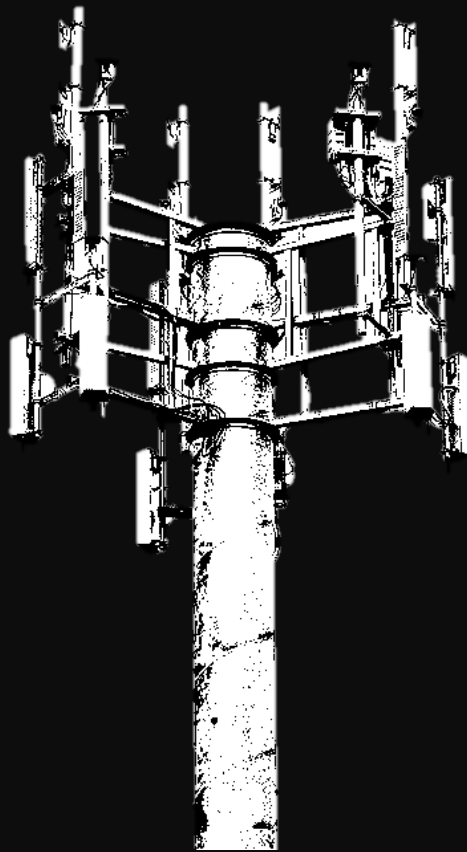


# Mobile Network Threats



Hassan Salloum

## Table of contents

1	SS7   Sigtran   GTP   Diameter .....	5
1.1	SS7 in PSTN network .....	5
1.1.1	SS7 protocol stack .....	5
1.2	SIGTRAN in IP Telephony network .....	6
1.2.1	SIGTRAN protocol stack .....	7
1.3	VOIP.....	8
1.3.1	VOIP Protocol Stack .....	8
1.4	SS7/Sigtran in GSM network .....	12
1.4.1	SS7/Sigtran protocol stack in GSM.....	12
1.4.2	GSM attachment .....	13
1.5	GTP in GPRS network .....	14
1.5.1	GPRS attachment and Activation .....	15
1.5.2	GPRS Tunneling Protocol .....	15
1.5.3	GTP protocol stack .....	15
1.5.4	GTP packet header .....	16
1.6	GTP in LTE network .....	16
1.6.1	GTP packet header .....	17
1.7	Diameter in LTE .....	18
1.7.1	Diameter base .....	19
1.7.2	Diameter application .....	19
1.7.3	Diameter message format .....	19
1.7.4	Diameter architecture.....	20
1.7.5	Diameter protocol stack .....	21
1.7.7	Summary.....	22
1.7.8	LTE attachment .....	23
2	GSM   GPRS   VOIP   VOLTE   LTE threats attack .....	24
2.1	GSM threat attacks.....	24
2.1.1	Attacker's profile.....	24
2.1.2	IMSI disclosure (Requesting MSC) .....	24
2.1.3	Subscriber Profile Manipulation (Send fake subscriber profile to VLR) .....	25
2.1.4	Cell Level Tracking using MAP's anyTimeInterrogation (ATI) service .....	25
2.1.5	Cell Level Tracking using MAP's SendRoutingInfoForSM (Fake SMSC) .....	26
2.1.6	Denial of Service (Fake MSC) .....	27
2.1.7	DOS call (using numerous roaming number requests) .....	28
2.1.8	USSD Request Manipulation .....	28

