No.83
February 2025

HardenStance Briefing

Trusted research, analysis & insight in IT & telecom security **PUBLIC/ SPONSORED**

Enea's Voice Firewall for Telcos

Sponsored by Enea

- Enea deployed its first voice firewall for Telecom Egypt back in 2022. Today, the company is bringing it to voice fraud prevention opportunities worldwide. Malicious caller ID spoofing is the initial use case, followed by Wangiri and Flash calls.
- Enea's voice firewall is built on the company's core signaling and messaging security platform. This isn't just cost effective; correlation of voice and signaling traffic in the same platform is also key to effective detection of scam voice calls.
- Enea's voice firewall supports many of the variants among caller ID spoofing prevention architectures that telcos have started deploying worldwide. The company is also contributing to accelerating industry momentum around defining industry best practice and guidelines for blocking CLI spoofing and other voice fraud.

Download the accompanying White Paper: "Proven ways to block Caller ID spoofing scams"

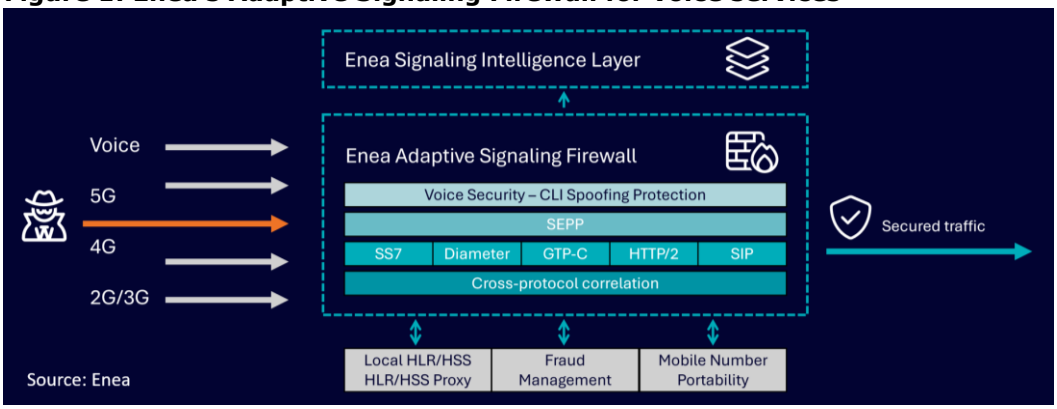
Enea is a company with a strong pedigree in network security. It's derived from its Qosmos DPI and traffic intelligence software used by a range of cybersecurity vendors, as well as its messaging and signaling security solutions that are used by many of the world's leading telecom operators. In a telecom vendor market characterized by a variety of niche network security specialists on the one hand, and some much larger, generalist networking vendors on the other, Enea is also distinguished among network security specialists by being a public company.

The additional development has centred on adding a SIP stack to existing signaling protocols like SS7, Diameter and GTP-C.

The addition of a SIP stack to existing signaling protocols

By far the most important extension of Enea's cybersecurity portfolio of late has been the launch of its new voice firewall. In development since 2021 and Generally Available (GA) since May 2024, the voice firewall has been developed in response to growing demand from regulators and telco customers to be able to block increasing volumes of nuisance and scam voice calls. Enea's solution competes in the established voice firewall market as defined and recognized by telecom operators and regulators throughout the world. It is built on the same platform that already supports Enea's core messaging and signaling security solutions. Additional development has been required to add a SIP stack to existing signaling protocols like SS7, Diameter and GTP-C.

Figure 1: Enea's Adaptive Signaling Firewall for voice services



Hosting the voice firewall on the company's core signaling platform is beneficial in terms of cost efficiency and scale. Even more importantly, the integration with signaling security functions is also critical to the product's core detection efficacy.

For the lead use case, which is malicious caller ID spoofing, Enea's voice firewall can support a range of rules. As discussed on page 3, chief among them it can correlate voice traffic with signaling traffic to verify whether incoming mobile calls coming in on the international interface are indeed roaming– and block them if they aren't. This is done by checking for a CAMEL trigger and correlating it with the SIP invite.

It's far more effective to perform this type of correlation within the same platform than two separate ones. It has the additional advantage of making the voice firewall an easy upgrade for Enea's existing customers. It's also an important new portfolio option for any telco that is evaluating Enea as a long term network security partner across their voice, text and data services.

