Review Article

Open Access CrossMark

A study on internet bypass fraud: national security threat

Volume 7 Issue 1 - 2019

Kala N
Assistant Professor &Director, Centre for Cyber Forensics and Information Security, University of Madras, India

Correspondence: Kala N, Assistant Professor &Director, Centre for Cyber Forensics and Information Security, University of Madras, Chennai- 600 005, India, Email kalabaskar@gmail.com

Received: October 25, 2018 | **Published:** February 06, 2019

Abstract

Internet bypass fraud is one of the most complicated fraud types in the recent times. Telecom regulators and mobile operators face a staggering revenue loss since bypass fraud is proving to be the most prolific and costly frauds. The gateway equipments such as fixed, Voice over Internet Protocol(VoIP), Global System for Mobile communication(GSM), Code Division Multiple Access (CDMA), VOIP to GSM, fixed line gateway are used to terminate international inbound calls to local subscribers by deviating traffic away from legal interconnect gateways. Operators sending outbound international traffic connect to interconnect operators with lower rates, leading to termination of network operator's loss of revenue. Bypass fraud is considered illegal since those who undertake it are not licensed to provide telecommunication services. Bypass fraud is also considered as a national security threat since terrorist groups use this device to make calls which appears to be a local call. This paper focuses on the study of bypass fraud as a National security threat. Further this study also suggests the methods for mitigating such security threat.

Introduction

What is Bypass fraud?

A call via a legitimate path/route will be bypassed so that there is a revenue loss.[1] Generally for making national or international calls, rates are fixed by regulators in a country or by an individual or group of operators. Bypass fraud is prevalent in countries where there is a difference in rates between the retail calling, national calling and international calling. Moreover in some countries, international gateways are monopolized by government operators. The fraudsters make use of difference in rates and ensure that there are enough profits for them and serve as the key motivating factor to invest in procuring the equipments and GSM connections for conducting a large scale Bypass fraud. In countries where the international to national terminating charge margins are low, nil or negative, the bypass fraud either does not exists or is conducted a very low scale. It is one of the latest and most severe threats to a telecom operator's revenue. It is an unauthorized exploitation or manipulation of an operator's network. This can happen in two ways:

i. SIM Box Interconnect Fraud

ii. GSM Gateway Fraud

Such methods make fraudsters gain incentives to evade such high tariff interconnects and deliver costly international calls illicitly. Fraudsters use Voice over Protocol – Global System for Mobile Communications (VOIP-GSM) gateways also called as "SIM Boxes", which are used to receive incoming calls (via wired connections) and deliver them to a cellular voice network. It appears as if it is through a local call appearing from a customer's phone. This practice not only dramatically degrades the network experience for legitimate customers violating the telecommunication laws in many countries but also extremely profitable for simboxers/fraudsters resulting in revenue loss significantly.[2]

Cellular networks

Commonly used standard for implementing cellular communication is a set of Global System for Mobile Communication (GSM). Majority of countries such as United States, Europe, Africa and Asia use GSM for mobile communication and is popularly called as 2G cellular networks and subsequently evolved into Universal Mobile Telecommunications Service (UMTS-3G) and Long Term Evolution(LTE-4G). A smart card called Subscriber Identity Module (SIM) is being used by GSM and it manages the SIM card that carries the identity and placed on any device authorized to operate on a carrier's. Every communication transaction in network is cryptographically authenticated. SIM cloning was prevalent in the recent past which negated guarantee of specific SIM card attribution. Latest advanced technology SIM cards have hardware security and practical key recovery protections that prevents card cloning. Additionally, GSM standards uses audio codec called GSM Full-Rate (GSM-FR) which is also frequently implemented in Voice over Internet Protocol (VOIP) software.[3]

Voice over internet protocol

Voice over Internet Protocol (Voice over IP, VoIP and IP telephony) is a methodology and group of technologies for the delivery of voice communications and multimedia sessions over Internet Protocol (IP) networks, such as the Internet. The terms Internet telephony, broadband telephony, and broadband phone service specifically refer to the provisioning of communications services (voice, fax, SMS, voice-messaging) over the public Internet, rather than via the public switched telephone network (PSTN). There are two ways in which clients can complete a VoIP call. Firstly, a call can be completed exclusively using internet; secondly calls might also be routed from/to a VoIP client to a Public Switching Telephone Network (PSTN) through a VoIP gateway. The transport is similar to traditional telephony network. It uses special media codec's protocol to encode audio and video. Popular VoIP providers are Skype, Vonage and Google which uses both IP-only and IP-PSTN calls. Step by step process for a VoIP is given below:

i. VoIP calls are setup using text based protocol called as Session Initiation Protocol (SIP).

