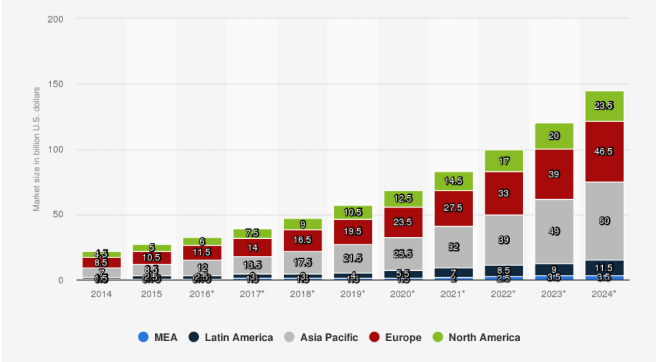
SUBEX

SIP Security: Why should it matter?

Point of View

The global VoIP market is growing at a rapid pace. The penetration of VoLTE networks, the surge of VoIP traffic, low data rates, low calling prices have contributed heavily to the rise of the VoIP market. The industry will further witness a spike owing to market disruption with the increasing commercialization of 5G and the rapidly growing use of VoIP networks. In addition, increasing dependence on cloud-based unified communications and transition from legacy systems promotes the acceptance of hosted VoIP services. The below diagram depicts the size of the VoIP market worldwide by region from 2014 to 2024.



Source: https://www.statista.com/statistics/691602/global-mobile-voip-market-size-by-region/

It has overshadowed the traditional communication technologies, which are comprehensible due to its benefits in terms of accessibility, portability, scalability, voice quality, flexibility, & lower costs. Although there are numerous protocols used in voice-over-IP (VoIP) communications, Session Initiation Protocol (SIP) has become a de-facto protocol for voice-over IP (VoIP) communication. It is now one of the most widely used and deployed telecom signaling protocols in the world. It is used in mobile, fixed, and enterprise networks to establish and manage voice and video calls and interconnection between networks and provide instant messaging and presence functionality. Within mobile networks, SIP is used by VoLTE (voice-over 4G), Vo5G (voice-over 5G), and Rich Communication Services (RCS). It is used everywhere, from the handset to the core IMS networks and onwards to the interconnects.

Also, another contributing factor for widespread use of SIP is that due to lower costs, a large amount of international traffic is being carried through SIP interfaces compared to traditional interfaces such as ISUP and Diameter; thus, operators are now moving from conventional services to SIP-based services.

However, due to the nature of the SIP, it is highly prone to attacks from external factors. It has a larger potential attack surface and a massive number of potential attackers with the necessary skills to understand and attack it. Attackers use techniques such as SIP network fingerprinting, DNS/Internet Reconnaissance, SIP Port scanning, etc., to carry out the attacks. It attracts far larger numbers and more sophisticated breeds of hackers, resulting in massive acceleration in the frequency and variety of VoIP attacks against 4G and 5G networks.

Let us now look at some of the top fraud types/methods.

Top frauds prevalent in SIP and the traditional protocols

Following are the frauds which continue to be a major cause of concern with traditional as well as SIP protocol; however, the inherent nature of SIP and the easy availability of tools/software has made it easier for fraudsters to commit these frauds at a larger scale and in an automated fashion.

CLI Spoofing

CLI Spoofing is one of the common methods used by fraudsters to identify themselves as a trusted caller. Spoofing is when a caller deliberately falsifies the information transmitted to your caller ID display to disguise their identity. VoIP technology using SIP lets fraudsters conduct caller ID spoofing with minimal cost and effort.

PBX/IP PBX Hacking

A PBX (Private Branch eXchange)/IP PBX is telephone equipment that is installed on corporate premises to provide a number of telephone extensions within an office and operate as a connection between the business and the external dial-out network. PBX hacking happens when someone gains access to a business's PBX phone system and generates a profit from the international calls at the business's expense. Fraudsters incorporate various methodologies to hack PBXs and IP PBXs, such as brute force IP-PBX with REGISTER messages and traditional PBX with PINS, etc.

Wangiri Fraud

In this fraud, the fraudster places a short call to several customers to leave a missed call notification on the display of customers' handsets, thus prompting them to call back. When the customer calls back, the call is either routed to an IVR or premium rate service (PRS) number only to realize that they have been charged heftily for the call. SIP technology has further paved the path for fraudsters to carry out such frauds easily.

IRSF

International Revenue Share Fraud occurs where traffic is artificially inflated to high-cost international destinations, and a proportion of the termination revenue is shared with the fraudster that has originated the call. Typically, the originator of the call has no intention of paying for the call and is either using a stolen subscription or a fraudulently obtained subscription.

Top Attacks unique to SIP

SIP Register Attacks

SIP Register flood consists of sending a high volume of SIP REGISTER or INVITE packets to SIP servers (indifferently accepting endpoint requests as the first step of an authentication process), exhausting the bandwidth and resource.

Malicious User Agent Attacks

Attackers make use of open-source tools available in the market to find the vulnerabilities in the server and exploit them.