2.1.9	HLR Stealing Subscribers (Roaming scenario)	29
2.1.10	Hybrid Attacks: TMSI De-anonymization	30
2.1.10.1	Hybrid Attacks: Intercept Calls	30
2.1.11	Intercepting outgoing calls	31
2.1.12	Redirecting incoming calls	31
2.1.13	SMS intercept (using Fake MSC)	32
2.1.14	Intercepting calls with CAMEL (Roaming scenario)	33
2.1.15	SPAM Message in mobile network	35
2.2	GPRS threats attack	36
2.2.1	Searching for mobile operator's facilities on the Internet	36
2.2.2	IMSI brute force	37
2.2.3	The disclosure of subscriber's data via IMSI	38
2.2.4	Disconnection of authorized subscribers from the Internet	39
2.2.5	Blocking the connection to the Internet	40
2.2.6	Internet at the expense of others	41
2.2.7	Data interception (Using a spoofed GSN addresses to SGSN and GGSN)	42
2.2.8	DNS tunneling	43
2.2.9	Substitution of DNS for GGSN	44
2.3	VOIP Threats attack	45
2.3.1	VOIP attack: DOS	48
2.3.2	VOIP attack: Eavesdropping	50
2.3.3	VOIP attack: SIP attacks	51
2.3.4	VOIP attack: SIP registration hijacking	51
2.3.5	VOIP attack: Spam over Internet Telephony	52
2.3.6	VOIP attack: Embedding malware	52
2.3.7	VOIP attack: Viproy test kit	53
2.4	LTE threats attack	54
2.4.1	IMSI Catching active and passive attack	54
2.4.2	Location tracking	55
2.4.3	RF and Low Power Smart Jamming	55
2.4.4	Rogue eNodeB	56
2.4.5	DoS and DDoS Attacks	57
2.4.5.1	Botnet Launched DDoS Attack	57
2.4.5.2	Soft Downgrade to Non-LTE Services	57
2.4.5.3	Denying All Network Services	58
2.4.6	HSS Overload	58
2.4.7	SGW Saturation	59

2.4.8 Signaling Amplification Attacks .....	59
2.4.9 Insider Attack .....	60
2.5 VOLTE threats attack .....	61
2.5.1 VOLTE architecture .....	61
2.5.2 VOLTE attachement .....	61
References .....	63

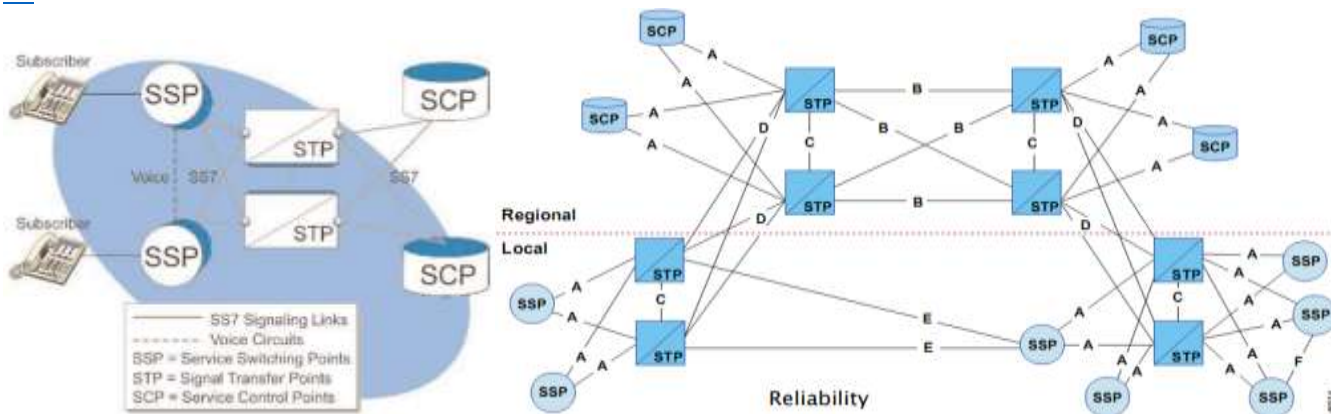
## 1 SS7 | Sigtran | GTP | Diameter

### 1.1 SS7 in PSTN network

Signaling System 7 (SS7) is an international telecommunication protocol standard that defines how the network elements in a public switched telephone network ([PSTN](#)) exchange information and control signals. Nodes in an SS7 network are called *signaling points*.

It is the system that controls how telephone calls are routed and billed, and it enables advanced calling features and Short Message Service (SMS). It may also be called Signalling System No. 7, Signaling System No. 7 or -- in the United States -- Common Channel Signaling System 7, or CCSS7.