Enea can correlate voice traffic with signaling traffic to verify whether incoming mobile calls coming in on the international interface are indeed roaming.

A 'Zero Trust' approach to blocking voice fraud

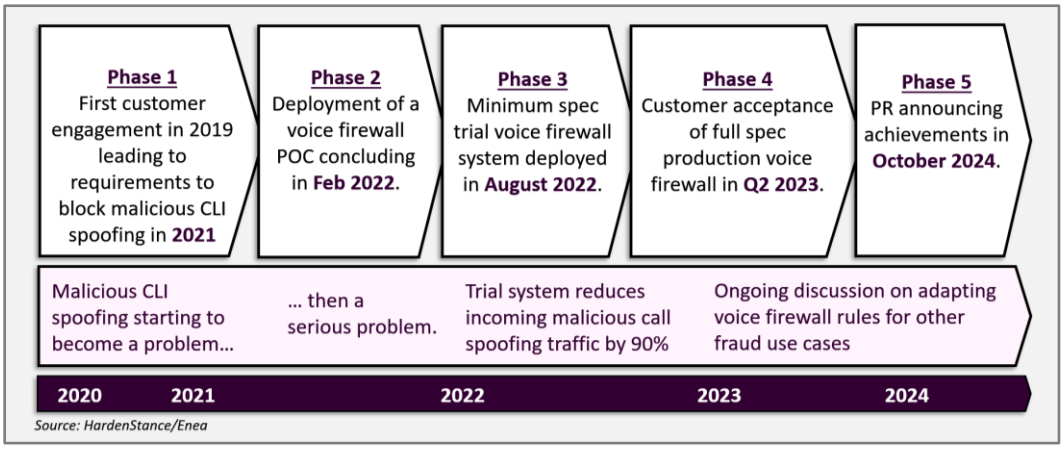
As described on page 3, Enea's solution assumes all traffic to be untrusted and therefore requires a variety of verifications. Consistent with that, the company brands its voice firewall as supporting a 'Zero Trust' architecture. This provides very clear differentiation from the STIR/SHAKEN standard which uses a trusted architecture leveraging certificates, key exchange and encryption. Having originally been considered as a potential standard for blocking CLI spoofing, many leading regulators and operators around the world have decided against using STIR/SHAKEN for this use case.

As depicted in **Figure 2,** Enea has worked with Telecom Egypt as its lead partner for bringing its voice firewall solution to market. Having deployed a Proof of Concept (POC) for blocking caller ID spoofing in February 2022, Telecom Egypt cut over a trial system in commercial service six months later. Enea developed additional rule sets that are tailored to CLI spoofing threats in the Egyptian market. Some of these rules are inherently static, such as whether a given international number is valid or not. Others are inherently dynamic such as whether the subscriber is roaming or not. Others still require periodic rather than dynamic updates. That includes Do No Originate (DNO) lists - lists of numbers that only receive inbound calls.

Rules can often be applied without any downtime

Enea's professional services organization has years of experience of regularly updating these types of rules for messaging and signaling security to assure up to date compliance with regulatory requirements. Rules can be applied in a live deployment with the Enea solution, often without any downtime or needing to plan a maintenance window.

Figure 2: Enea has partnered Telecom Egypt to block CLI spoofing since 2021



As verified by Telecom Egypt's press release of June 2024, by dramatically reducing the success that scammers were enjoying using this technique, Enea's voice firewall reduced the operator's incoming scam calls using spoofed caller IDs by 90%.

Around the world, early adopter markets have had very significant success blocking malicious caller ID spoofing with a variety of approaches (see "Proven ways to block caller ID spoofing scams" at the foot of this paper). Enea positions its voice firewall as meeting the requirements of the large majority of these variations in approaches.

Verifying outbound mobile roaming traffic is the sweet spot

In terms of basic voice firewalling, Enea supports things like Do Not Originate (DNO) lists and various other 'allow' and 'block' rules. For example, it can block a given international number if it does not conform to designated formats, number ranges and prefixes or any national landline numbers coming in via the international interface. In most markets, however, outbound mobile roaming traffic is the sweet spot for blocking the largest volume of malicious CLI spoofing calls. That's because mobile calls tend to account for at least 80% of all voice traffic now. Moreover, most unwanted and fraudulent phone calls, including malicious CLI spoofing calls, originate from overseas.

