In our highly networked world, passive sensors are everywhere. And once the Internet of Things takes off, the number of sensors will probably multiply a hundred fold.

But in the area of fraud detection, we are beginning to see the limits of pure passive signature analysis. While the CDR analysis in Fraud Management Systems (FMS) is great for detecting IRSF and other frauds, it’s relatively weak at false answer supervision fraud and advanced SIM Box bypass. Why? Well, the fraudsters have gotten better at flying below the statistical bell curves.

This is precisely why active probing and testing of very specific interconnection routes, such as those with a bad history — has proven to be such an invaluable aid in locating and blocking SIM boxes that an FMS may take hours to detect.

But Kenneth Mouton, Fraud Business Unit Manager at SIGOS has a better idea. He asks: “Why not combine the virtues of FMS CDR analysis and test call generators to create a single integrated tool?” In that way, he reasons, maybe the anti-fraud solution's value would increase, as in $1 + 1 = 3$.

Well, Kenneth is here to give us some background on that intriguing idea. What’s more, he provides a nice tutorial on the use of test calls in the SIM box fight and explains an altogether new threat: OTT bypass through mobile services such as VIBER.

**Dan Baker:** Kenneth, the origins of your anti-SIM box fraud business at SIGOS are interesting. Can you explain a bit of your company's history?

**Kenneth Mouton:** Dan, for 8 years I worked for Meucci Solutions, a test call generation firm, who was acquired by SIGOS in early 2014. Now Meucci focused in SIM Box fraud detection, serving 85 customers in that space. Meanwhile, SIGOS is a much larger test call generation firm providing mostly

---

**Related Stories**

- **A Sweeping 239-Page Research Report on Fraud Management Solutions & Strategies** — by Dan Baker
  — TRI has released a comprehensive analyst report on fraud management solutions. The study is based on interviews with three dozen leading FM consultants and solution experts. Download the free Executive Summary.

- **SMS Bypass Blocking: A Service that Protects & Maximizes A2P Revenue for Mobile Operators** — interview with Claire Cassar — A2P messaging is a multi-billion dollar revenue stream that mobile operators need to protect. In this interview, you’ll learn how a managed service solution blocks bulk marketing messages and other bypass fraud in enterprise-to-operator SMS traffic.

- **Device Intelligence and Big Data Linkage: Guarding Consumer Access Points from the Fraudsters**

---

quality of service and roaming testing for about 400 mobile operators worldwide.

Bottom line, this merger turns out to be a remarkable fit. In fact, when you add the anti-SIM box customers SIGOS had, we now serve about 120 operators worldwide there. But best of all, the fraud team can now tap into the R&D resources of SIGOS, who has no less than 50 people doing product research.

Being involved in the fight to stop SIM Box fraud for so many years, I’m curious to hear your assessment of the damage this fraud causes operators around the world.

Well, the biggest concern, of course, is lost revenue. The CFCA recently estimated the annual global revenue loss was about $2 billion.

Yet SIM box fraud also creates a lot of quality issues. People experience more delay, echoes, and noise on the line. And these quality issues, in turn, cause people to make shorter duration calls.

More dropped calls are experienced, too, because the prepaid balance often runs out on the SIM card. And because the telephone number is not visible on the phone, you’re not sure who is sending you a call.

A typical SIM Box has 32 modems and antennas and makes calls continuously, so it also causes congestion problems, prompting the operator to invest in new antennas and cell towers in the region.

Ten years ago in the UK, the market was flooded with SIM boxes and we helped eradicate the problem there. All of the major UK operators were customers of ours, and when the SIM boxes were stopped, many of them admitted to us that they now had pockets of massive over-capacity in their networks.

So when you add it all up, SIM box fraud causes a lot more damage than you would normally suppose.

How do test calls do their work in stopping bypass fraud? And how do you differentiate your solution from what your test call competitors offer?

Certainly one of the biggest advantages of test calls is their speed. SIM boxes can be profitable very fast. Within 60 minutes or less they are making a profit. So even if your FMS finds thousands of SIM boxes after three hours, that detection effort has little effect because the fraudsters will just replace the SIM cards.