SS7 was first adopted as an international standard in 1988, and the latest revision of the standard was in 1993. It is still the current standard for telephone calls and is in use for both [landline](#) and mobile phone service all the way up to and including [5G](#).

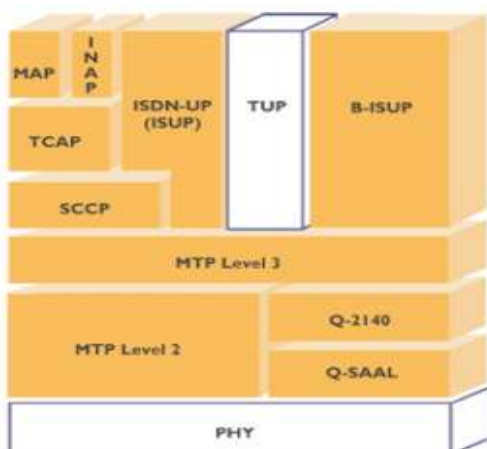


**Service Switching Points (SSP)** are the telephone “switches” that are interconnected to each other by SS7 links. The SSPs perform call processing on calls that originate, tandem, or terminate at that site.

**Signal Transfer Points (STP)** are “routers” that relay messages between network switches and databases. Their main function is to route SS7 messages to the correct outgoing signaling link, based on information contained in the SS7 message address fields.

**Service Control Points (SCP)** contains centralized network databases for providing enhanced services. Examples of services include toll-free numbers and prepaid subscriptions.

#### 1.1.1 SS7 protocol stack



**MTP** (Message Transfer Part) Layers 1-3: lower level functionality at the Physical, Data Link and Network Level. They serve as a signaling transfer point, and support multiple congestion priority, message discrimination, distribution and routing.

**ISUP** (Integrated Services Digital Network User Part): network side protocol for the signaling functions required to support voice, data, text and video services in ISDN. ISUP supports the call control function for the control of analog or digital circuit switched network connections carrying voice or data traffic.

**SCCP** (Signaling Control Connection Part): supports higher protocol layers such as TCAP with an array of data transfer services including connection-less and connection oriented services. SCCP supports global title translation (routing based on directory number or application title rather than point codes), and ensures reliable data transfer independent of the underlying hardware.

**TCAP** (Transaction Capabilities Application Part): provides the signaling function for communication with network databases. TCAP provides non-circuit transaction based information exchange between network entities.

**MAP** (Mobile Application Part): provides inter-system connectivity between wireless systems, and was specifically developed as part of the GSM standard.

**INAP** (Intelligent Network Application Part): runs on top of TCAP and provides high-level services interacting with SSP, SCP and SDP in an SS7 network.