INVITE Replay Attacks

In this, the attacker can perform reconnaissance on the telecom network to discover the SIP services. Then the attackers flood the services with INVITE messages to perform DoS attacks on various services. In fact, attackers may also use INVITE messages to inflate traffic to certain networks.

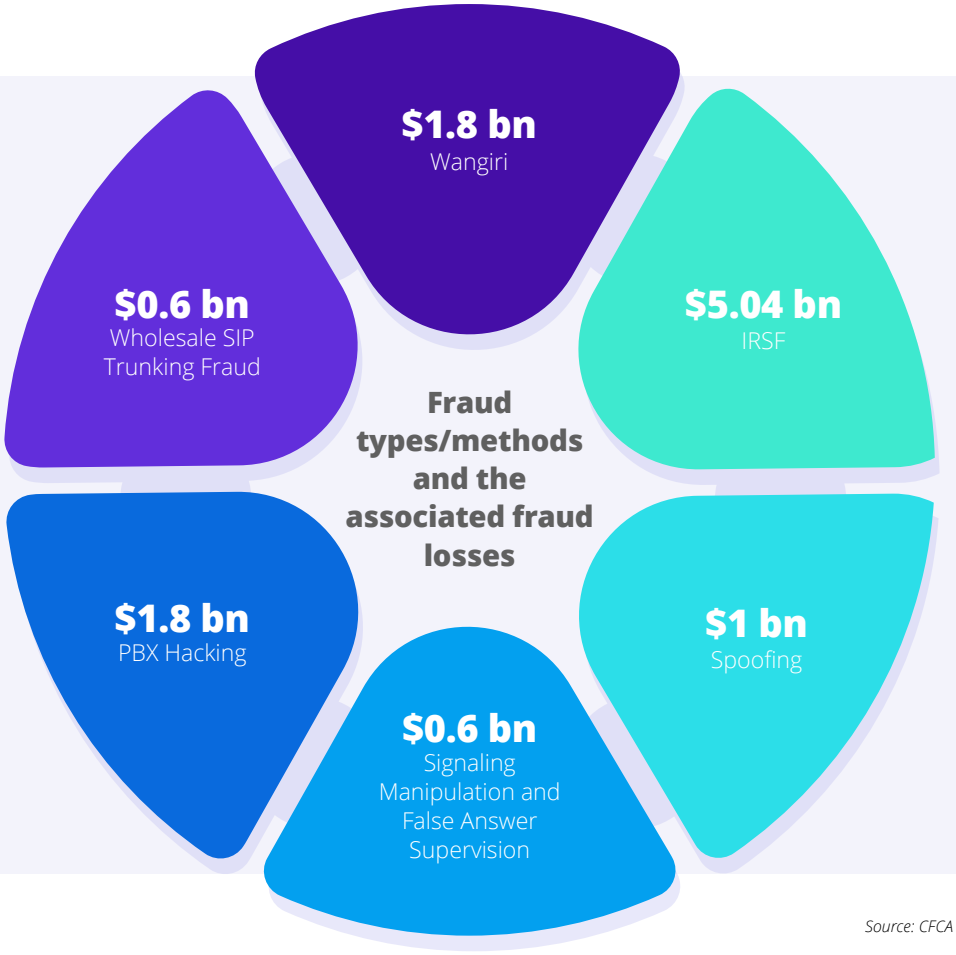
False Answer Supervision

In this, the fraudulent carrier, instead of terminating the call, would route it to a recorded message that then plays a ringing tone followed by a recording. The fraudsters use FAS to make these calls appear as completed calls which would be further billed.

Wholesale SIP Trunking Fraud

In this scenario, the fraudster makes money by selling wholesale trunking services, using stolen credentials to terminate the calls.

The below diagram provides the fraud losses associated with some of the fraud types/methods mentioned above.



Source: CFCA Fraud Loss Survey 2019

Given the widespread SIP usage and the varied types of SIP fraudulent attacks and its direct and indirect repercussions, securing this protocol is very important.

In fact, one new area of focus within the GSMA Fraud and Security Group (FASG) has been the Session Initiation Protocol (SIP). The new GSMA's FS.38 SIP Network Security permanent reference document (PRD) aims to highlight how vulnerable SIP is to different types of attacks and outlines potential SIP based security, privacy, and fraud attacks against fixed, mobile and fixed-mobile converged (FMC) networks and their customers, as well as describing countermeasures for those attacks. All of this points towards one thing: it is of pressing priority to secure the communication via SIP at the earliest.

The Way Forward:

It is now more than ever that the SIP needs to be seen as a significant threat vector and be included within threat analysis for all relevant fixed and mobile networks, including 5G. We believe the robust and defense mechanism that abides by the recommendations provided by the industry bodies, that goes beyond the SBCs and the firewalls to protect your network is the need of the hour. The way forward for the CSPs should be to look at incorporating a proactive approach that makes use of a multi-tier strategy that combines the real-time threat intelligence, pre-configured heuristics, leverage Deep Packet Inspection (DPI) techniques along with machine learning capabilities to proactively tear down the call in a particular state of the call thus stopping the fraud before it happens. As it is said, ***"An ounce of prevention is worth a pound of cure."***

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, Varthur Hobli,
Bengaluru560103 India

Tel: +91 80 6659 8700
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