Mavenir and the Role of Machine Learning

Deep Fraud Investigations: Mavenir and the Role of Machine Learning in IRSF Control

Black Swan Telecom Journal recently visited with Mavenir's Ilia Abramov, GM, Security Business Unit and Marie Casey, Senior Product Manager, to discuss the virtues of Machine Learning-based fraud protection and some unusual and interesting fraud schemes Mavenir has uncovered.

Are we ready to fight fraud when these advanced services are widely deployed?

Consider International Revenue Share Fraud (IRSF), the highly successful criminal framework that enables dozens of fraud schemes from wireline calls to mobile roaming. Up to now, telecoms have controlled IRSF using rules engines that leverage historical data, number ranges, IPRN lists, and calling behavior profiles. That's great. But will that approach protect us in the years ahead?

"Not likely." That's the opinion of Richardson, Texas-based Mavenir, a company that's fully committed to Machine Learning as the way to protect next-gen networks and services.

OK, so who is Mavenir and why does their opinion count? Honestly, six months ago I had not yet heard of the company. But I've since learned they are a 2,500 employee firm who competes directly with the big mobile Network Equipment Providers (NEPs): Ericsson, Nokia, and Huawei.

Turns out Mavenir is an un-NEP. Yes, it's definitely in the NEP business, but it sells no equipment. Mavenir is a pure software firm that builds both Core Networks (VoLTE, IMS, etc.) and Access Networks (5G Core, RAN, etc.). In recent years it's also expanded into Special Services, in places like IoT, and UCaaS. Today, it's also teamed with Syniverse to compete with Samsung and Google in the hot new RCS Business Messaging space.

Joining us to discuss the virtues of Machine Learning-based fraud protection is Ilia Abramov, VP and General Manager of the Security Business Unit at Mavenir, as well as Senior Product Manager, Marie Casey. Together, they point to some unusual and interesting fraud schemes their deep investigations at Mavenir have uncovered.

Dan Baker, Editor, Black Swan: Ilia, to begin, can you give us a quick overview of your fraud control business? Several solution vendors offer protection from IRSF fraud. How do you differ?

Ilia Abramov: Dan, we are leveraging our deep multi-domain knowledge in telecom networks to solve fraud and security problems — which we see as two sides of the same coin. What makes us unique, I think, is our ability to natively integrate fraud and security control into our network fabrics.

One of the key issues, of course, is dealing with legacy systems when we want to implement forward-looking capability in the network. Our network portfolio covers signaling and security for 2G, 3G, 4G, and now going to 5G.

The whole system we use for fraud detection is based on real-time machine learning. Real-time is critical because it does no good to run analytics only to find you lost $20,000 yesterday on IRSF calls.

As far as use cases go, the data-side fraud control we sell as a service to our customers is quite popular and achieving great results. And since we are rolling out an RCS Business Messaging (RBM) solution, we are keen on making sure the RBM channel is clean of fraud and security issues.

What difference does it make to have the fraud solution native to the operator’s network?

Whenever you look at the core networks, whether it’s IMS core, an SS7 network or a Diameter network, these networks are not designed to add central elements in the architecture to perform special filtering or detection.