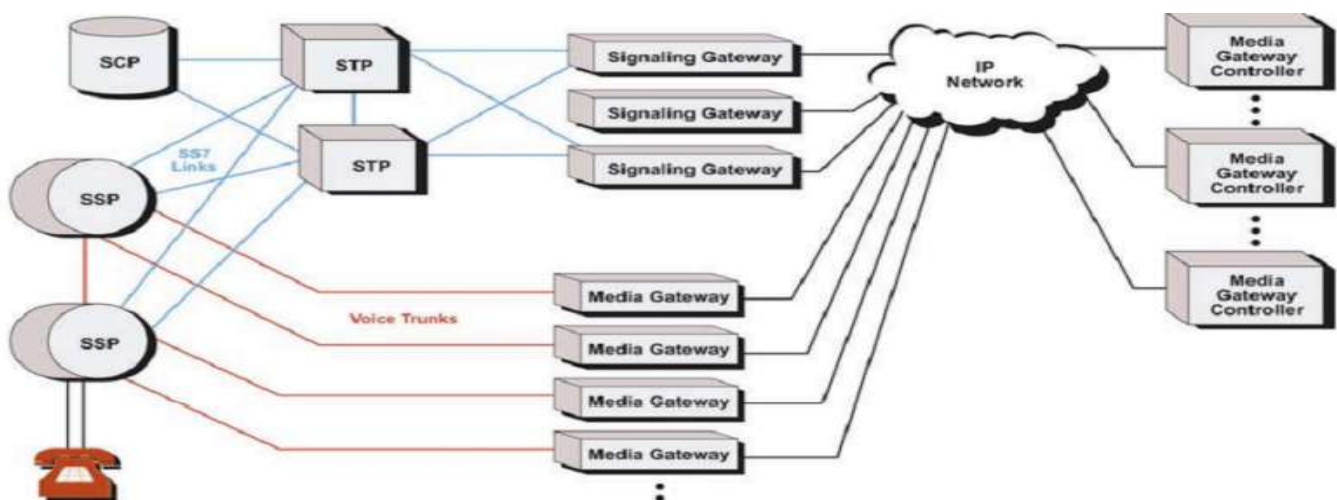
## 1.2 SIGTRAN in IP Telephony network

IP telephony has to do mainly with digital telephony systems (LAN based IP PBX systems) which use the IP protocol entirely for voice communication.

All components of the IP telephony system use digitized voice which is transferred as IP packets through an IP network (usually the LAN network).

The call control system is usually a software based (softswitch) server or even a [hardware device like the Cisco Call Manager Express](#), which handles all call signaling, call routing, IP phone management etc, again using IP protocol for transport. So think about IP telephony as a bigger concept compared to VoIP.

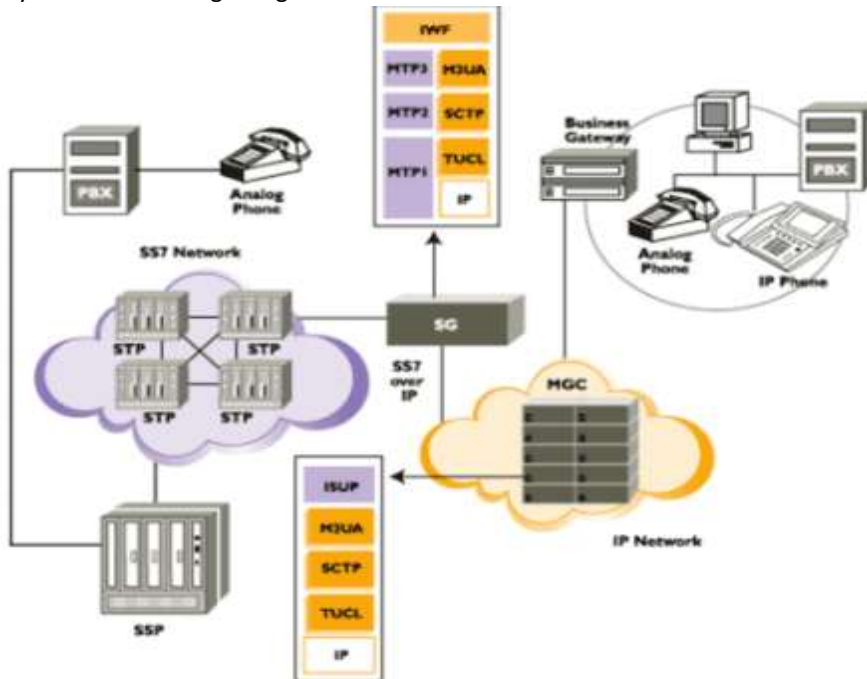
IP Telephony is the overall concept of the modern form of voice communication which harnesses the power and features of VoIP technology in order to offer the overall experience of communicating effectively and with lots of extra features.



