The Most Powerful Name in Corporate News and Information
All rights reserved! ceocfointerviews.com
Issue: January 14, 2014

Security and Authentication based on Analyzing User Interaction for PCs, Smartphones and Tablets

***Benny Rosenbaum -** CEO*

BioCatch biometrically authenticates users and detects cyber threats such as Trojans and remote access attacks. BioCatch tracks and analyzes user interaction with online and mobile apps (e.g. Mouse, keyboard and touch) and leverages its “Invisible Challenges” patent pending technology to deliver high detection accuracy and speed. In 2013, the company released its first product and received recognition from multiple publications and from top research firms - Aite Group and Gartner Research. BioCatch is currently deployed at several North American and European banks, protecting millions of online banking users. The company was founded in 2011 by experts in neural science research, machine learning and cyber security. Privately funded and headquartered in Boston MA with R&D offices in Israel.

Interview conducted by: Lynn Fosse, Senior Editor, CEOCFO Magazine

CEOCFO: ***Mr. Rosenbaum, what is the concept at BioCatch?***
Mr. Rosenbaum: The concept of BioCatch is to protect an online or mobile account in a new, disruptive way. The traditional way for authenticating the user is by something you know like a password or something you have like your PC or a special token. We want to authenticate the user by answering a simple question, “Is it the user or not?” The way we do it is by analyzing the user interaction with the device, whether it is a PC – through input interfaces such as a keyboard or mouse - or with the mobile device, through analyzing the way you hold and touch it. That helps us to build a profile of the user and say whether it is the real user or not.

CEOCFO: ***How do you do it?***
Mr. Rosenbaum: Let us start with the PC. In a PC environment we analyze the way the person works with the keyboard, mouse, trackpad etc. It appears that everyone is unique in the way we work with the keyboard and the mouse. Analyzing keystrokes and mouse is something many people tried to do in the last twenty years. There are many universities, many PhDs and professors who have done it. But there was always one problem: there was no way to take it to the commercial world, because you needed something like 15 minutes of interaction in order to make the call about the identity of the user. This made it impractical for any commercial application you can think of, like online banking or eCommerce. Alternatively you could do it fast, with horrible false positives or detection rates. So they proved the concept; they showed that they can separate people by analyzing the keyboard and the mouse, but it stayed an academic exercise.

What BioCatch did – and that’s by leveraging our patent pending technology – is to decrease the detection time from fifteen minutes to less than one minute. The main problem with existing technologies is that it’s an uncontrolled environment: the user can do whatever they want, and you need to wait for the user to provide you with sufficient biodata. We introduce into the session a series of controlled environments where we know exactly what the user is about to do; and we do it without the user ever noticing any change to their user experience.

How do we do that? We actually inject into the session an invisible challenge. We place a very subtle deviation – say, when you move the mouse, we add a small sideways motion – and since the user is moving the mouse towards a certain target, their brain automatically compensates for the added motion and a corrective maneuver is carried out. This is a spontaneous reaction that the user is never aware of, because it’s a low-intensity challenge and you basically filter such small adjustments out. But we just created a small controlled environment where we know exactly what the user is about to do (offset the challenge as they continue their previous movement), and can now look at things like: how fast did your brain recognize the deviation? Did you make one corrective move or several? Did you overshoot the target and only then made a correction, or did you correct on route to the target? What sort of corrective move did you do?

The bottom line is this: we challenge you, and you respond without feeling any change to the regular user experience. The way you react gives us a lot of cognitive-behavioral biometric data that allows us to increase accuracy dramatically, and decrease the detection time from fifteen minutes into the session to less than one minute after it started.

CEOCFO: ***Would you provide another example?***
Mr. Rosenbaum: Think of what happens when you work with your computer and the cursor disappears. You start searching for it by nudging your mouse. Now, imagine that we hide the mouse for a short while, and when people start looking for it they get it back immediately. This happens a lot in any case. We then look at how you searched for the mouse. Was it clockwise or count-clockwise? Wide search patterns or very small ones? Fast, sharp movements or round, slow circles? Everyone is different, and this is another example of how to introduce a small 'island' of controlled movement into an otherwise random session. So, from time to time we will introduce such a challenge, and see how you respond. We make sure people are not consciously aware of any change to their user experience – that's important. If I ask you at the end of the day if something went wrong with your interaction with the PC, you would say, "No, everything was just great." But these challenges and responses turn the tide. They allow us to look for consistent, distinct behaviors. The way you react is very unique to you, and it gives us a lot of biometric data; this allows us to do the detection much faster and with a great accuracy.

