suspicious wrenches into the engine. During its analysis and observation of this quick event, it appears that there were some concerning activities caught by BehavioSec. See Figure 3 on the next page.
As we can also see in Figure 3, there are anomalies in how the user interacted with the web form fields. These anomalies are classified as “Active Flags” by BehavioSec, as we can see in Figure 2. We can see that there is a discrepancy between characters in a field vs. keystrokes captured, which may be indicative of someone attempting different passwords or mistyping an entry. The tool also recognized that the password field was entered via a CTRL+V command, which would be indicative of a copy/pasted password. Is this inherently suspicious? No—but it shows that BehavioSec is analyzing even the smallest nuance for an indication that a user might not be whom they say they are.

Let’s take it a step further. In the aforementioned figures, we examined suspicious activity from a single login session. While it yielded a lot of data, that one session didn’t establish a well-developed profile of user activity. As we’ve mentioned, behavioral biometrics must be cumulative and accepting of user habits. As we can see in Figure 4, BehavioSec also provides the capability to view the history of a user, as well as scoring of various behavioral observations in points in time.

During our testing, we accessed the platform multiple times, sometimes changing tiny behaviors and other times making drastic changes that would introduce indicators of concern. Sure enough, BehavioSec kept pace with our testing and was able to determine, even in intra-minute changes, the different risk profiles that our user data presented to the platform. Notice that between 22:09:06 and 22:09:24—a mere 19 seconds—our activity changed enough to remove any confidence in the session and raised the risk considerably. BehavioSec provides us another view where we can get direct insight into each login transaction. Note that in Figure 5, we can see BehavioSec working through its algorithm and adjusting its recognition of our activity ever so slightly.

This level of data analysis—performed in the background—can be crucial in detecting and preventing attacker access to your enterprise. Attackers can steal credentials, hijack sessions, and impersonate a user within a matter of seconds. It helps to have a tool that can move as fast as they can.
Enriching Your Authentication Data

Thus far, we've covered BehavioSec’s unique approach to profiling user activity based on tracking user interaction and nuances. Luckily, the analysis does not stop there. BehavioSec also has the capability to enrich its detection data with external sources and/or additional correlation. Figure 6 examines some of these enrichment capabilities.

Integrating with Your Platform

Let’s be frank: The last thing your security and/or SOC analysts need is another dashboard to analyze—or another data set to wrangle. This is yet another benefit we found in BehavioSec's favor: Its platform is not designed as an additional, passive tool. BehavioSec operates best when integrated within your authentication platforms, helping to refine your user profiles and assist in controlled access. To facilitate this design, BehavioSec is highly extensible and prefers to be correlated with other data sources via an API.

Before we dive into our testing results, we want to examine a larger point: When considering new security implications, consider how these tools can integrate with your current environment for automated defense. This has been a constant trend in many of our SANS reviews and surveys lately, including high-level topics such as incident response and endpoint management. Organizations are looking for ways to automate and integrate security, without providing another “pane of glass” or a complicated system that requires a team of specialized engineers. User authentication and verification should be no different, and the creators behind BehavioSec obviously felt the same way and designed their platform as such.

BehavioSec in Action

We set out to test BehavioSec with a straightforward objective: We wanted to take over a user account and perform some unauthorized activity. Obtaining that access was another story. We took a fairly straightforward, and attacker-typical, approach: We attempted to make ourselves look like a bot and steal a user’s credentials to access the site remotely. Unfortunately for us, but to BehavioSec’s credit, we were unsuccessful.

With other authentication mechanisms, the logging and alerting may start when a malicious actor visits a site, but telemetry (such as an external IP) can be a weak indicator of attacker activity. The problem for attackers is that immediate interaction with the authentication platform tells BehavioSec to start analyzing. Furthermore, because BehavioSec relies on user interaction to fine-tune a profile, the product is constantly monitoring activity. Thus, even if we attempted to take over an active session—which we did—it profiled us quickly. Figure 7 illustrates some of the initial detection mechanisms.
Obviously, our attempts were not successful. It’s easy to see that the platform quickly detected that something about our user session had changed. Figure 8 shows us why these sessions were flagged as malicious.

We can see that BehavioSec alerts in a few different areas:

• Using known heuristics, the tool was able to detect that a bot was being used for form completion and login activities. We were fascinated to read the activity that the tool detected: Terms such as “too-uniform typing rhythm” gave us insight into just how much detail the tool can collect.

