SUBEX

Multiple Facets of CLI Spoofing: Risks, Impact & the Way Forward

Point of View

Introduction

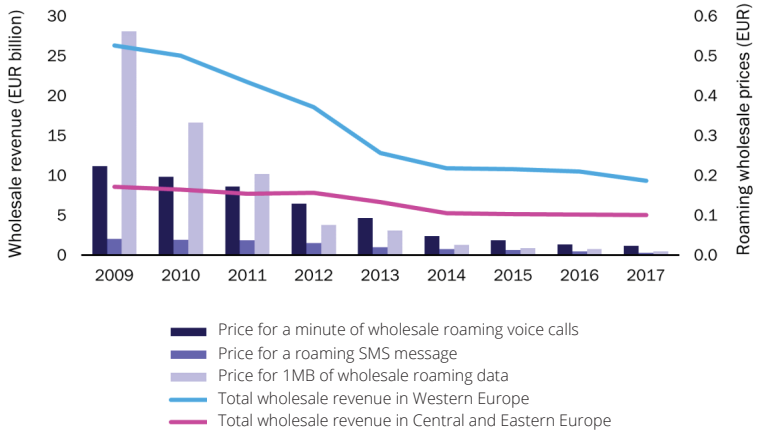
'CLI Spoofing' provides a generic categorization of a range of different fraud scenarios, which involve the manipulation of the calling number (A-Number) as a key feature/aspect of the 'exploit.'

Although this characteristic may be common across a range of fraud scenarios, other key aspects are not necessarily shared, for example, the primary motivation for changing the CLI. In this article, we will compare and contrast some of the ways 'CLI Spoofing' is used as part of a range of very different fraud scenarios.

Location, Location, Location...

In Europe, factors such as increased competition as well as national and regional regulation have led to a steady decline in mobile wholesale revenue. Figure 1 clearly shows the pattern from 2009 – 2017 (1). However, in June 2017, the European Commission enacted Regulation (EU) 2016/2286. Commonly referred to as "Roam like at home," it established a single market in the EU, effectively abolishing roaming charges and allowing European Union residents to use their mobile phone in other EU countries at their domestic rate, thus further eroding roaming revenues.

Figure 1: Mobile wholesale revenue in Europe and theaverage international roaming wholesale prices in the EEA, 2009-2017



In recent years, legislation has also driven the adoption of Origin-Based Rating/Charging (OBR/OBC), where calls to the same destination have different prices depending on where the call originated from, with legislation dictating that EU-originated calls should have a lower termination rate than & Non-EU-originated traffic.

To facilitate this method of charging, CLI plays a critical role in identifying the origination of the call and the appropriate charging. This has created a significant opportunity for unscrupulous carriers to gain a commercial advantage by manipulating the CLI to show an origination that would benefit from a lower termination rate. 'Refiling' techniques have been with us since the commencement of Origin Based Charging and continue to impact carrier and operator revenues.

Interconnect Bypass is another type of fraud where the original (International) CLI is removed as part of the bypass of the international gateway. The bypass call can be 'routed/presented' in a range of ways, e.g., via a SIM Box containing SIMs belonging to the target mobile network and/or other in-country mobile operators fixed-line services in the country, e.g., via an IP PBX. In all these scenarios, an international originating call is presented as an on-net or national call. To provide some context to the extent of the impact, the RAG RAFM Survey 2020 suggested Bypass related fraud cost the industry **$ 6.86 billion** (2).

The above examples show how CLI Spoofing is used to a greater or lesser degree to obfuscate or manipulate the true origin of the call in order to gain a financial advantage. The use of these techniques further erodes margins and revenues for legitimate carriers and operators, impacts law enforcement, and may impact the call quality for the originating subscriber.

However, CLI Spoofing also plays a critical but very different role in other fraud scenarios for example, as part of a scam call.

You Look Familiar!

Scam calls are unsolicited calls where fraudsters utilize a range of social engineering techniques to steal money or information from the victim through deception. Common scenarios include demands for (fictitious) unpaid fines or payments, offers of 'too good to be true' bargains, and fictitious investment opportunities. In some scenarios, the scammers will not directly

attempt to scam the customer but will focus on obtaining personal information, payment, and security details which they can then use later to facilitate other frauds.

A key tool in building 'trust' and credibility with the victim can be the use of CLI Spoofing to present a phone number that the victim may have some form of familiarity with, e.g., a local number. In more sophisticated scams, the scammers may present the freephone number of a bank. If the victim is unfortunate enough to be a customer of that bank and has their details stored on their phone, the incoming call may present with the name of the bank, potentially increasing the victim's level of trust.