However, test calls give you the ability to find the SIM boxes very fast and with 100% certainty, so you can deactivate them automatically.

The real secret of our success in SIM box detection is our network: we have the largest network of test call equipment in the world. In fact, we have a presence in every country with the exception of the five on the US embargo list.

Sometimes when you detect SIM boxes, it’s very local. For example, SIM box fraud in Bolivia is mostly coming from Peru. So it’s key to be able to make calls from Peru: global flexibility and resources can make a big difference.
Now when I say test call “network”, I'm also referring to our non-automated network of people on the street. Let me explain.

Mobile-to-mobile calling is mostly good quality. Where the fraud is usually found is on the low quality routes, and that's why we specialize in testing those low quality routes.

In countries like the United States where you have a high population of immigrant people, a lot of those folks want to call home to their relatives and friends. But to save money, they don't call using a mobile or fixed line. They generally use cheap calling cards or “scratch cards” as they are called. You find them sold everywhere — in vending machines, supermarkets, and convenience stores.

Those calling cards are a key source of bypass. And how can these cards be sold at budget prices with lots of minutes? It's because behind it all are cheap and fraudulent routing: the calling cards are connected to carriers who use SIM boxes to terminate their traffic.

In fact, we have people in certain countries who do nothing else but buy calling cards on the street to bring back so we can run test calls through. So a wide logistics chain is required for finding fraudulent routes. And if you want an effective program to detect SIM box fraud, it's essential to have that network of people.

One of the challenges of using test calls is they are an active detection mechanism. So how do you prevent the fraudsters from detecting you?

Yes, these days, we have to be very careful to use our test equipment wisely. And to be honest, we used to do things like make hundreds or thousands of calls all over the world with just one SIM card. But that pattern is very suspicious call behavior.

So in the last 10 years we have invested in counter-measures to avoid being detected. So when we make test calls today we never do a test call with the same telephone number. And we make sure our calls are made using random durations. You also have to make sure the calls don't start exactly on the minute. There are many, many techniques, and of course, most of them are confidential.

Now we also have the means to determine if we are in fact detected. For example, we use a shadow network that involves using different SIM cards and we compare results. So this really is a cat and mouse game.
The fraudsters continue to improve their game. In fact, as they step up their attacks using the latest SIM server technology, it looks like SIM box fraud has become more formidable to detect than ever.

Dan, while we firmly believe test call generation is still the most mature method of detecting SIM box bypass, we also feel you need a cocktail of medicines to cure your disease: one medicine is not enough.

For example, an operator should be able to extrapolate from our test call results with their FMS system or their own CDR profiling. We advise them to take the data we provide them on the SIMs we detect and find similar SIM cards with the same behaviors or those calling from the same antenna.

But unfortunately, many operators don’t execute on our advice or execute on it poorly — for various reasons. Maybe the operator only has 3 or 4 people trained in SIM box fraud, and they have many other fraud types they are concerned about.

So companies like FraudBuster and Mobius saw a market need to deliver dedicated CDR profiling for SIM box detection. And we also saw that need and have invested heavily in it and are just rolling out such a solution.

This is very exciting for us because we are now the first solution company combining CDR profiling and test calls. And the solution is fully integrated. The same person doing the test calls is doing the CDR profiling. We also incorporate a shared service center so our customers get the benefit of sharing intelligence with each other.

In a recent trial of the solution, we increased an operator’s traffic by 40%. So we created millions of additional Euros in revenue for them each month.

Scanning your website, I noticed you have a solution for a kind of bypass I was not familiar with: OTT bypass. What’s that all about?

OTT bypass is a brand new kind of bypass that requires no SIM boxes at all. Basically the fraudulent interconnect carriers are terminating on mobile phones that have VIBER, an application like Skype that has a large following in Africa and Asia.

Let’s say I’m going to call you mobile-to-mobile. The carriers have the capability to pass the traffic to VIBER. VIBER will check if you have an account or not with them. And if VIBER is running on your mobile phone, they will terminate the call on the VIBER application and in that way the interconnect carrier avoids paying the normal, legal termination rates.

Gee, I use Skype quite a bit. Can the OTT bypassers commit fraud through Skype?