> **"BioCatch brings something completely different to the security market: a unique visibility into user behavior, so you can verify it's really them without changing the user experience. It works on PCs, Smartphones and Tablets, 100% friction-free, and works against all forms of advanced cyber threats. This is priceless, and the market is really excited about it."**
> **- Benny Rosenbaum**

CEOCFO: ***How can there be so many variations looking for your cursor, for example, that it would be unique to an individual user?***
Mr. Rosenbaum: There are around three hundred fifty parameters that we are using. Not all of these will be consistent for you: there are many parameters where we'll observe a high variance: say, between times where you are alert and times you are tired. There are also many parameters that are not distinct: you like exactly like me in these specific parameters. However, out of these three hundred and fifty parameters there are around twenty to twenty five parameters that are both consistent and distinct for an individual. My twenty will be different than your twenty, and the selection of these parameters is done automatically through machine learning algorithms. I will give you a few examples. You make a lot of mouse movements to the right, and a lot to the left. If we look at the ratio of certain parameters for right movement vs. left movement, this is very consistent for a given user. Same for up vs. down, or moving in certain diagonals. Other parameters have to do with whether you type looking at the keyboard or using blind-typing. There are certain parameters that have to do with muscle strength and the length of your hand. The bottom line is that out of the three hundred and fifty parameters which we have a developed, around twenty parameters are consistent for the person and are also distinct when compared with others.

CEOCFO: ***Would you tell us about the mobile aspect?***
Mr. Rosenbaum: With mobile there are many additional parameters that we can use. That is because with mobile is something you hold and touch. First, we look at the way you hold it, what happens to the device when you touch it in certain ways, how fast you type on the device when it's held in a certain way, how strong is your finger press when you touch the screen, and many more parameters like that. In fact, the mobile environment is extremely rich and we collect a huge number of parameters, and it helps us understand the unique way in which the person is going to work with the device.

CEOCFO: ***Where are you in the development, roll out and commercialization process?***
Mr. Rosenbaum: We started the company two in mid 2011, invested in a significant amount of research into behavioral analysis and testing our invisible challenges on thousands of real people, and finished the product development in May 2013. One month later we made the first big deployment in a bank in Canada with a customer base of over a million users. Last month we installed the system in three other banks; a Top 50 bank in the US, a Top 5 bank in Spain and another bank in Italy. The Italian bank is an interesting story: it's one of the biggest banks in Italy. They heard about BioCatch, liked it immediately and we integrated it into their new platform in just one day, which is half of our usual deployment time of two days. They expect hundreds of thousands of users in the coming years and we are going to protect their accounts on PCs and mobile devices. To summarize, we are running even faster than we planned; we planned to do POCs this years and sell in 2014, but we've already closed a significant deal in 2013.

CEOCFO: ***When you are speaking with a prospective client do they believe it? Is there something you can say or do where they really understand that it is going to work?***

Mr. Rosenbaum: When we come to a customer they immediately like the solution, and want to test it. And the test results are very much in line with our lab data. The system works.

We normally talk to the fraud team, who likes the fact we can fight the most advanced attacks they experience, and then they bring over the digital banking team – who quickly spots the enormous value of authenticating users in a friction-free manner.

The banks are telling us that we bring a completely new domain into fraud fighting. They already have technologies for looking at user's devices and say if they are new ("device recognition") or if the PC has been compromised. One example is a company called Trusteer, which was recently sold to IBM for six hundred and thirty million dollars and can tell the bank whether there are Trojans on the user's machine. Then there are technologies that look at your transactional behavior; whether you usually transfer money in the morning and now you transfer money in the middle of the night, or the amount is too high, which triggers an alert that says "Something is wrong here."

But spotting suspicious things around your device or transaction isn't providing sufficient defenses. Fraudsters know how to bypass these controls, and they create more and more false positives – basically suspecting more and more genuine traffic.

We come from a different angle, and leverage a completely different set of data. We do not care about the computer; we do not care about your transactions. We only care about one thing: is it you or is it someone (or something) else. For the banks, it is very easy to test our performance. The first thing they do is open the staging environment so we can install a Java Script for data collection; this takes 1-2 days, doing some functional testing and then moving the change into production. Then after a couple of months they can see the results for their own customers. Once the bank establishes the need and sees the path to testing our performance is very easy, it's the best way to convince them that our technology is working.