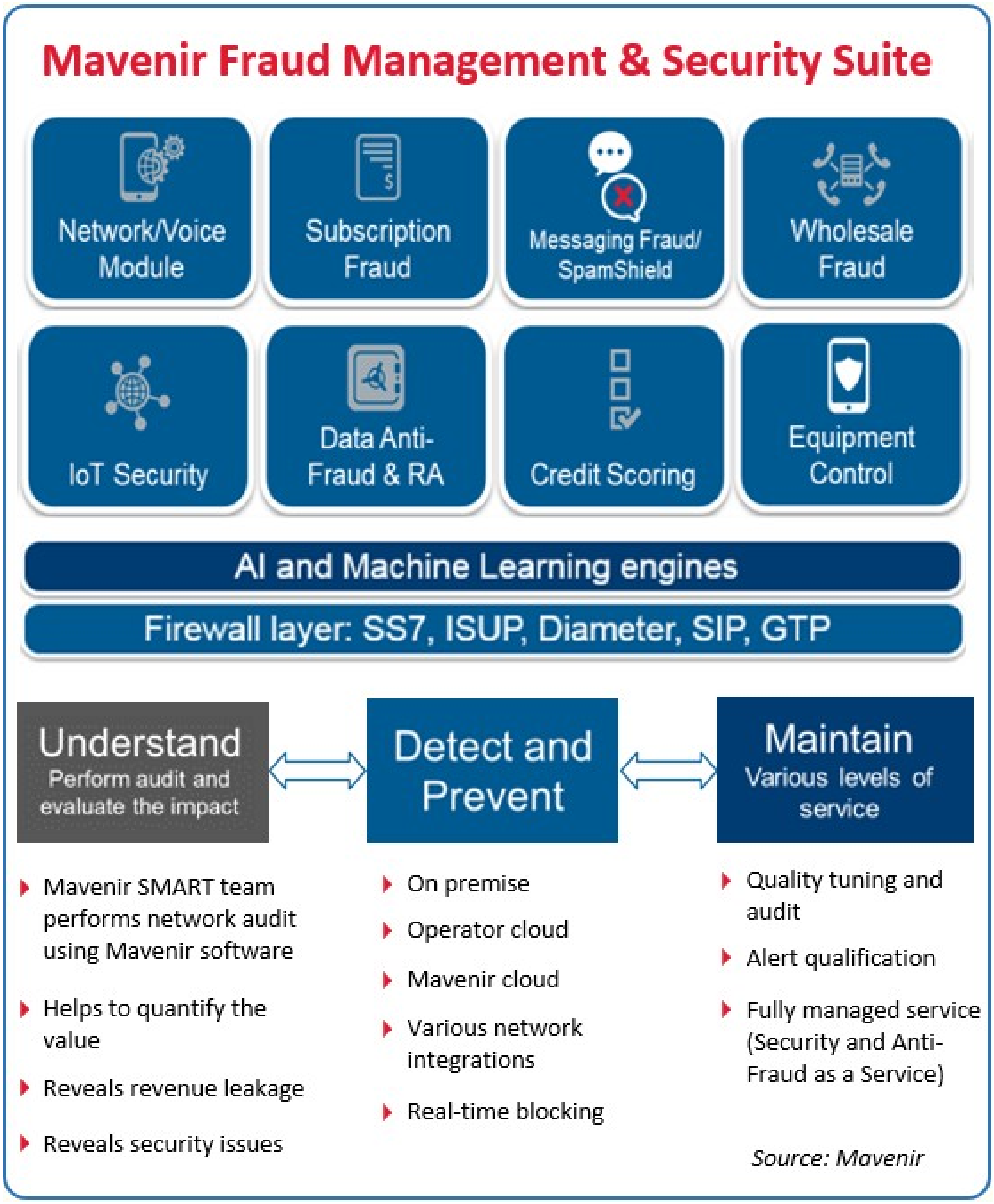
If you look at the 3GPP-defined elements like the Interconnect SBC (ISBC) or Access SBC (ASBC), the fraudsters are well aware of those standards, so they look for vulnerable network elements at an operator where industry standards are not fully supported.

A Tier 1 operator network in the U.S. would have multiple regions and data centers. So to control such a network, you have to insert additional hardware or more router machines into each and every data center to cover fraud and security.

But using native integration, Mavenir enables an operator to protect themselves from fraud while also saving them capex and opex.

Now that’s our preferred approach, however, some operators do prefer to have a dedicated element that allows them to implement some kind of policy control or integrate other learning engines or apps.

But we support all integration religions: whatever approach the customer desires, our team can deliver it, and we can also help them choose the best integration scenario.



