CEO CFO

pindrop™ security

Issue:
October 28, 2013

CEOCFO Magazine - The Most Powerful Name In Corporate News and Information

Fraud Prevention for Enterprise Call Centers and Phone Users

Business Services
Security

Pindrop Security
75 5th St. NW
Atlanta, GA 30308
404-721-3767
www.pindropsecurity.com

Vijay Balasubramaniyan
CEO

BIO: Vijay Balasubramaniyan, PhD is the Founder, CEO and CTO of Pindrop Security. Vijay holds patents in VoIP security and scalability and he frequently speaks on phone fraud threats at technical conferences, including CCS and ICDCS. Vijay was recently recognized by the MIT Technology Review in its annual Innovators Under 35 list as an outstanding inventor. Vijay has held various engineering and research roles with Google, Siemens, IBM Research, and Intel. He earned a PhD in Computer Science from Georgia Institute of Technology. His PhD thesis was on telecommunications security.

About Pindrop Security:
Pindrop Security provides solutions to protect enterprise call centers and phone users. Pindrop's solution combines authentication and anti-fraud detection technology to verify legitimate callers while detecting malicious callers. Pindrop's unique Phone Printing™ technology is the first of its kind to analyze and fingerprint individual phone calls, providing the caller's true location and calling device and matching them to Pindrop's CallDNA™ fraud database. Named SC Magazine 2013 Rookie Security Company of the Year, a Gartner "Cool Vendor" in Enterprise Unified Communications and Network Services for 2012 and one of the 10 Most Innovative Companies at the 2012 RSA conference, Pindrop Security's solutions restore enterprises' confidence in the security of phone-based transactions.

Interview conducted by:
Lynn Fosse, Senior Editor
CEOCFO Magazine

CEOCFO: Mr. Balasubramaniyan, what is the concept at Pindrop Security?
Mr. Balasubramaniyan: We stop fraud on the phone or the voice channel. We have phone fingerprinting technology that allows us to uniquely identify any phone device as well as its characteristics, such as type of phone device and location; all of it just from the audio. What this allows us to do is identify whether a call coming into an enterprise is fraudulent or legitimate. This is a big issue to solve. That is because many of these enterprises currently use only knowledge based authentication questions; things like what is your mother's maiden name or what is your social security number. Not only does this not stop fraud, it is also a huge customer satisfaction issue and operational inefficiency issue, where call center agents need to ask all of these questions. Therefore, what Pindrop does is completely streamline the process and makes it very simple for enterprises to identify when a call is coming in is legitimate or fraudulent.

CEOCFO: More specifically, what is it that your technology is measuring?
Mr. Balasubramaniyan: Specifically, we look at about one hundred and forty seven features in the audio of a call, which includes path characteristics, noise characteristics and spectrum characteristics introduced by phone devices as well as the networks that a call is taking. I will give you one specific example. When a call goes over a voice over IP network, that voice over IP network has packet loss. That packet loss manifests itself as tiny breaks in the call audio, which is something that you and I cannot hear. However, with these breaks in the call audio, once we see them not only do we know that the call has gone over a voice over IP network, but the length of the break actually tells us the kind of voice over IP network. Therefore, all of these characteristics essentially identify that device that the call had started from as well as the path that the call has taken.

CEOCFO: Would you give us another layer into understanding what you are detecting that is suspicious?
Mr. Balasubramaniyan: Once we have managed to identify all of these characteristics, we do two big things: one is that we look for anomalies. I will give you an example of an anomaly. Let us say that a phone call comes from phone number 404-385-1234. We have access to the area code databases. That allows us to know that this is supposed to be a landline in

Atlanta. It has never been ported to a different device and it is a completely working telephone number. We then compare that our analysis of the audio characteristics and say, "Why is a landline in Atlanta actually sounding like a Skype phone in Nigeria? There is something very wrong with this call." Therefore, the risk score of that call goes up. We look at a variety of these anomalies and start building out a risk profile for the call. In that specific case, let us consider a call that is supposed to be from New York or Atlanta and shows as being from California. That is something that would be a warning sign; would elevate the risk profile a certain extent. However, for example, if we now got a call from your phone from some really far out region, it would elevate that risk profile even more. It could be that you have actually travelled to that region. However, if at the same time, for example, if with you bank you tried to do a wire transfer of ninety thousand dollars, then that is cause for concern for that financial institution.