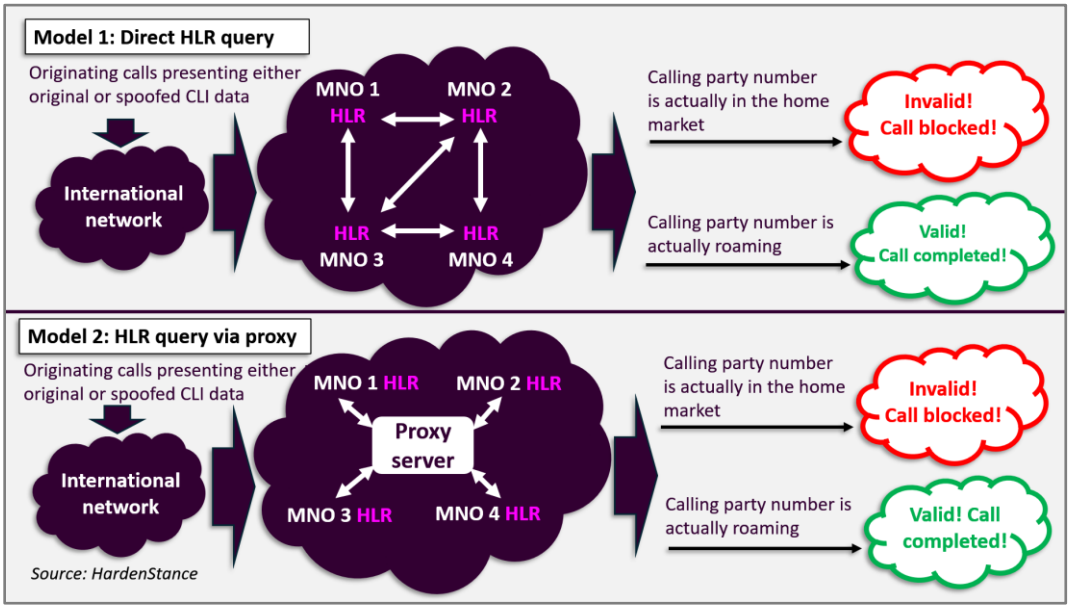
As verified by Telecom Egypt, Enea's voice firewall achieved a 90% reduction in incoming scam calls with spoofed caller IDs.

To verify that caller IDs that imply they are one of another domestic operator's mobile subscribers while roaming are actually roaming, operators and regulators in early adopter markets have used a number of different approaches. As depicted in **Figure 3**, they have used two main types of architecture - direct HLR querying and HLR querying via proxy. Both require expertise in mobile network signaling of the kind Enea excels at:

1 **Direct HLR querying:** with a Direct HLR query model, mobile operators have to expose signalling interfaces to one another and send each other details about the status of one another's mobile customers on request and in real time.

2 **Inter-operator HLR querying via proxy.** The alternative to rival operators querying one another's HLRs directly is to deploy a proxy server between them. This allows each operator to provide as well as access the same type of information about one another's customers, albeit in a more anonymized, less intrusive way. In this model, the operator that submits a query to the proxy doesn't know which of its competitors the subscriber is served by. Similarly, the queried operator doesn't need to know from which of its competitors the query is coming from. Usually, the neutral third party best suited to managing a proxy is the national regulator.

Figure 3: Verification options for outbound roamers



Either of the two models depicted in **Figure 3** has to be executed in a way that protects against compromise of sensitive subscriber information like the user's IMSI, cell ID or Visited Location Register (VLR). A telco's own confidential business information also has to be protected. For that reason some early implementations of the direct query model rely on a bare-bones binary response to a query that either means 'yes' the subscriber is roaming or 'no' they're not. Providing richer context can be helpful for more granular detection but it also carries greater risk of exposing confidential information.