'Robocalling,' which is a term coined in the USA to describe the range of unsolicited calls (including scam calls) containing pre-recorded messages, has plagued customers in the USA and other parts of the world over recent years. Robocalls can also use CLI Spoofing to mask the real origination of the call, which is commonly from an international origination, and present a spoofed local or national CLI. Due to the phenomenal volumes of Robocalls being generated, telephone subscribers' behavior has changed significantly in the USA. Hiya's "State of the Call 2021" reports that 94% of respondents surveyed let unidentified incoming calls go unanswered.

Due to the continued customer complaints and negative publicity generated from the victims of these scams in the US, the Federal Communications Commission (FCC) drove a range of initiatives to mitigate the impact of robocalling culminating in the definition and rollout of STIR/SHAKEN. This provides a mechanism for providing the receiving operator/customer with a level of confidence on the validity of the CLI. The FCC summarises the capability as follows.

"calls traveling through interconnected phone networks would have their caller ID 'signed' as legitimate by originating carriers and validated by other carriers before reaching consumers. STIR/SHAKEN digitally validates the handoff of phone calls passing through the complex web of networks, allowing the phone company of the consumer receiving the call to verify that a call is, in fact, from the number displayed on Caller ID"

In Canada, the telecoms regulator (CRTC) also plans to implement STIR/SHAKEN. CRTC reported that 40% of the total complaints received annually were related to unwanted phone calls arising from caller ID spoofing (3).

STIR/SHAKEN is clearly a positive initiative, but it is not a "silver bullet". Although the approach has been accepted in the USA and Canada, there have been delays in the rollout. The deadline for deployment for operators in Canada has now moved back to September 2021 (4).

From an industry adoption perspective, STIR/SHAKEN has not been accepted as a global standard, with different industry groups in other regions currently promoting alternative solutions. Apart from the timelines for the rollout of similar solutions in other regions, interoperability of the different solutions will also need to be considered. Other limitations with STIR/SHAKEN in terms of coverage exist; hence it may not be surprising that YouMail still estimated the level of robocalling in the USA to be just under 46 billion calls in 2020. Clearly, there is still significant work to be done.

Challenges With Traditional Approaches And The Way Forward

A range of solutions and approaches exist to try to identify some of the fraud scenarios discussed. However, for CLI Spoofing, it is recognized that CDR-based analysis is not an effective method of detection. However, the use of real-time signaling level analysis, paired with advanced machine learning techniques, provides new opportunities to drive a prevention-based approach. It supports both carriers and operators in addressing these types of fraud risks effectively and preventing them from continuing to impact revenues, margins, reputation and drive increased consumer and regulatory pressure.

References:

(1) https://www.analysysmason.com/contentassets/bd234e3b6389461d94fcf59d3fde564f/analysys_mason_mobile_wholesale_europe_may2020_rddf0_rd008_rddc0.pdf

(2) https://riskandassurancegroup.org/rag-rafm-survey-2020/

(3) https://www.ctvnews.ca/business/phone-service-providers-expected-to-adopt-new-caller-id-verification-program-1.4722001

(4) https://crtc.gc.ca/eng/archive/2019/2019-402-2.htm

SUBEX

www.subex.com

About Subex

Subex is a pioneer in enabling Digital Trust for businesses across the globe. Founded in 1994, Subex helps its customers maximise their revenues and profitability. With a legacy of having served the market through world-class solutions for business optimisation and analytics, Subex is now leading the way by enabling all-round Digital Trust in the business ecosystems of its customers. Focusing on risk mitigation, security, predictability and intelligence, Subex helps businesses embrace disruptive changes and succeed with confidence in creating a secure digital world for their customers.

Through HyperSense, an end-to-end augmented analytics platform, Subex empowers communications service providers and enterprise customers to make faster, better decisions by leveraging Artificial Intelligence (AI) analytics across the data value chain. The solution allows users without a knowledge of coding to easily aggregate data from disparate sources, turn data into insights by building, interpreting and tuning AI models, and effortlessly share their findings across the organisation, all on a no-code platform.

Subex also offers scalable Managed Services and Business Consulting services. Subex has more than 300 installations across 90+ countries. For more information, visit www.subex.com

Subex Limited

Pritech Park, SEZ Block -09,
4th Floor B Wing Survey No. 51
to 64/4 Outer Ring Road,
Karnataka 560103, India

Tel: +91 80 37451377
Fax: +91 80 6696 3333

Subex, Inc

12303 Airport Way,
Bldg. 1, Ste. 390,
Broomfield, CO 80021

Tel : +1 303 301 6200
Fax : +1 303 301 6201

Subex (UK) Ltd

1st Floor, Rama
17 St Ann's Road,
Harrow, Middlesex,
HA1 1JU

Tel: +44 0207 8265300
Fax: +44 0207 8265352

Subex (Asia Pacific) Pte. Limited

175A, Bencoolen Street,
#08-03 Burlington Square,
Singapore 189650

Tel: +65 6338 1218
Fax: +65 6338 1216

For more information write to **info@subex.com**

Regional offices: Dubai | Ipswich