Mavenir Fraud Management & Security Suite

Understand
Perform audit and evaluate the impact

- Mavenir SMART team performs network audit using Mavenir software
- Helps to quantify the value
- Reveals revenue leakage
- Reveals security issues

Detect and Prevent

- On premise
- Operator cloud
- Mavenir cloud
- Various network integrations
- Real-time blocking

Maintain
Various levels of service

- Quality tuning and audit
- Alert qualification
- Fully managed service (Security and Anti-Fraud as a Service)

Source: Mavenir

There are some excellent, widely-available databases on the market that help identify IRSF fraud. Does your machine learning system take advantage of that intelligence?

In a machine learning system, you can drop in blacklist numbers anytime, but that’s merely a starting point for the system and the number would never appear in real-life anymore.

Our practice shows that real-time machine learning is very efficient in detecting IRSF scenarios. And when we find a valuable database that bounces against a rules engine, what we can do is put that rules engine on top of the machine learning.

Now I realize at first glance that shifting away from proven blacklist databases toward more machine learning doesn't seem wise. But where Machine Learning adds value is it allows you to add more nuance and detail to the decision-making around fraud. Machine Learning is a better way of balancing fraud intelligence from many sources, not just blacklists.

Take a company like Syniverse, who is a major player in the telecom fraud control business as well.

For a company the size of Syniverse, the fraud control business is a relatively small revenue contributor. After all, they operate the largest IPX platform in the world connecting hundreds of mobile operators. They are also telecom's largest global roaming clearinghouse and are a major A2P aggregator.

So Syniverse is exceedingly rich in fraud intelligence, especially on the roaming and international mobile side. But unfortunately, it's hard for them to fully exploit that intelligence because using it might expose the private information of customers — somebody's privacy is violated.

But imagine if Syniverse hooked into Mavenir's machine learning system. Well, when you do that, you totally anonymize the intelligence and can create an in-network service for detecting and stopping fraud. In that scenario, there would be no privacy issue of any kind.

Let's talk about IRSF in the roaming channel. We know that's a complex area in voice traffic where fraudsters like to hide. What is Mavenir doing there?

Marie Casey: Dan, it's very true. When an IRSF fraud call happens through roaming, it has a much better chance of getting through because roaming confuses the billing picture and introduce delays. Now, as you know, the GSMA standard NRTRDE (Near Real Time Roaming Data Exchange) requires operators to get back the roaming files to the originating operator within four (4) hours.

Trouble is the network where the customer roams very often can't meet that 4 hour SLA. Rating may get delayed for many reasons. In fact, our investigations reveal that operators around the globe are often dramatically out of SLA on getting their NRTRDE feeds.

So Mavenir has figured out how to ingest roaming intelligence in real-time: as soon as the call passes to the visiting network, we capture the details.

Now there's an interesting clause in the GSMA's standard roaming agreement which basically states: "If an IRSF fraud is committed while roaming and the operator doesn't get his NRTRDE files within four hours, then the visiting network operator is responsible for absorbing the fraud loss."

OK, so here's a potential way to put the burden of paying for a fraud loss on the visiting network operator. That's great, except for one thing: verification. How does the home operator know the exact time when the visiting operator took the roaming call and ended it? Better yet, how do you prove the delay was real?

Well, that's precisely what Mavenir has figured out. By developing a method of quickly analyzing the discrepancies in huge volumes of TD35 files, we've made it quite easy for the operator to record these roaming call events and get the instant proof to say, "Hey, you sent these files to us too late, so any IRSF fraud losses you are responsible to pay on this call."

Great, so you've put some pressure on delivering NRTRDE files on time.

Marie Casey: When you explore the network roaming process as deeply as we have, you start to notice lots of unexpected things.

For example, looking simply through the TD35 roaming records for one of our customers, we identified thousands of roaming "customers" who weren't even authorized to be there. In fact, they were not really active on the home network they were supposed to be coming from.

After these guys were deactivated, we discovered the fake customers didn't even have credit balances in their phones and should not have been able to receive any access at all.