ii. SIP function is to establish which audio codec will be used for the call.

iii. Once a call connection has been established audio flows between the callers

iv. It uses Realtime Transport protocol (RTP) for this purpose

v. This is typically carried over User Datagram Protocol (UDP)

vi. There are many codec's are mandatory, although some are optional.

vii. When GSM-FR is implemented outside of cellular network and sometimes used by VoIP software.

Simbox

Simbox is a device used as part of a VoIP gateway installation. It contains a number of SIM cards, which are linked to the gateway but housed and stored separately from it. A SIM box can have SIM cards of different mobile operators installed, permitting it to operate with several GSM gateways located in different places. The SIM box operator can route international calls through the VoIP connection and connect the call as local traffic, allowing the box's operator to bypass international rates and often undercut prices charged by local mobile network operator's that connects VoIP calls to GSM voice network. It does not use data network. Simbox device requires one or more SIM cards to wirelessly connect VoIP call to GSM network. A Simbox acts as a VoIP client whose audio input and output are connected to a Mobile Phone. These devices have strong market in private enterprise telephone networks. Such private enterprise use GSM gateways with the permission of the licensed telecommunications provider and this causes to tariff reduction enabling them to pay often at lower cost for terminating a call. However, this is possible and legal only for domestic calls. It is enabled by Voice over Internet Protocol (VOIP) Global System for Mobile Communication (GSM). The equipment is called SIM Boxes and the same is illustrated in Figure 1. In this process Simboxing connects the VOIP calls to a local cellular voice network through a collection of SIM cards and cellular radios. In a normal course the calls will be received by the network service provider and call tariffs will be charged. In Simboxing, calls will bypass the normal course of connection, appearing to originate from customer phone, to a network provider. The calls are delivered at a subsidized domestic rate instead or international rate. Such an activity has its negative impact availability, reliability and quality of service for legitimate consumers. Moreover, it also creates network hotspots by injecting huge volume of tunneled calls, thereby causing revenue loss to network operators.

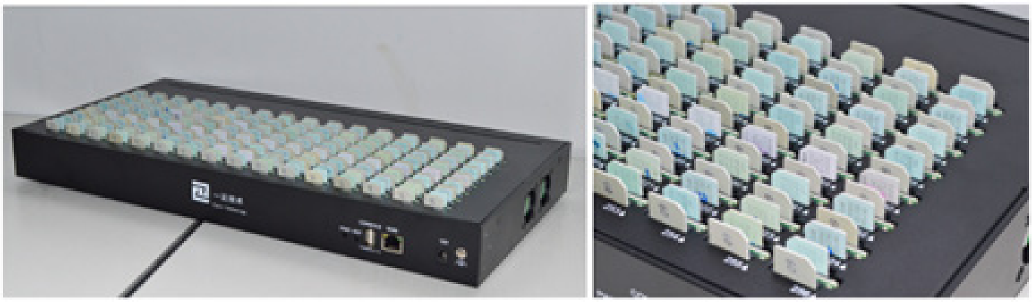

Figure 1 Simbox.