By virtue of being among the pioneers in this space, Enea had to build a solution for Telecom Egypt in the absence of any agreed international best practices and guidelines. Work to bring global guidelines and best practices to market was started by national regulators, the Conference of European Post and Telecommunications administrations (CEPT) and the GSMA and has been picked up the i3Forum. The first i3Forum Working Group reports are expected in Q1 2025. Even when those guidelines are agreed and published, they will still embrace different options to meet the different requirements of a variety of different regulators and telcos in different countries and regions. In the meantime, in a market which is moving at pace with no formally agreed industry guidelines to draw on, key stakeholders are even more reliant on a voice firewall supporting flexible rule sets that can be adapted to local needs, local regulations, and changes in the local threat landscape.

Malicious caller ID spoofing is the initial use case Enea is targeting with its voice firewall but Wangiri, flash call and other use cases are also on the roadmap.

Wangiri and flash call use cases as well as caller ID spoofing

When telcos select vendor partners, it's always important to verify that a vendor's solutions comply with global standards such as 3GPP in the case of mobile networks. In the case of many voice fraud solutions, where the industry has already made a start deploying commercial solutions at scale before guidelines and best practices have even been agreed, aligning with vendors that are deeply embedded in developing those new global industry guidelines is arguably even more important.

As well as being actively involved in GSMA, and the I3Forum, Enea was also engaged in the first international standardization effort in this area. This was the publication of ECC Recommendation 23 (03) on "measures to handle incoming international voice calls with suspected spoofed national E.164 numbers" by CEPT in November 2023.

In recent years, Enea has sought to differentiate itself more and more via its threat intelligence capabilities. The company has distinguished itself with the quality and quality of the research it has published on the activities of Russian cyber threat actors exploiting signaling vulnerabilities to monitor Ukrainian and other European targets.

This core competence in harvesting and curating cyber threat intelligence is also important for blocking voice fraud. That's because fraudsters are constantly looking for ways around the sorts of simple binary rules that telcos have to implement for regulatory compliance. The ability to draw on advanced, threat intelligence-led verification techniques is important for any telco that wants to give customers the best possible protection. Malicious caller ID spoofing is the initial use case Enea is targeting with its voice firewall but Wangiri, flash call and other use cases are also on the roadmap.

Telcos and regulators are used to thinking of Enea as a partner or potential partner for signaling security and SMS firewalling. These days the company is competitive in the voice firewall space too. ■

About Enea

We are a world-leading specialist in advanced telecom and cybersecurity software with a vision to make the world's communications safer and more efficient. Our solutions connect, optimize and protect communications between companies, people, devices and things worldwide. We are present in over 80 markets and billions of people rely on our technology every day when they connect to mobile networks or use the Internet. Enea is headquartered in Stockholm, Sweden and is listed on NASDAQ Stockholm. Visit us at Enea.

More Information

- Enea's "CLI Spoofing Buyers' Guide"
- Enea's Voice Protection Products
- June 2024 PR: "Telecom Egypt reports 90% reduction in incoming scam calls"
- HardenStance White Paper: "Proven ways to block Caller ID spoofing scams"

About HardenStance

HardenStance provides trusted research, analysis and insight in IT and telecom security. HardenStance is a leader in custom cyber security research and leading publisher of cyber security reports. HardenStance is also a strong advocate of industry collaboration in cyber security. HardenStance openly supports the work of key industry associations, organizations and SDOs including NetSecOPEN, AMTSO, The Cyber Threat Alliance, The GSM Association, MEF OASIS, ETSI and TM Forum. www.hardenstance.com.

To receive an email notification whenever HardenStance releases new reports in the public domain, register here (there are only four fields): Registration Link

HardenStance Disclaimer

HardenStance Ltd has used its best efforts in collecting and preparing this report. HardenStance Ltd does not warrant the accuracy, completeness, currentness, noninfringement, merchantability or fitness for a particular purpose of any material covered by this report.

HardenStance Ltd shall not be liable for losses or injury caused in whole or part by HardenStance Ltd's negligence or by contingencies beyond HardenStance Ltd's control in compiling, preparing or disseminating this report, or for any decision made or action taken by user of this report in reliance on such information, or for any consequential, special, indirect or similar damages (including lost profits), even if HardenStance Ltd was advised of the possibility of the same.

The user of this report agrees that there is zero liability of HardenStance Ltd and its employees arising out of any kind of legal claim (whether in contract, tort or otherwise) arising in relation to the contents of this report.