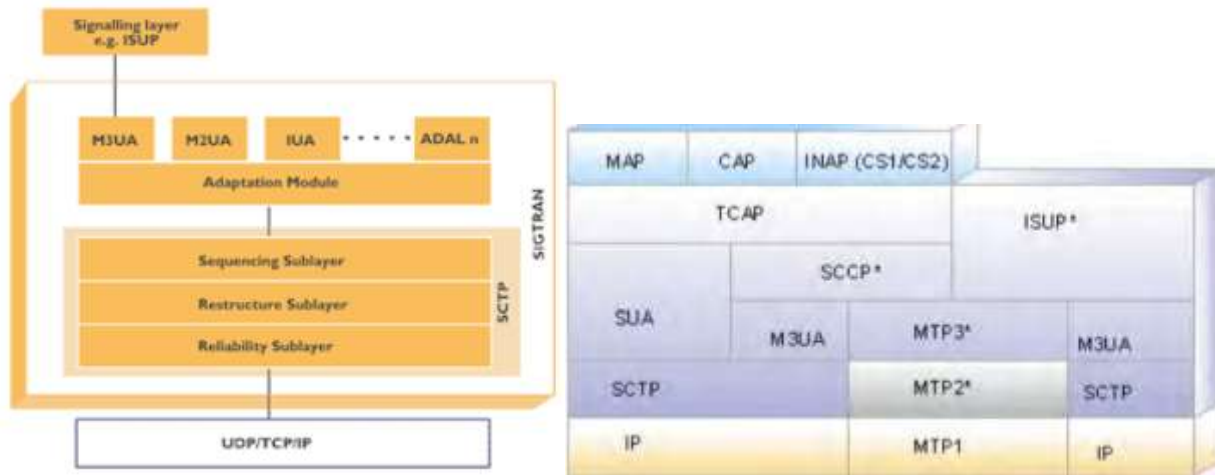
**Media Gateway (MGW)** terminates voice calls on inter-switch trunks from the PSTN, compresses and packetizes the voice data, and delivers voice packets to the IP network. For ISDN calls from the PSTN, Q.931 signaling information is transported from the MGW to the media gateway controller for call processing.

**Media Gateway Controller (MGC)** handles the registration and management of resources at the media gateways. An MGC exchanges ISUP messages with CO switches via a signaling gateway. Sometimes called a softswitch.

**Signaling Gateway (SGW)** provides transparent interworking of signaling between switched circuit and IP networks. The SGW may terminate SS7 signaling



## 1.2.1 SIGTRAN protocol stack



The SIGTRAN protocols specify the means by which SS7 messages can be reliably transported over IP networks.

The architecture identifies two components: a common transport protocol for the SS7 protocol layer being carried and an adaptation module to emulate lower layers of the protocol. For example:

- ♣ If the native protocol is MTP (Message Transport Layer) Level 3, the SIGTRAN protocols provide the equivalent functionality of MTP Level 2.
- ♣ If the native protocol is ISUP or SCCP, the SIGTRAN protocols provide the same functionality as MTP Levels 2 and 3.
- ♣ If the native protocol is TCAP, the SIGTRAN protocols provide the functionality of SCCP (connectionless classes) and MTP Levels 2 and 3.

## 1.3 VOIP

The telephone handsets (VoIP phones) translate the analogue voice signal into digital voice (binary voice) which is transferred as IP packets from one phone to another.

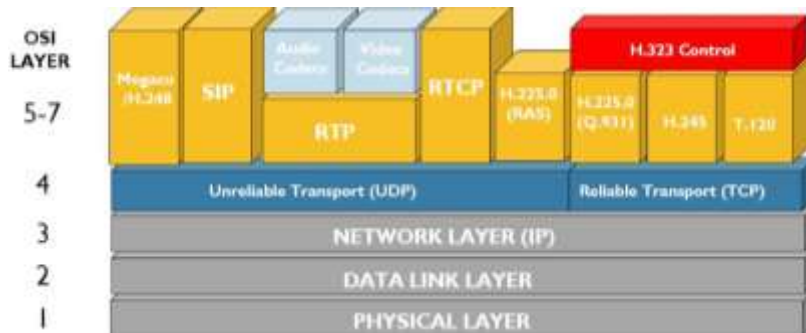
VoIP on the other hand is a subset of IP Telephony. Basically, VoIP is the technology which is used by IP Telephony as the vehicle to transport phone calls.

VoIP is the technology in which the analogue voice signal is digitized (analog to digital conversion) and becomes binary numbers in order to be transferred by the IP protocol.

