MAVENIR BLOG POST

Spotlight on Security and Fraud Challenges for Mobile Operators

Spotlight on Security and Fraud Challenges for Mobile Operators

Jon Arnold, Principal of J Arnold & Associates, recently spoke with Ilia Abramov and Marie Casey of Mavenir about the security and fraud challenges mobile operators are facing today. In the interview below, Ilia and Marie share how operators can protect revenue utilizing AI/Machine Learning & Big Data Analytics providing Real-Time Network Protection and Fraud Prevention.

Jon Arnold (JA): As a means of introduction, please say a bit about Mavenir. Having attended your last two analyst events, I know the story, but the company is not a household name, although it probably should be for anyone investing in wireless technology.

Marie Casey (MC): Mavenir is the telecommunication industry's only end-to-end, cloud-native network software provider, redefining network economics for communications service providers (CSPs).

Mavenir is focused on accelerating software network transformation and redefining network economics for CSPs by offering a comprehensive portfolio across every layer of the network infrastructure stack. From 5G application/service layers to packet core and RAN, Mavenir leads the way in evolved, cloud-native networking solutions, enabling innovative and secure experiences for end-users. Mavenir enables CSPs to compete more effectively with innovative cost reduction, revenue generation, and revenue protection solutions.

Following a history of mergers and acquisitions that combined elements of Comverse, Acision, Xura, Ranzure Networks, and Mitel Mobility, Mavenir was relaunched at the 2017 Mobile World Congress Barcelona. Since then, Mavenir has been on an aggressive path for innovation, including the acquisitions of Brocade's vEPC in 2017, Aquto Sponsored Data Platform and Argyle Data Security Analytics in 2018.

Ilia Abromov (IA): Mavenir's Fraud and Security portfolio is a full end-to-end solution for mobile networks. While traditional anti-fraud and security players have to focus on an "add-on" approach and try to address specific issues, Mavenir has the capabilities to embed our solutions right into the network elements. This is aligned with 5G principles that are trying to follow Security by Design principle.

JA: Building on this, Marie, your role may seem unusual for a company like this, but it's actually quite important. Briefly describe it, along with the backstory, since you came into this via Mavenir's acquisition of Argyle Data.

MC: I joined Mavenir as part of the Argyle Data acquisition in 2018, where I worked as a Fraud Specialist. Argyle began as a small, VC-backed, Silicon Valley startup, primarily focused on real-time fraud detection using machine learning (ML) technology across MNOs, MVNOs, and wholesalers, which was a pretty novel concept as we started introducing the idea to CSPs. Typically, in telecoms, fraud detection is managed through a series of manual reports and threshold-based alerts, where a level of false positive is simply accepted.

This is where Argyle saw the opportunity to change the game entirely and introduced the idea of ML technology to identify when something unusual was happening on an Operator's network. Based on the concept that all 'unusual activity' is fraud, and when viewed as anomalous, it can be detected. The concept worked, and this approach allowed us to identify new types of fraud that were taking advantage of loopholes Operators didn't know they had.

Also, it did this in real-time, which dramatically increased detection time in comparison to side-by-side traditional systems that often missed attacks due to activity levels hiding just under the threshold limit of the latest high-usage report. The Argyle solution fitted nicely to complete Mavenir's end-to-end fraud and security offering, while also enabling Argyle's ML concepts to be shared across all their fraud and security products.

JA: The fact that Mavenir made that acquisition says a lot about how important security protection and fraud detection and prevention have become. How are you seeing this space evolving, not just for carriers as they move to 5G, but also for their enterprise customers who depend on wireless communication and also need business-grade security?

MC: Mavenir's decision to strive in the direction of both ML and fraud detection says a lot to its value. Especially with regard to 5G, CSPs need to be prepared for the 'unknown' nature of what the risks may be. 5G brings us to a place of new security and fraud issues, where ML is truly the optimum approach to be prepared.

Recent evolution in the market reflects some of the newest areas within our Fraud and Security Suite, including 5G security, robocalling (with STIR/Shaken support), data fraud, and IoT. These are the big 'hot topics' with our customers, as they have moved beyond basic fraud and security topics.

IA: All 5G principles underline the importance of data not only for anti-fraud and security use-cases but also for the core network and radio network management. For example, Network Data Analytics Function (NWDAF) is not only meant to serve as a reporting capability embedded into the core network, but also to become a control point 'artificial brain', orchestrating the functioning of 5G networks.

Our products have evolved to utilize all market achievements we have so far. For instance, our NWDAF product is leveraging our ML developments in security and anti-fraud area and applying them to 5G requirements. Real-time capabilities also distinguish our approach and have become a key focus of mobile operators when deploying 5G networks.

