CASE STUDY

Keysight Lawful Intercept Solution Saves Customer €1 Million per Year

KEYSIGHT

Case Study at a Glance

Organization

- Large international mobile phone carrier with extensive roaming subscribers
- 15 million subscribers

Challenges

- Needed to identify calls that were bypassing the LMISF
- Needed call data correlation of signaling and bearer info
- Needed to troubleshoot why calls bypassed the LMISF
- Needed to mitigate the issue

Solutions

- Vision X network packet broker
- MobileStack
- AppStack
- Flex Taps with 10, 40, and 100 GE transceivers
- CloudLens virtual tap
- 10, 40 and 100 GE transceivers

Results

- Prevented €1M in annual revenue loss
- Reduced diagnosis time 87% per incident
- Improved compliance to CETS No. 224 for LI

Overview

When it comes to regulatory compliance, you can't afford not to have complete network visibility. You need to know what is, and what is not, happening on your network at any given time. A large wireless voice and data carrier with 15 million subscribers worldwide had this exact problem — they had blind spots that they knew were causing problems but couldn't see a solution.

Customer Challenges

The wireless communications carrier needed a solution to address the following four pain points:

- Identify calls that were bypassing the Lawful Intercept Mirror IMS State Function (LMISF) network functionality.
- Correlate the signaling and data streams for those calls for packet capture file (PCAP) creation.
- Analyze the information to determine if the scenario was created by a malicious entity or if it was some sort of misconfiguration error.
- Finally, mitigate the problem by either fixing the configuration error or sending the malicious information to the legally authorized enforcement agency.

Specifically, the carrier needed to capture specific pieces of voice and data packets on their network and then be able to forward a copy of that data to legally authorized government collection points. While lawful intercept of voice and data isn't a new concept, a problem has been created by an increase in encrypted data and VoLTE roaming calls due to the discontinuance of 3G network equipment. Some calls were believed to be bypassing the LMISF unit. Exacerbating the problem is that fact that multi-roaming calls are routed through a disaggregated network, meaning that logs produced by individual elements are not sufficiently detailed for root cause analysis of the problem.

In this case, the European wireless service provider turned to Keysight Technologies — the only network visibility vendor that is part of the ETSI standards group. Keysight has a long history of understanding visibility solutions for service providers, which was clearly evident by the solution that was provided.

Keysight's Solution

Keysight was able to solve the customer's problem by deploying a solution with the following components:

- Vision X packet broker that has a backbone capacity of full-duplex, non-blocking, and line rate traffic at 12.8 Tbps.
- A variety of fiber interfaces for the Vision X that can support 10GE, 25GE, 40GE, 50GE and up to 100GE wire speeds.
- The MobileStack feature package which supports data correlation and packet capturing and filtering for wireless carrier networks.
- The AppStack feature package which supports application filtering and the collection and correlation of metadata.
- 100 GE Flex taps and CloudLens virtual taps that enable user traffic to be collected using physical taps and the control plane traffic to be captured using virtual taps.

One of the most important features that the customer was looking for was QCI-based bearer identification. In this case, QCI stands for **Q**oS **C**lass **I**dentifier, as described in the 3GPP TS 23.203/ ETSI TS 123 203 standards. User traffic bearers are assigned a QCI number between 1 and 9. As an example, a QCI of 1 is used for real-time voice (best quality), a QCI of 5 is used for call signaling (e.g. call setup and call tear down), and a QCI of 9 is the low priority level which is used for standard internet traffic. In certain situations, like when an inbound roamer from another carrier, completes a call into the roaming network, this can present challenges, especially when encryption is used. While calls are normally encrypted, which is good for privacy, it causes a problem for lawful interception obligations. This is because the encryption keys are managed by the whole network of the roaming subscriber. To resolve this issue, carriers agree to turn off encryption for roaming voice calls. If encryption is accidentally or maliciously turned on, the LMISF unit does not get activated.

