Fighting Fraud with Behavioral Biometrics and Cognitive Fraud Detection

IBM Security’s Brooke Satti Charles on the Power of These New Capabilities
As fraudsters continually refine their techniques to steal banking customers’ credentials, IBM fights back with new tools that use behavioral biometrics and cognitive fraud detection. IBM’s Brooke Satti Charles offers a preview.

Satti Charles, a Financial Crime Prevention Strategist with IBM Security Trusteer, is enthusiastic about the new behavioral biometric analysis capabilities in Trusteer Pinpoint Detect, which uses patented analytics and machine learning for real-time fraud detection.

“This new behavioral biometric capability leverages cognitive technology that seamlessly analyzes users’ mouse gestures, understanding subtle mouse movements, and delivers actionable risk recommendations,” Satti Charles says. “And these capabilities help to maximize detection, reduce false positives and optimize strong authentication.”

In an interview about IBM Security’s new antifraud solution, Satti Charles discusses:

• How behavioral biometrics differs from traditional biometric solutions;
• Why cognitive fraud detection is not just artificial intelligence;
• Potential use cases for detecting and preventing financial fraud.

Cognitive Fraud Detection

TOM FIELD: Brooke, you’ve just announced some new capabilities, specifically in your Trusteer Pinpoint Detect Solution. Talk to me about some of its innovations.

BROOKE SATTI CHARLES: We’re now incorporating behavioral biometrics, patented analytics and machine learning for real-time cognitive fraud detection. This new behavioral biometric capability leverages cognitive technology that seamlessly analyzes users’ mouse gestures, understanding subtle mouse movements, and delivers actionable risk recommendations. These capabilities help to maximize detection, reduce false positives, and optimize strong authentication.

What Is Behavioral Biometrics?

FIELD: What is behavioral biometrics, and how do you differentiate it from traditional biometrics as well as what people now refer to as behavioral analytics?

SATTI CHARLES: Behavioral biometrics is about what a user does, rather than what a user knows. These capabilities leverage cognitive machine learning to study how users interact with their remote access tools, are designed to bypass these systems. Having behavioral biometrics in place is an additional layer of security, and it helps prevent against continuously evolving threats.

Finding Patterns Through Machine Learning

FIELD: Brooke, you talked about cognitive fraud detection. Is your approach truly cognitive, and how is it distinguished from what we commonly talk about with artificial intelligence?

SATTI CHARLES: Yes, this really is cognitive. This is machine learning that understands patterns of what is normal and abnormal behavior, and algorithms are using machine-learning techniques to continuously create user models automatically. The system learns the user’s normal behavior pattern, ultimately delivering an understanding of current user activity patterns to help better distinguish a fraudster from a trusted user in real time.
Cognitive computing is built on self-learning technology but uses pattern recognition and much more in a way to mimic the way the human brain works. Cognitive computing is part of artificial intelligence applications, so therefore, we say that cognitive leads to artificial intelligence.

Detecting Financial Fraud

FIELD: Let’s get to the good stuff now. How specifically are you using behavioral biometrics to detect financial fraud?

SATTI CHARLES: The new behavioral biometric capability within Trusteer Pinpoint Detect leverages machine learning to study how users interact with their banking website, and as I’ve already said, the system is designed to analyze and understand mouse movements and clicks while creating profiles with each interaction. Basically, the system gets smarter and more accurate over time, and the main goal is to identify the true user versus the fraudster by understanding a true user’s behavior.

In addition, Trusteer uses both cognitive fraud detection capabilities and proprietary threat intelligence to deliver adaptable intelligence to our customers. Trusteer identifies and deploys real-time protection to ongoing new and emerging threats. IBM has a dedicated security research team that is now using the cognitive detection capabilities with an automated malicious pattern recognition tool to help financial institutions identify anomalies and understand and prioritize evolving threats.

The tool allows our researchers to quickly analyze and classify new threats by correlating unstructured data to reveal threat patterns indicative of these malicious activities. It gives researchers actionable insights to help detect new forms of malware, such as zero-day attacks, detection by helping identify new malicious patterns by capturing and analyzing big data.

Using Continuous Analysis

FIELD: Brooke, can this solution be “tricked” either by a fraudster or even by a user?

SATTI CHARLES: We know cybercriminals are dynamic in their attack methods. They continuously adapt, evolve and create new and complex malware strains targeting banks and their customers. The interesting thing about behavioral biometrics is that Pinpoint Detect functionality includes relay capabilities to prevent and detect against attempts on a replay attack. This is because Trusteer Pinpoint Detect performs continuous analysis, not just during the login process, meaning a fraudster using a replay attack would be limited to previously recorded actions while simultaneously raising red flags based on other indicators, such as geolocation.

Additionally, the system is designed to support multiple user behavior patterns within the same account. It’ll take this activity and compare it to every known behavior pattern of a user. The reason this is both pretty cool and important is because it could be an indicator of a joint account where there are in fact multiple users, or it could indicate the same user using their account from a different platform. For example, a mouse connected to a machine or a touchpad connected to a laptop.

Preserving the Customer Experience

FIELD: Brooke, these are all wonderful capabilities, but does the process in any way compromise the customer experience and add that one extra hurdle that makes customers shy away from it?

SATTI CHARLES: No, it will not. The great thing is this is seamless and noninvasive to end users, so it preserves the online customer experience while making it harder for fraudsters to circumvent. Unlike any other authentication process that requires multiple verification steps, behavioral biometrics takes place behind the scenes.

“Behavioral biometrics is about what a user does, rather than what a user knows.”
“This is machine learning that understands patterns of what is normal and abnormal behavior, and algorithms are using machine-learning techniques to continuously create user models automatically.”

**Additional Use Cases**

**FIELD:** It sounds like there’s so much potential here. What do you see as some of the other possible use cases beyond financial fraud?

**SATTI CHARLES:** Behavioral biometrics really can be used to validate who’s accessing any web application, not necessarily just financial. However, since this capability is not available as a standalone within Pinpoint Detect at this time, it’s only used in financial fraud from an IBM standpoint.

**FIELD:** Brooke, I know that these capabilities are new to Trusteer IBM. When and how will this new solution be available broadly to customers?

**SATTI CHARLES:** They will be available this month. We go live with behavioral biometrics for Trusteer Pinpoint Detect this December in 2016. Now, if you’re an existing customer, it’ll be seamlessly rolled out at no additional charge by a system update. However, for new customers to have access to these cognitive detection and behavioral biometrics features, they will have to purchase Pinpoint Detect.

About ISMG

Information Security Media Group (ISMG) is the world’s largest media organization devoted solely to information security and risk management. Each of our 28 media properties provides education, research and news that is specifically tailored to key vertical sectors including banking, healthcare and the public sector; geographies from North America to Southeast Asia; and topics such as data breach prevention, cyber risk assessment and fraud. Our annual global Summit series connects senior security professionals with industry thought leaders to find actionable solutions for pressing cybersecurity challenges.

Contact

(800) 944-0401
sales@ismgcorp.com