JA: Let's talk further about the problem set, and then we'll move on the solutions. During your presentation at Mavenir's analyst event, you spoke about providing a bridge between the threats and risks related to security and fraud. When VoIP came along, the PBX became a new point of entry into wireline networks for these risks, and that persists to this day. Enterprises still struggle to address this for a variety of reasons – what's needed to change that?

MC: Fraud and security are often thought of as one category, but in reality, fraud teams and security teams are often split across different departments with no common systems.   Mavenir has introduced to CSPs the opportunity to change that, by leveraging our modular approach across our fraud and security suite module, enhanced with our real-time ML learning detection. This provides one system with common interfaces and on the most basic level allows insights from the same data feed to be reused in multiple ways across teams for various purposes.

PBX hacking/VoIP traffic is a terrific example to show the benefits of merging these worlds. It's hard to believe, but to this day, many hacked PBX cases are still due to PBX passwords being things like 1234, showing the clear risk when security is not embedded from the beginning. I remember one specific case where an enterprise's PBX was hacked for exactly this reason, and after the Operator warned that they needed to change their PBX password, they weren't even aware they had a PBX or what a PBX was. Clearly a catch 22 kind of situation!

Now, you might think it's logical for enterprises to simply have better passwords on their devices. It's also more than reasonable to say the device should have been enabled with minimum password standards by the manufacturer to begin with. It would also be a normal expectation to trust that their Operator will protect them against fraud.

The issue most Operators face with providing this is that the traditional threshold-based alarms they are using for detecting fraud simply isn't equipped to handle this level of sophistication, such as when a subscriber's phone is stolen while roaming, an IMEI change occurs, and calls are generated to the same number that the hacked PBX is heavily calling that same day. This is exactly the spot where real-time ML really shines.

In today's world, both personal and enterprise customers should expect this level of service and not just hope that security is embedded in their device. ML is how Operators gain the opportunity to protect their customers in this fashion and to really stand out from the crowd of their competitors with the added benefit of better protecting their own revenue.

JA: With LTE and the coming of 5G, wireless networks are poised to play a much bigger role in the enterprise. To provide a bridge here, enterprises must first understand the threats. In what ways are they different from what wireline networks must contend with? Building on that, what the prime risks that IT decision-makers need to be aware of?

IA: 5G follows the paradigm of Security by Design, which is the driver for enterprises to start using this technology. Current technologies have made a number of concessions on security measures in favor of performance, hardware footprint, etc, leading to a number of new threats specifically coming from the convergence of wireless and wireline networks. A typical example here is the robocalling problem faced in North America.

Currently, the entry point for robocalls is primarily wireline networks, and this has an explicit impact on enterprises. The industry has realized the threat and is actively working on solutions against it, like STIR/SHAKEN, dedicated analytical solutions, etc. 5G protocols will assume better protection for the subscriber identities, more transparent partner identification, encryption of sensitive information, all the while making 5G networks far more secure then traditional wireline networks.

In terms of what risks enterprises should be thinking of, these would primarily depend on the end-to-end use cases required. While IoT is named as one of the main use cases for 5G, it is also one of the biggest threats. The problem that we see there is beyond 5G technology, but rather on the application layer. As IoT devices and business logic around them might have poor implementations, that would impose threats for businesses and 5G networks (for example, in the form of overload of DDoS attacks). Therefore, the concept of supply chain security is something that goes beyond telco providers all the way to the enterprises building their service on top of new technologies.

JA: For carriers, fraud translates into revenue losses, so the business case for a solution has a solid basis. Can you speak to the order of magnitude you're seeing, as well as the trends? Then, going downstream to enterprise customers, how are carriers pitching a similar business case to them?

MC: There are definitely scary numbers for CSPs to hear. Global reports indicate annual losses of $6B to revenue share fraud, $4.5-6B to messaging fraud, and $2.3B to subscription fraud to name a few.

Where single small fraud events may be in the hundreds of dollars, some of the cases we've encountered with Operators reached the tens of thousands of dollars from a single SIM card. There are also non-tangible losses to Operators when fraud happens; customer brand is affected when large scale 'missed call fraud' (or 'wingari' fraud, as it's officially known as) occurs, where you get an innocent missed call or 'call me back' SMS, and, of course, when you do, nothing but silence. By the time your next bill rolls around, you're going to see that sky-high charge for the single call, and you're naturally going to think it's somehow your Operator's fault.

For enterprise customers, an area we are currently investing in is credit scoring. This offers telco subscribers to receive a real-time credit score that can be accepted by banks and other institutions as proof of credit worthiness, based on prior spending and payment patterns. This is another example of how we are trying to bridge the gap between worlds that can benefit from each others' insights and data.