CEOCFO: What was the most difficult part of the technology or the offering for you to put together? Where was the challenge?

Mr. Balasubramaniyan: At the end of the day, what we are essentially doing is phone printing and identifying what they characteristics are across the audio spectrum. In order to be able to do this, when we started to research we were doing it on a very small scale. It worked across hundreds or thousands of phones in identifying the type, the geography and the actual phone device, and we were able to scale it across much larger phone populations, and convert that same technology to become a truly effective fraud fighting tool. Currently, our detection rates are well over eighty percent and our false positives are well below two percent. Therefore, making the technology an effective fraud fighting tool. There was a lot of work that went into making it both scalable and robust.

CEOCFO: Would you tell us a little bit about your customer base? Who is using your services?

Mr. Balasubramaniyan: Currently, we have financial institutions using it. We are just moving in to the Telco vertical. However, it is largely financial institutions. We have a couple of the top five financial institution customers. We have one of the top three online brokerages as a customer. Those are some of the customers.

CEOCFO: What is the competitive landscape? Are there many companies specializing in the area?

Mr. Balasubramaniyan: No. Phone fingerprinting or the notion of being able to identify a phone device from the audio and characteristics that come with the call is a technology that we have created and we invented. However, there are people who have come at this problem from different angles. We have folks who have tried to use voice biometrics in order to identify people. For example, let us say a call comes in. The fraud analysts at a particular organization identifies that it is fraud. Then voice biometrics used on any subsequent call can then say, "It is the same voice that called a couple of days back and tried to defraud us." The one thing with a solution such as that one, you first need to identify the fraud source. You need to take that first fraud call and be able to clearly identify that it is the fraudster's voice and create a voiceprint of it. More importantly, you have to make sure that the fraudster never changes his voice, does not use significant amounts of distortion and things like that. Now, with that said, our technology allows you to identify these fraudsters on that very first call. It is not just a black list. On that first call, anomaly detection engines identify these fraudsters. Once we have identified a fraudster we create phone prints for those fraudsters and identify then on subsequent calls. Therefore, our customers find it very easy to operationalize us. They do not have to worry about maintaining any kinds of prints. We automatically enroll these phone prints. We automatically enroll which fraudsters are repeat fraudsters and constantly protect them from even taking that first fraud hit.

"What Pindrop does is bring back trust and protection and security to that phone channel."
- Vijay Balasubramaniyan

CEOCFO: When you speak with potential customers do they understand immediately? Is there an "aha moment" when they believe that you can actually do what you say?

Mr. Balasubramaniyan: Yes, absolutely! The interesting thing is that it largely depends on the kind of customer. One day you could be selling to fraud or the risk group, or the security team of a business unit at a particular organization. In their particular case they have actually listened to many of these fraud calls. They have heard their call center agents saying, "There is some noise here and I cannot hear you very clearly." Once they realized that they could fingerprint the phone device and the part that it plays, that clearly opens their eyes to a variety of new ways to identify the fraud. With call center folks, they have a similar "aha moment". That is because they are the ones who are maintaining the call center infrastructure, so they know if they introduce faulty equipment the quality of that particular call drops significantly. When someone calls us from a cell phone it is less clear than if someone calls us from a landline. Usually there is something outside of the voice that is making that different. We are systematically identifying those characteristics and what we find is that we have a very unique way of identifying these calls.

CEOCFO: Do many of your clients follow through with any legal measures or make attempts to have authorities prosecute or does it just stop with detection?