Interconnect bypass fraud using simboxing

Most common implementation of interconnect bypass fraud[4] is known as SIM Boxing. Fraudsters use simbox bypass the international calls and make it appear as if it is a domestic call causing revenue loss to telecom operators. There is a high demand for GSM-VoIP gateways spanning a wide range of features; numbers of concurrent calls are supported. Some of them have only limited functionality, while others hold several simcards and also supports a variety of audio codecs in a "SIM server". Sometimes one or more radio interfaces calls using the "Virtual SIM cards" from the server. This prevents location based fraud detection. Miscreants, utilize this and commits the fraud. The cost of simbox equipment goes upto 200,000 USD. A typical international call which is routed through a regulated licensed interconnect is illustrated in the Figure 2. Let us assume client A is located in India and client B is located in UK. In a typical call, when client A is calling client B, the call is routed through the telephone network in India (labeled as "Foreign PSTN core") to an interconnect between client A and client B network in UK. This passes through client B's domestic network (labeled as "Domestic PSTN Core") and communication establishes between client A and client B. If client A and client B are not in neighboring countries, there can be many interconnects and intermediary networks. This is very critical the connections are heavily monitored for billing purpose and quality. It can be seen that VoIP calls initiated from services such as Skype that terminates on a mobile phone also passes through regulated interconnect. A Simbox call is represented in Figure 3. A Simboxed international call avoids regulated interconnect by routing the call to a Simbox which completes the call using the local cellular network. In a simbox case, client A call is routed through domestic network, but instead of passing through the regulated interconnect, the call is routed over internet protocol (VoIP) to simbox in the destination country. In doing so, the simbox places a separate call on the cellular network in the destination country, then routes the audio from IP call into the cellular call, which is routed to client B through the domestic network. The same is illustrated in Figure 3. The main disadvantage here is neither of end users is aware that the call is being routed through a simbox. This causes a contractual breach of trust between two Internet Service Providers (ISPs) who have agreed to route traffic between their networks. The intermediaries own profit from reduced prices. Two types of attack can take place. Firstly, hijacking of international call; secondly, hijacking and re-injecting of an international call. First type has been described above. In the second type, Simboxes re-inject telecom voice traffic into the mobile network masked as mobile customers and operator has to pay for the re-injected calls.[5] In general there are three types of routes that are used in communication networks. They are:

i. **White Route**: both source and destination have legal termination.

ii. **Black Route:** both source and destination have illegal termination.

iii. **Grey Route:** the termination is legal for one entity or country, but illegal for the other end.

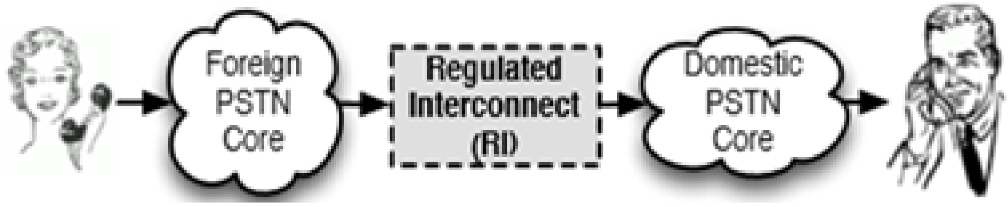

Figure 2 Typical international call routed through regulated licensed interconnect.[4]

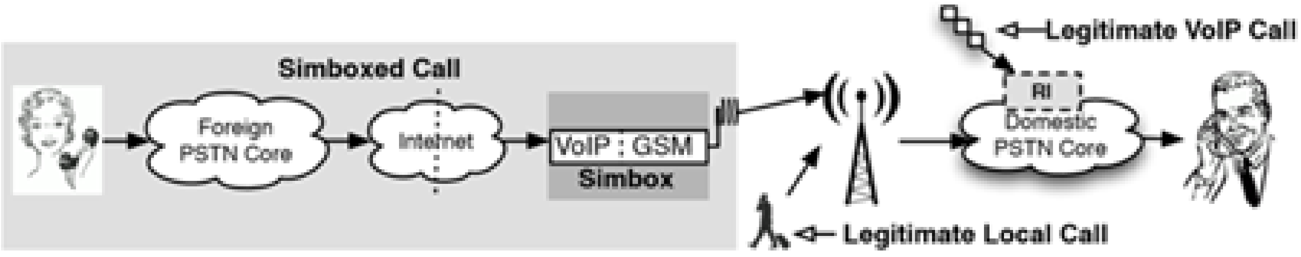

Figure 3 A Sim box international call.[4]

GSM gateway interconnect devices

Interconnect systems, such as gateways, allows voice interoperability between otherwise incompatible radio communications systems. Interoperability is achieved by retransmitting voice over interconnected radio subscriber both mobile as well as portable units. Linking incompatible radio frequency bands and systems can be relatively easy and effective. Interconnect deployment requires a new strategy and operational procedures. The gateway approach to interoperability has significant potential, considering the ease of gateway deployment and relatively low cost when compared to wide area radio system. A gateway is a type of interconnect system. They can also connect trunked talk groups, encrypted networks, public telephone systems, and cellular or satellite phone connections. Most gateway devices are mobile and portable, but many are used in permanent configurations.[6]