Even though the wireless carrier has a LMISF unit to implement lawful interception of calls, delivering a copy of those calls to law enforcement when activated for targeted users was a challenge because the unit only looks at calls with a quality with a QCI of 1 or 5. Everything else is ignored. So, some use cases, like misconfigured settings or deliberate obfuscation by the user, can trigger a bypass of the LMISF unit. This is where Keysight's Lawful intercept solution is able to fill the gap. Keysight's MobileStack product supports the QCI function, as described in 3GPP TS 23.203/ ETSI TS 123 203. The product filters user plane traffic matching a specified QCI value, enabling the monitoring of specific services. Once engaged, MobileStack sends the live correlated control plane information, along with the user plane traffic that matches the filtering criteria, to a configured egress destination where the traffic can be captured and stored in a PCAP file by another device. If the filtering criteria is the user id (e.g IMSI, MSISDN), the result will be that the live correlated traffic for those users will be sent towards the configured egress ports where capture can occur.

The AppStack product then adds the ability to generate subscriber aware metadata, thus having mobile core related details (e.g. user identifier, device identifier, location details, etc) in the produced data records together with metadata on the content of the Bearer (e.g. voice, video and data traffic). Once the carrier's engineering team has this information, they can then look for malicious and misconfigured traffic. If the problem is due to a misconfiguration error, the engineering team can conduct an internal investigation to fix the problem(s) in the database or customer handset. If the source of the problem was deemed to be malicious activity, then this issue can be passed to the authorities and lawful intercept agency.

This diagram shows exactly how the Keysight solution was integrated into the customer's network.