• BehavioSec tripped on a few data integrity rules, similar to our earlier example, but this time we can see that paste and/or autocompletion was detected, again indicative of automated activity.

• The tool was able to enrich the session data and discover that remote activity was evident due to the presence of TeamViewer protocols. TeamViewer itself is not inherently malicious and is used legitimately by IT administrators around the world. However, in this example, BehavioSec detected that my account typically did not utilize remote access software, and thus it was flagged and alerted on. It detected, and successfully defended against, unauthorized remote access activity.

Even in our simple test, we were able to observe the power of BehavioSec’s use of behavioral analytics. We attempted to use automated and remote access means to compromise a financial website, and were quickly shut down due to rapid anomaly detection techniques.
Defeating attackers with legitimate credentials can sometimes feel like trying to recognize a person you've never seen or met before. How can you tell the difference between a good user and a bad user if you don't know anything about the user? Multiply that problem by the number of users within your organization, and the problem no longer seems tough—it seems almost impossible. In this paper, we examined the use of behavioral biometrics to combat this problem and found that BehavioSec offers a viable, easy-to-use solution.

When it comes to capturing, modeling and implementing behavioral biometrics, we found BehavioSec's product to be a clear leader in the space. One of our top priorities during this review was seamless integration: Any authentication mechanisms that ruin user experience (or even cause friction) will make users abandon and reject your added effort, putting your shiny new purchase back on the shelf. BehavioSec understands this problem and makes it a top priority.

We found that BehavioSec provided clear insight into our user sessions and real-time feedback to continually assess user legitimacy. The confidence and behavior scoring provided easy-to-pivot data points that can be integrated with other tools to enrich user authentication activity. But we continue to stress our favorite feature of BehavioSec: continuous authentication. BehavioSec's model works by constantly tuning to the user session, microsecond-by-microsecond and session after session, and thus was always testing data based on user activity. This provided the user with data that becomes stronger and stronger with each user session. In our experience, stronger data allows for better security decision-making.

We would recommend that you examine whether behavioral biometrics would be a good fit within your organization. If your security team is struggling to keep attackers out or to enforce strong authentication policies on your users, consider a stronger and more seamless option. Attackers aren't stopping anytime soon. We know their game—it's time for them to guess ours.
**About the Author**

**Matt Bromiley** is a SANS Digital Forensics and Incident Response instructor, teaching Advanced Digital Forensics, Incident Response, and Threat Hunting (FOR508) and Advanced Network Forensics: Threat Hunting, Analysis, and Incident Response (FOR572), and a GIAC Advisory Board member. He is also a principal incident response consultant at a major incident response and forensic analysis company, combining experience in digital forensics, incident response/triage and log analytics. His skills include disk, database, memory and network forensics, as well as network security monitoring. Matt has worked with clients of all types and sizes, from multinational conglomerates to small, regional shops. He is passionate about learning, teaching and working on open source tools.

**Sponsor**

*SANS would like to thank this paper’s sponsor:*

![BehavioSec Logo]
# Upcoming SANS App Sec Training

<table>
<thead>
<tr>
<th>Event</th>
<th>Location</th>
<th>Dates</th>
<th>Format</th>
</tr>
</thead>
<tbody>
<tr>
<td>SANS 2020</td>
<td>Orlando, FL</td>
<td>Apr 03, 2020 - Apr 10, 2020</td>
<td>CyberCon</td>
</tr>
<tr>
<td>SANS Amsterdam May 2020</td>
<td>Amsterdam, Netherlands</td>
<td>May 11, 2020 - May 18, 2020</td>
<td>CyberCon</td>
</tr>
<tr>
<td>SANS Silicon Valley - Cupertino 2020</td>
<td>Cupertino, CA</td>
<td>Jun 22, 2020 - Jun 27, 2020</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS Copenhagen August 2020</td>
<td>Copenhagen, Denmark</td>
<td>Aug 24, 2020 - Aug 29, 2020</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS Network Security 2020</td>
<td>Las Vegas, NV</td>
<td>Sep 20, 2020 - Sep 27, 2020</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS OnDemand</td>
<td>Online</td>
<td>Anytime</td>
<td>Self Paced</td>
</tr>
<tr>
<td>SANS SelfStudy</td>
<td>Books &amp; MP3s Only</td>
<td>Anytime</td>
<td>Self Paced</td>
</tr>
</tbody>
</table>