VoIP is the basis for the implementation and functionality of an IP Telephony system. VoIP can also be used by legacy TDM based PBX systems to transport voice calls over an IP WAN network or even over the Internet.

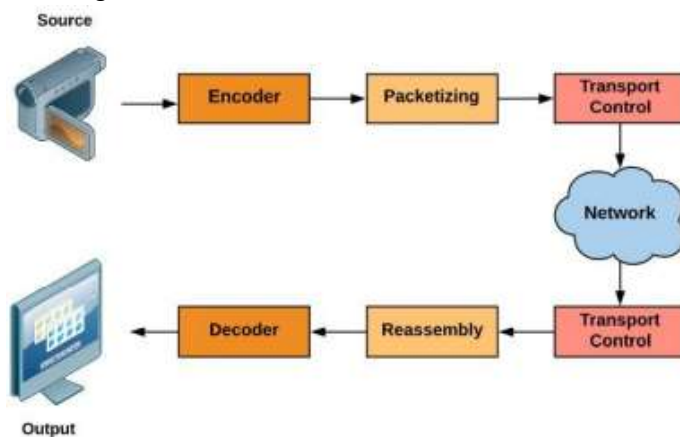
Special voice gateways are used to connect to the legacy PBX telephone system on one end and to the IP network on the other end in order to translate the TDM voice stream into IP voice packets.

### 1.3.1 VOIP Protocol Stack



❖ **Real-time Protocol (RTP)** is a transport protocol, specifically over UDP, based on RFC 3550. It is used in real-time multimedia applications and in end-to-end real-time data stream transfer. In order to achieve that, a video, for example, goes through a number of steps:

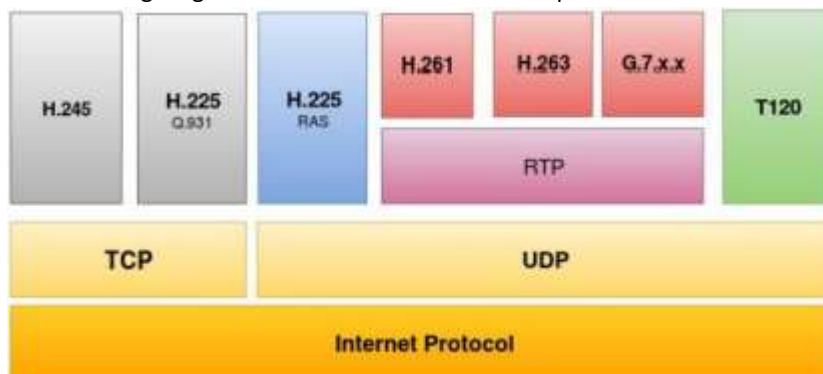
- Encoding
- Packetizing
- Transport Control
- Reassembly
- Decoding





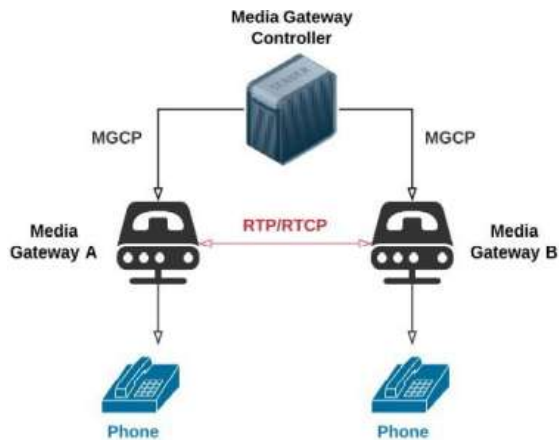
- ❖ Although RTP is specified to carry the media stream, there is another protocol that works with RTP called **Real-time Control Protocol (RTCP)**. This protocol works side by side with RTP to monitor transmissions and assure Quality of Service (QoS). The aim of RTCP is checking whether there is packet loss during the process.
- ❖ **H.323** is a data over IP standard introduced by the International Telecommunication Union Standardization Sector (ITU-T). As you can see, this standardization body uses letters to define the scope based on many criteria, listed here:
  - H: For audiovisual and multimedia systems
  - G: For transmission systems and media
  - Q: For switching and signaling
  - T: For terminals for telematic services
- H.323 is one of the oldest packet-based communication systems protocols. Thus, this protocol is stable. The current version is v6. It is well used by many vendors in many products, such as Cisco call manager, NetMeeting, and RadVision.
- H.323 uses many types of devices:
  - Terminals: These are user devices such as IP phones and videoconferencing systems.
  - Multipoint control units: These are composed of two logical components— the Multipoint Controller (MC) and the Multipoint Processor (MP). Their role is managing multipoint conferences.
  - Gatekeeper: This is optional. Gatekeepers provide some additional services such as user authentication and address resolution.
- The H.323 stack is based on the following components:
  - IPv4 network layer
  - User datagram protocol layer
  - Real-time protocol
  - Signaling protocols
  - Pre-call setup
  - Video codecs
  - Audio codecs
  - Data