JA: To explore this further, Mavenir's Security and Fraud Management Suite is quite comprehensive. Can you highlight the key elements, along with the overall thinking behind this group of offerings?

MC: Mavenir's Fraud and Security Suite offers a 360 approach to fraud and security. The modules range from: network usage voice fraud, subscription fraud at connection time, data fraud, roaming fraud, wholesale fraud, anti-spam and A2P revenue assurance, robocall detection, and prevention, all the way to an EIR.

All our fraud and security suite products are modular to enable easy scaling and share the same common architecture. All modules are supported with dedicated real-time ML algorithms tuned to specific data types on a specific Operator's network. All modules are also enabled to leverage our own Signaling Firewall as a network integration point, as well as automatic blocking actions for detected cases.

In spite of this extensive list of 'known' fraud and security risks our modules address, one of the most common events we identify to date with our ML approach is 'unknown' fraud and security issues, most often allowing Operators to identify blind spots they weren't aware of.

JA: The secret sauce here seems to be Mavenir's use of artificial intelligence (AI) and ML in particular. AI is everywhere these days, and, while not normally associated with network infrastructure, it clearly has a role to play. Can you briefly explain this, provide some examples of ML applications, and illustrate the benefits of these applications, both for carriers in their networks and for their enterprise customers?

MC: A good way to imagine it is that ML is looking for anomalies or something out of the norm that's happening on your network, with your unique patterns in mind. Unique is important here, as, even in the same country, some Operators will be pre-pay orientated, others post-pay, so this unique aspect is key. ML is also not magic. Domain expertise and long hours of experience across different data types are necessary to know what it should be looking for.

This deep knowledge combined with ML is especially true regarding 5G. It's key to keep an open mind on what risks might be out there, but simply throwing an algorithm at the problem won't help. Quite simply, there's an amazing amount of noise that happens on all networks you're not expecting, and you need to rely on experience to sort it all out. Working across a multi-region landscape is how we achieve this, ranging from MNOs, MVNOs to wholesalers.

IA: It is also the case that we use ML beyond anti-fraud, and it's very useful for network security scenarios as well. The challenge most operators face today is that they do not have proper visibility into the functioning of their core networks, especially when adding interconnect complexity into the equation. This approach enables ML technology to complement our firewall offering by providing insight into the signaling elements and helping to prevent signaling attacks or fraud attempts.

JA: We're still in early days with AI, and there's a lot more innovation coming that will bring new value to your customers. During your talk, you mentioned a few examples, such as deep learning, blockchain, and security as a service. Could you provide a brief glimpse for what some of this might look like?

IA: R&D for AI and ML algorithms has increased 70-fold from the last century. The specifics of telecoms are a requirement for real-time prediction. This is quite different from earlier use cases for photo-matching or information filtering. Current latencies achievable in production environments are now less than 10ms to provide a verdict on an event. When looking at radio optimization use cases and 5G orchestration use cases, 10ms is actually too slow, so more research is needed here.

Another focus area is accuracy improvement. The majority of operators are focusing on lowering their OPEX, and, therefore, they cannot accept high levels of false positives. At the same time, they are looking to maximize their revenue saving or quality of attack detection. Therefore, smart combinations of some bespoke ML algorithms with proprietary telecom specific algorithms we built in-house provide good results in this area.

Blockchain technology is currently under-utilized in telecoms. However, problems like caller ID spoofing require worldwide solutions. This is an area where blockchain can be used more efficiently instead of centralized certificate management concepts.

JA: To wrap up, I'm sure you'd agree that data security and fraud remain poorly understood, and IT has been more reactive than proactive when threats occur. For that to change, what course of action needs to happen, and how does IT's thinking need to change?

MC: That change in thinking is exactly what we're hoping to help bring more Operators to. Within Operators, on one hand, you have base management teams eager to grow customer bases by X, and on the other, fraud teams are going to be right there refusing service to many for good reasons but understood only by them. This issue truly shows poor internal understanding even with CSPs, and because fraud and security domains are usually incredibly specialized, it often means that exact same base management team doesn't realize they are holding back growth in the long term.

That 'lack' of domain expertise is exactly what Mavenir seeks to help with. With our footprint across such a wide variety of network solutions across MNOs, MVNOS, and wholesalers, our customers get the chance to hear this story first-hand and benefit from the advice on what we know works, all the way from exec-level relationships, to working 1-on-1 with analysts to help them explore the newest anomaly we've identified.

See how Mavenir's Network Security and Fraud Management Suite is built with big data analytics and advanced AI techniques such as machine learning and deep learning to provide real-time network protection and fraud prevention. Learn more