Interconnect bypass fraud global scenario

According to a survey conducted by Communication Fraud Control Association (CFCA), in the year 2015, the revenue loss amounts to $3.77 Billion USD. According to this survey, top 10 countries where the fraudulent calls originated, is listed in Table 1. Further survey points out the percentage of top five frauds, in which interconnect Bypass fraud in network is around 5%, whereas in roaming status, interconnect bypass fraud amounts between 20 – 25%. This can be seen evidently from the following Figure 4. Authorities in US say that the hackers were involved in an international crime ring that scammed telecommunication companies out of an estimated $50million USD in last few years. FBI most wanted list of cyber criminals have been arrested by authorities in their native Pakistan. Serbian Police cracks down on illegal SIM Box Scheme. According to Serbia's interior Ministry in cooperation with the special department of cyber crime of Prosecutor's Office and the Ministry of Interior Macedonia have identified miscreats using Simboxes to bypass international communications via VoIP and making low-cost calls in Serbia. More than 40,000 SIM cards were found in Macedonia of mobile operators from Serbia, Croatia, Slovenia, Albania, Bosnia and Herzegovina. There are incidents in Ghana where the fraudsters connived with partners abroad to route internet calls via VoIP to make it appear as if the call is a local one. Even. The seized Simcards and connecting devices are illustrated in Figure 5. There has been incidence where even women have been arrested for alleged simbox fraud.[7]

Table 1 Country wise fraudulent calls in percentage based on call origin.

Countries	Fraudulent calls percentage
United states	5%
Pakistan	4%
Spain	4%
Cuba	3%
Italy	3%
Philippines	3%
Somalia	3%
United Kingdom	2%
Dominican Republic	1%
Egypt	1%

Figure 4 Seized sim cards and simbox.

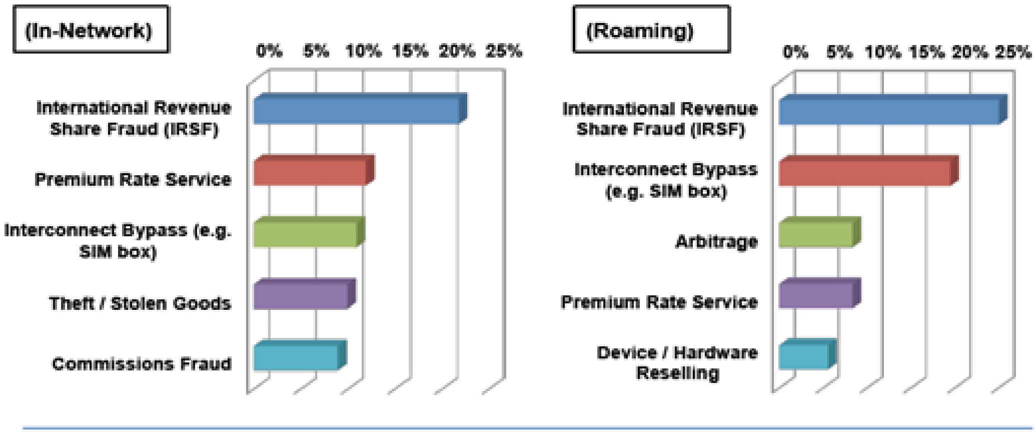

Figure 5 Percentage comparison of Simbox fraud in network vs. roaming.[5]

Interconnect bypass fraud Indian scenario

Recently, in India, a techie has been arrested for operating telephone exchange for a Pakistan spy. According to the sources the Uttar Pradesh[8] Anti-Terrorism squad have busted an illegal telephone exchange and spying racket causing national security threat. This act has been committed by a software engineer from south Delhi and ten others from Lucknow and other parts of UP. The exchanges were not only making lakhs of rupees by routing international calls bypassing the legal gateways. These systems were used for Pakistan's Inter-Service Intelligence (ISI) to call Army officials to elicit information from them. The racket was busted after the defence ministry and Army alerted the military intelligence in Jammu & Kashmir. ISI has been spying over and innocent victims have been sharing information. Intelligence officials unearthed the racket and found illegal network was using Simbox to carry out their spying activities. The callers based in Pakistan, Bangladesh made calls using VoIP through Simbox and connected to receivers in India. The receivers in India could only see Indian numbers on their phone screens. The law enforcement authorities have recovered 16 SIM BOX units, 140 prepaid cards, 10 mobile phone and 28 data cards and five laptops. The SIM Box recovered from the suspects is illustrated in Figure 6.