Mr. Balasubramaniyan: We talked in the last question about if they "get it". One of the big things about whether they get it or not is when they do a proof of concept and they see how well we identified both existing fraud as well as new fraud, that is when the light bulbs completely switch on. Oftentimes, the organization realizes how much of their fraud it had not been observing. It is the classic saying; "You don't know what you do not know." Once we do an assessment

of the calls coming into your call center, you realize that there are so many calls that they have not identified. Therefore, I think the industry is at this point where they first are coming to terms with the problem itself. Prosecution and law enforcement is a logical next step. It will happen once they are more comfortable with the nature of the problem.

CEOCFO: How do you reach potential customers?

Mr. Balasubramaniyan: Since our focus is selling to financial institutions, we have a pretty targeted list. As we expand to these other verticals we are approaching them vertical by vertical. That gives us a very direct way to identify whom we need to talk to.

CEOCFO: Is there one solution or are there some bells and whistles and different aspects that various companies might use?

Mr. Balasubramaniyan: Yes, absolutely! This comes to operationalizing this technology. When you want to use this technology, do you want to use it as soon as someone calls in and it is essentially the portion of the call which is known as the automated part, where you are talking to what is known as an IVR, or an Interactive Voice Response Unit, where you are punching all of these numbers. They will ask you what is your date of birth and you punch that in. It will ask you what your social security number is and then once you punch that in they say, "Now let us transfer you to a call center agent." Therefore, you can essentially deploy that technology on the input side at the IVR, at the call center agents themselves or even after the fact with unrecorded calls. Therefore, you can analyze calls after they have come through and been recorded and do some more offline analysis of the fraud that you are seeing. In some organizations the "after the fact" analysis is very useful, because of many of their important transactions have a time window where they can explore many of these questions. Again, how you present this information based on whether you analyze in real time or after the factor who consumes that information, falls into the bells and whistles. Do you send that information in to a call center agent? And if you are sending to that call center agent, how do you make sure that the call center agent does not reveal important things about the call. You do not want call center agents to tell the fraudster what your Pindrop score is. Therefore, we will adjust so that we change the way that they have that information. Then you also have some of the really large organizations; they have their own fraud fighting call center agent unit, who will handle the caller directly, once we have established that the call is risky. Then finally, in the offline case, you have the fraud analysts who are handling the calls directly. In that case, you are presenting them that information so that they can work these cues as and when calls come in. Very few of these calls get through because they have some fraudulent characteristics and then the fraud analysts can go take a look. In some of the larger financial institutions they do a combination of this. Then we also have cases where we have integrated with their own third party risk management software. All of this forms the bells and whistles.

CEOCFO: Commercialization and development are typically quite expensive. Would you tell me a little bit about how you are funded as you move forward?

Mr. Balasubramaniyan: We have been well funded. We started off with a National Science Foundation Small Business Innovation Research Grant. That is how much of this technology was developed. We started commercializing this, which was really good. At the point in time we were translating from research to production, we received a seed round of about a million dollars. Then in June of 2013 we took in a Series A for about eleven million dollars from Andreessen Horowitz, Citi Ventures, Redpoint and Felicis. That has allowed us not only to expand across verticals; it has also allowed us to expand across geographies.

CEOCFO: It seems clear that people understand the concept and the value!

Mr. Balasubramaniyan: Absolutely! Not only does the technology work really well, but we have customers who have deployed and have been watching the technology in action for quite a while. We achieve return on investment very, very quickly, so that makes it particularly attractive.

CEOCFO: What makes Pindrop Security stand out for investors and people in the business community?

Mr. Balasubramaniyan: If you look at the history of security, you start off with physical security where people would walk into these enterprises with guns and walk out with bags of money. Then, security changed into the online world where people would hack into websites, hack into your accounts and manage to steal money. Therefore, there were many companies that were built to try and protect enterprises from that. That has left the phone channel or the voice channel as the most vulnerable and the weakest link for many of these organizations. Pretty much, most organizations use the phone channel to be a data communication tool with their customers. Now that that has become the weakest link these fraudsters are going after that link. What Pindrop does is bring back trust and protection and security to that phone channel.

Pindrop Security
75 5th St. NW
Atlanta, GA 30308
404-721-3767
www.pindropsecurity.com