CEOCFO: ***What happens when you sense that it is not the right person? What happens next?***
Mr. Rosenbaum: We actually provide the bank with a score. The score says whether we believe that this is the customer or not. Now, what the bank is doing with the score depends on their risk management strategy. If the user just goes into their account and look at the balance, perhaps the bank won't do anything even if the score is high. However, if we there's a transfer of money to someone that user never transferred to before, and the BioCatch system says that it is not the genuine user, they will probably stop the transaction, challenge the user, or manually review the event. For example, they may investigate and decide to call the user via phone, present the user with a secret question, or use Out of Band authentication, in which they send you a one-time code via SMS text message. There are many actions that the bank can decide to do if they feel that something is wrong.

Another thing we do is detecting advanced cyber attacks via analyzing user interactions. It's the same technology, but rather than focus on building a profile for the genuine users, we focus on understanding what advanced cyber threats like Man in the Browser, bot activity and Remote Access attacks (RATs) look like. We can then immediately detect them, which gives the bank a terrific benefit. We do it very differently than anti-virus and anti-malware companies; we don't analyze the malware itself, but rather the discrepancies it creates in the user interaction when used in an online banking session. It saves the usual cat-and-mouse game of chasing malware.

CEOCFO: ***You have talked about banks. What other targets will you be looking at? What other types of companies in the beginning?***
Mr. Rosenbaum: When we started working on our technology, we figured out we have a (good) problem: it is good for many use cases in many industries. We can protect your email account or your social network account or your cloud solution; we can protect not just consumers, but also employees that access corporate applications on mobile devices or via PC.

But a start-up must focus to succeed, and we decided to start with online banking, because the banks are experiencing significant difficulties with current authentication and fraud prevention tools: they can be defeated by cybercriminals, and create a growing friction problem for the users. Once we've helped the banking industry, the next step will probably be email accounts and social applications and then cloud and mobile applications. The list is almost endless, but this is for the next two or three years.

CEOCFO: ***You personally have a long history with developing and running companies and technology. What attracted you to this opportunity?***
Mr. Rosenbaum: The fact that there is an actual online battle between the industry and the bad guys, and we can help. Most of my team is based on military intelligence people who were involved in signal intelligence or cyber operations. What they actually do there is behave like hackers, but for a good cause. Now they've gone to the other side: the Defense

side. They try to protect against the same tools and know-how they used in their service. Every week we discuss the new challenges the industry is facing and think about ways to defend against them; it is very exciting! It's ten times more exciting than developing applications and software tools. It's very dynamic, and if we do our job well, it will help millions. And every day there's something new. That's because thousands of people around the world wake up in the morning and think about new ways and methods to steal our money, to steal our secrets, to steal everything; and we are here to counter these efforts. This is very exciting.

CEOCFO: ***Are you funded for the steps that you would like to take next?***
Mr. Rosenbaum: We are privately funded. So far we've raised four million dollars and now we're actually in the beginning of a new round of around five million dollars, out of which the existing investors contribute one million; in fact they already put that money. The rest will be raised from venture capital; we are in the beginning of negotiations with a few VCs in Israel and the US. This is expected in the first half of 2014.

CEOCFO: ***Why pay attention to BioCatch today?***
Mr. Rosenbaum: BioCatch brings something completely different to the security market: a unique visibility into user behavior, so you can verify it's really them without changing the user experience. It works on PCs, Smartphones and Tablets, 100% friction-free, and works against all forms of advanced cyber threats. This is priceless, and the market is really excited about it. We finished 2013 with multiple installations in US, Canada and Europe; we already protect millions of users. Gartner picked us as a Cool Vendor for 2013, and financial services consulting firm Aite named us an emerging player in biometrics, and mentioned in their report that our biggest opportunity is in Mobile. We absolutely agree. Banking and all other financial applications are already available on mobile devices, and in the coming years they want to add more functionality, which means taking more risk; but they don't want to add friction. They can't – the users won't tolerate any high-friction security on mobile devices. The way that we protect the mobile device is very unique, and has no impact on the user experience. The protection that we provide to mobile applications is something very unique in the market today.

BIO: Benny Rosenbaum brings to BioCatch over 25 years of experience. Prior to establishing BioCatch, Benny was the co-founder of Magic Software Enterprises (NASDAQ: MGIC). During his 14 years at Magic Software he was a key player in increasing the sales to $100M annually and to selling millions of installations worldwide. Previously Benny established the enterprise division of Babylon (TASE: BBYL) and held the position of CEO at VapiSoft and MyNayad. Benny is a respected chief executive officer highly valued for his guidance and implementation of innovative solutions amongst startup companies. His extensive sales experience has influenced the success of numerous large companies worldwide.

BIOCATCH.
Behavioral Profiling

Biocatch Inc
155 Seaport Blvd.
Boston, MA 02210
617.480.4262
www.biocatch.com