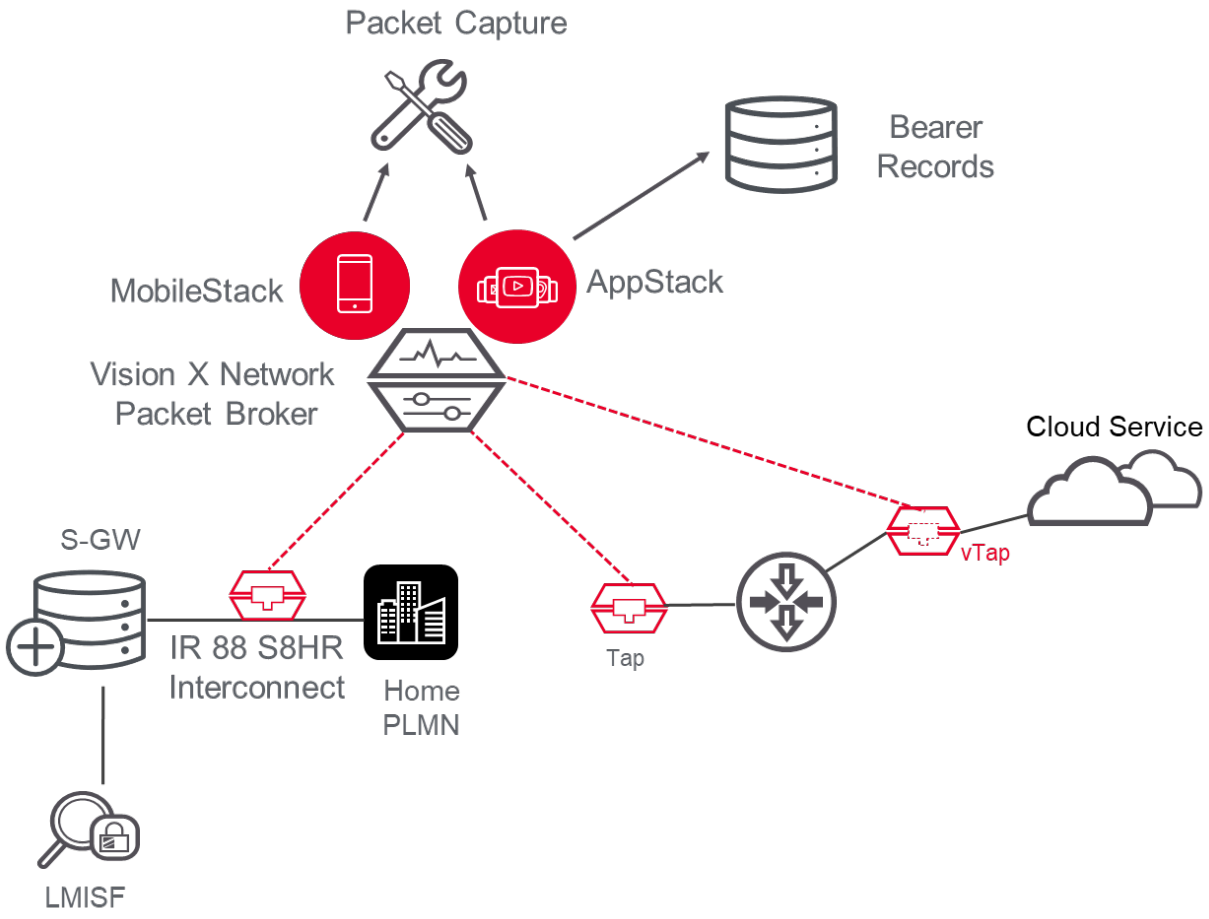

Figure 1. Keysight's Lawful Intercept Solution

As Figure 1 indicates, the core network interfaces use 100 GE links. The lawful intercept probes use 10 GE and 40 GE links. A combination of physical taps and virtual taps were used to capture data traffic across the network and forward that traffic to the Keysight network packet broker. A Keysight Vison X packet broker was installed in the core for data aggregation, filtering, and regeneration. The AppStack and MobileStack applications run on processor modules installed into the Vision X.

Results

Due to the Keysight solution, the customer was able to experience the following results:

- Revenue loss was reduced due to improper circuit configuration and fraud by €1 million per year.
- Reduction of diagnosis time by approximately 87% per incident
- Improved compliance to the CETS No. 224 law regarding the proper capture and passing of legally requested data to the law enforcement agency (LEA)

The Keysight solution was able to provide the customer's engineering team with the data they needed to determine which calls were fraudulent, i.e. where subscribers were deliberately trying to use a QCI settings of 5 or 9 to reduce voice and streaming data costs. By fixing configuration errors and by eliminating improper conduct by subscribers, the customer was able to eliminate some of the fraudulent activity (€1 million) on their network. While this is a small portion of the $5.97 billion annual interconnect bypass fraudulent activity that takes place on telecom networks (according to BICS research), it's a good start.

The Keysight solution also reduced personnel analysis costs by automating the filter and data collection process. This was equivalent to saving 1 full time equivalent (FTE) day of labor that was occurring approximately twice every month. By reducing data collection and diagnosis time from 8 hours to less than 1 hour, the engineering staff realized a productivity gain of approximately 87% per incident.

With the proper identification of subscribers who were trying to subvert lawful intercept attempts by government agencies, the customer was able to deliver more complete and accurate information to the LEA service points. This enabled better compliance with the European Union law requiring lawful intercept capabilities.

Conclusion

The customer implemented a Keysight lawful intercept solution and were able to accomplish their key goals that included:

- Identifying calls that are routed as data channels, when in fact they should be voice channels
- Identifying calls that are encrypted when they should have encryption turned off
- The capture and correlation of signaling data streams with the bearer data for analysis of misconfigured equipment or traffic that needs to be forwarded to the LEA

In addition, the customer was able to realize the following benefits:

- They reduced revenue loss due to improper circuit configuration and fraud by €1 million per year.
- Reduced diagnosis time by approximately 87% per incident
- Improved compliance to the CETS No. 224 law regarding the proper capture and passing of legally requested data to the LEA

See what Keysight lawful intercept solutions can do. Visit the Keysight Service Providers solution webpage for more information.

.