Actually, no. Skype uses its own unique user names: it’s not associated with a mobile number. The difference is that VIBER uses your telephone number to take incoming VIBER calls. Just like WhatsApp.

So instead of terminating on the voice network, and paying termination rates to the mobile operator, it will go to my data connection through WiFi or GPRS. And when that’s done, if the mobile operator normally gets 10 cents a minute to terminate, they get zero revenue.

So this is a new form of bypass and has only existed for a few months, and yet we have a solution for this. It’s now a big deal in many countries. Even in

Related Articles

- Fraud Management at Kyivstar in Ukraine — interview with Anton Pivala — Kyivstar from Ukraine is a leading mobile operator in both voice service quality and consumer value. This case study gives details on Kyivstar’s fraud control program, reveals some of the unique operator challenges faced in Eastern Europe, and explains how Kyivstar is successfully winning the battle against IRSF and SIMbox fraud.
- Gratifying Ghana: Why Listening to Operators Trumps Vendor Technology and Size — interview with Ludwig Lindqvist — The value of technically excellent software is negated if the solution is not implemented right. This article makes a strong case that vendors need to focus on first things first — get in full sync with a service provider’s business, capabilities and unique needs before you recommend or implement any software. Topics discussed include: the benefits of retaining in-house expertise, implementation challenges in Africa, and the meaning of “through engagement” with the client.
- “Fraud Is a Wind that Always Blows” and Other Wisdom From a 28-Year Old Software Firm — interview with Gary Beck — Here’s the amazing story of how Beck Computers was pulled out of a Tier 1 account only to be brought back in a few months later. The article explores software vendor service and support challenges, real-time computing requirements, advanced fraud management functions, and ways to educate management on the value an FMS investment.
- Fraud & Credit Risk Software: Setting the Client Free to Innovate — interview with Luke Taylor — Not every operator wants the freedom to configure its own fraud management solution, but certain providers wouldn’t live without such a “framework” approach . This article discusses: the reasons why operator choose this strategy as it covers many other fraud and credit software implementation issues.
- Fraud & Credit Risk Software: Setting the Client Free to Innovate — interview with Roger Ansin — The richest criminal path to International Revenue Share Fraud (IRSF) goes through the enterprise PBX. Hijacking the PBX has cost businesses and telecoms countless billions of dollars in the past 15 years. In this interview you’ll learn about this industry challenge and an affordable and proven tool that blocks IRSF at the enterprise.
- INSIDER: The Value of Technically Excellent Implementation Issues — interview with Luke Taylor — Not every service provider’s business, capabilities and unique needs before you recommend or implement any software. Topics discussed include: the benefits of retaining in-house expertise, implementation challenges in Africa, and the meaning of “through engagement” with the client.
- Recruiting Smartphone Users as Partners in Telecom Fraud & Security Control — by Tal Eisner — Premium Rate Service (PRS) fraud and spyware on a mobile phone can ruin an operator’s relationship with a subscriber. The attacker uses malware to automatically generate phone calls, SMSs and data sessions to high cost (premium) phone numbers. This article discusses a new crowd sourcing mobile app that addresses the problem and helps operators better manage the threat.
- Roaming — if Managed Correctly — Can Be a Spark to Revenues — by Brian Silvestri — Major analyst firms are predicting that roaming revenues will almost double in five years. What’s more, roaming remains at the pivot point of Wireless Carrier strategy. Drawing lessons from the...
Integrated Test Call and FMS to Fight international Bypass fraud via SIM Box and OTT Services like VIBER
places like Belgium — which has no SIM boxes — VIBER bypass is happening.

What we do is make test calls to smartphones controlled by our machines. And we simply measure: is the call coming in on the regular connection or through the VIBER application. It’s fully automated — we take care of set-up, testing, analysis and reporting. There’s very high demand for this kind of solution and we are the first to market one, so it’s quite exciting.

Kenneth, thanks for this fine briefing. The fraudsters are innovative and clever. So we’re fortunate to have solution vendors like SIGOS who are focused on bypass issues and are keen to make the right R&D investments.

Copyright 2015 Black Swan Telecom Journal