Figure 6 Simbox recovered from Accused.[5]

Countermeasures for interconnect bypass fraud

Most common approaches to detect Bypass fraud are:

i. Bypass route detection through call generation

ii. Simbox detection using Fraud Management systems (FMS)

iii. Unusual flows and volumes

iv. Unusual called number spreads

v. A-typical traffic peaks for on-net traffic

vi. Many SIM card identities (IMSIs) to a single equipment identity (IMEI)

vii. Use of only one cell site

viii. An absence of SMS, data or roaming service use

Hybrid analysis: Call generation providers and FMS tools providers collaborate to pool their alerts in order to more efficiently detect the characteristics described above.

i. Network traffic analysis

ii. Call Data Record (CDR) Analysis

iii. Features extracted from CDR data are utilized to build a decision tree that can be used to distinguish between legitimate and Simbox accounts.

Features include: total number of outgoing calls, incoming calls, number of SMS originating and SMS terminating, total number of hand over and the total number of different location.[9]

Ammit

Simbox detection tool focuses on loss rate and simbox codec. Moreover, simbox detection based on measurable differences between true GSM and tunneled VoIP audio. Ammit is the first system to combat simboxing using call audio.[10]

Mocean simbox detector

The detection of Simbox tracks the calls based on caller line identification.[11]

Statistical profiling system

Identification based on monitoring complex call patterns including outgoing call count, distinct destinations ratio, cell sites used, incoming to outgoing call ratio and so on. It is also called statistical profiling based detection. Other type of detection mocean Simbox detector which has capabilities to distinguish between the normal international call traffic path and simbox bypass international traffic path.

Fraud management system (FMS)

FMS system includes the following detection systems:

i. Traffic analysis

ii. International Mobile Subscriber Identity (IMSI) number/ Integrated Circuit Card ID (ICCID) series analysis

iii. International Mobile Equipment Identity number.[12]

Conclusion

Telecommunication networks in developing nations rely upon the tariffs collected through regulated licensed interconnects in order to subsidize the cost of their deployment and operation. Fraudsters Bypass the legal connection and commit fraudulent activity using simboxes by tunneling traffic from VoIP connection into a genuine network unauthorized way. In this study an attempt has been made to identify the different ways interconnect bypass occurs. Further, this study has also identified the different devices used to commit such fraudulent activity. Moreover, a comparison between the current scenario from global perspective and Indian perspective has been made. Focus has been made to identify how the antisocial element and miscreants use such methodology and cause a national security threat across the globe. Finally, different fraud management systems that are currently in vogue have been discussed.[13]

Acknowledgments

None

Conflicts of interest

The author declares that there are no conflicts of interest.

References

1. Alphabet revenues rise 22% in Q4 marked by record contribution from Google Other, higher expenses. 2019.
2. Subex-telecom-fraud-alerts.
3. Telecom fraud - introduction, types & solutions.
4. Bradley Reaves. Boxed Out: Blocking Cellular Interconnect Bypass Fraud at the Network Edge. *24th USENIX Security Symposium*. 2015.
5. Ilona Murynets. Analysis and Detection of Simbox Fraud in Mobility Networks. 2015.
6. MOCEAN. SIM –Box Detector. 2015.
7. Woman arrested for alleged SIM Box fraud. 2016.
8. Uttar Pradesh ATS busts international call racket spying on Army units, 11 arrested. 2017.
9. Simbox product. 2015.
10. Fighting SIMBOX Fraud: We will root out simbox fraud in Ghana-Afriwave. 2015.
11. Techie Arrested For Operating a Telephone Exchange for Pakistan's Spy Agency in Delhi. 2016.
12. Mahmood A Khan, Syed Yasir Imtiaz, Mustafa Shakir. *Automatic Monitoring & Detection System (AMDS) for Grey Traffic*. Proceedings of the World Congress on Engineering and Computer Science 2015 Vol II WCECS. 2015.
13. Mueller's prosecutor tipped CNN off to armed FBI raid – Roger Stone's lawyer. 2019.

Citation: Kala N. A study on internet bypass fraud: national security threat. *Forensic Res Criminol Int J.* 2019;7(1):31‒35. DOI: 10.15406/frcij.2019.07.00262