So it's another case proving the value of machine learning. By our ability to look at the roaming process in a different way, we arrived at results much faster.

Machine learning can identify when something shouldn't be happening. It knows: "Something strange is going on." In fact, we often discover these cases by comparing the records of two systems in parallel.

Ilia Abramov: Let me build a bit on Marie's point about the interesting things Machine Learning discovers.

It's often the case where a mobile operator has multiple interconnect options. It could be through iBasis, BICS, Telefonica, or hundreds of other interconnect partners.

But knowing what kind of fraud protection an interconnect player has makes a big difference to the fraudster. Maybe they are aware that a certain route is protected by Syniverse's anti-fraud service, so the fraudster decides to avoid that route.

In short, there are often very good reasons why fraudsters roam to a very specific country or geography rather than choose a more natural path. The fraudsters may be trying to exploit intelligence on very specific interconnect routes. And that deeper intelligence could be supplied, say, by a dishonest employee bribed by or working for the fraudster.

Certainly, most IRSF protection systems are designed to block calls based on a blacklist or by identifying suspicious behavioral patterns from a caller's point of view. Looking at things from the fraudster's point of view is another fruitful path for analysis.

When you come right down to it, simple detection or correlation mechanisms don't work when call routing, handoffs, and partner accounting get too complex.

This is why I think behavioral analysis is really the best solution. A good behavior analysis will look at many facets of a telecom event: the data channel, the voice channel and all the destinations and sources.

And once again, the biggest challenge is often: how do you detect strange events and fraud without breaking privacy? Well, the behavioral analysis gives us a way to maintain that privacy.

It is not that we are going to block a specific user. Indeed, maybe the user is a business traveler and you'd rather not stop their communication.

The key is to build up enough evidence from millions of cases so a mobile operator can approach its roaming partner (or wholesaler) and start the discussion about what should be done given what the behavioral analysis indicates, not what one particular person did.

We've discussed the fraud side of Mavenir's mission. What's hot on the security side of your practice?

Dan, maybe our most popular security solution is in a category we call "network security analytics". As you're probably aware, the U.S. government and operators in America are concerned that certain equipment vendors, such as Huawei and ZTE, may be using signaling channels to communicate back to their own data centers where private, commercial, or national security information could be compromised.

What Mavenir does is create a behavioral profile of each network element, a profile specifically related to data being sent out through various signaling channels. So this is our way of detecting anomalies.

For example, if a network element claims to be an MSC or P Gateway or S Gateway, then all-of-a-sudden starts sending all its information outside of the network via signaling, then we can block that communication and raise an alert. The issue here is that signaling might be a way to bypass normal IP data protected by firewalls and private networking protocols.

So this case is being driven by geo-politics and national security, but it's nonetheless an interesting twist: doing machine learning and behavioral monitoring of elements in core networks.

By the look of things, the complexity of 5G and IoT deployments will be another opportunity to apply machine learning.

I think the principle security challenge of 5G and IoT will be verifying identity. Experts are already showing how 5G radio technology is vulnerable to IMSI harvesting.

By combining the IMSI mobile ID with your mobile phone number, a fraudster can place a call, intercept call and messages, and snoop on data communications too.

So by placing a small radio unit somewhere, say in the center of New York City, a fraudster can intercept voice calls, regardless of whose network they are on.

However, if we block the unauthorized usage of that identifier, then I think we can provide sufficient security to the mobile networks. That's the concept.

Well, it certainly sounds like a high-tech version of SIM box bypass — another way of exploiting the RAN for criminal purposes. Thank you, Ilia and Marie. Your insightful case studies show the power of machine learning in the fraud fight. I foresee a great need for the kind of deeper fraud investigations you specialize in.

Mavenir offers the industry's most advanced Network Security and Fraud Management Suite, a unique platform built with AI/Machine Learning & Big Data Analytics providing Real-Time Network Protection and Fraud Prevention. Learn more