- The following diagram illustrates the different components of the H.323 stack



- ❖ **Media Gateway Control Protocol (MGCP)** is a protocol developed by Cisco. The goal of MGCP is to handle signals and session management. It is a communication mechanism between media gateway controllers and media gateways. Thus, the control is centralized.

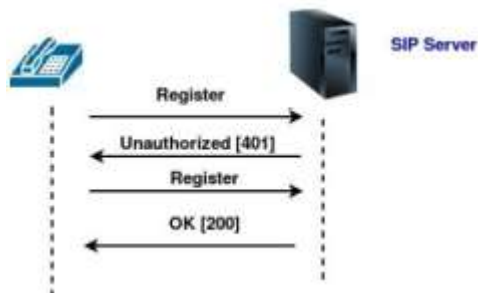
In other words, the controller communicates with many media gateways. The controller also supervises terminals and registers the new ones in its zone. H.248 is also like H.323, an ITU-based protocol. It is an enhanced version of MGCP. As you can see in the diagram, MGCP is a master-slave protocol:



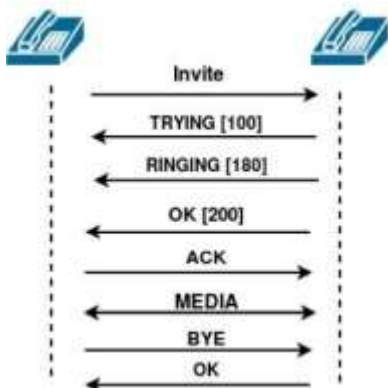
❖ **Session Initiation Protocol (SIP)** is a session management protocol based on the RFC 3261 protocol. It works on both UDP and TCP, and it also supports TLS. It is more scalable than H323. SIP handles calls in the following five steps:

- User location
- User availability
- User capability
- Session set up
- Session management

▪ To start a SIP operation, a registration is needed by the user:



▪ The following diagram describes the steps required to establish a connection between two user agent clients:



▪ SIP requests are similar to HTTP requests. They are in the following format:

METHOD URI SIP/X.X  
HEADER: XXX

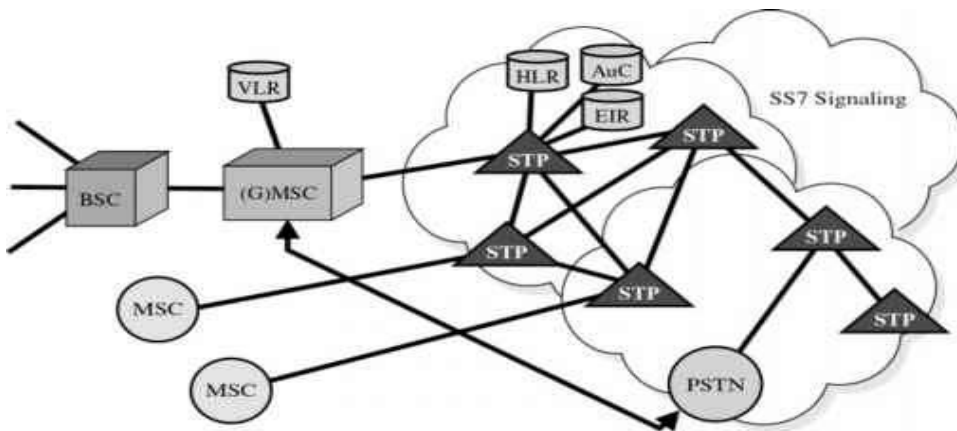
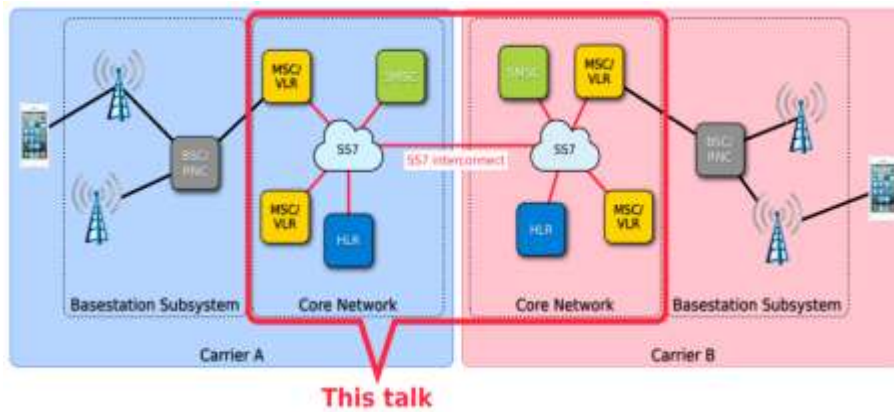
▪ Here, the method is the request type, and we have the following six methods:

- Register

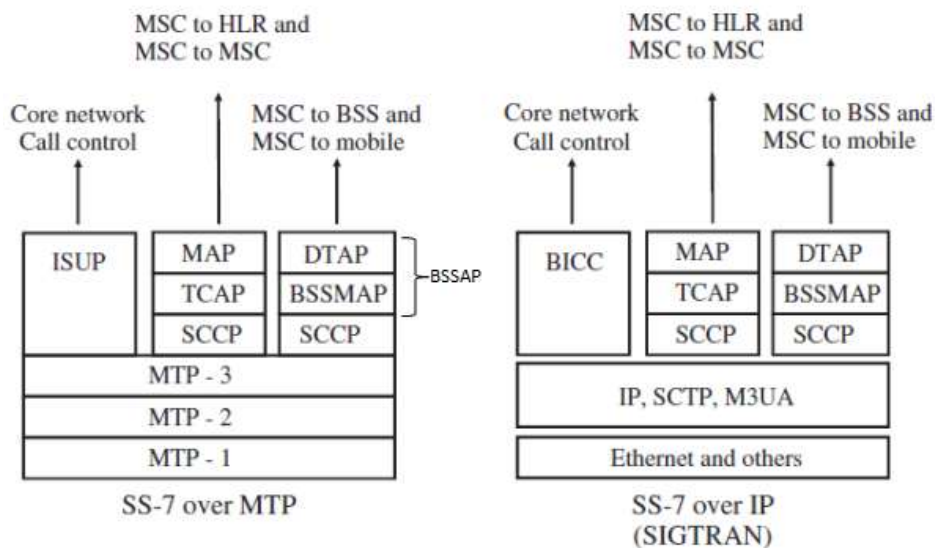
- Invite
  - ACK
  - Cancel
  - Options
  - Bye
- 
- SIP reply requests require this format:
    - SIP/X.X description
    - Header: XXX
    - URI: The file identification
    - SIP/X.X: SIP version
    - Header: This contains the information about the receiver (To, From, Call-ID are some of the SIP header fields)
- 
- Following are the possible status codes:
    - 1xx: Informational
    - 2xx: Success
    - 3xx: Redirection
    - 4xx: Failure
    - 5xx: Server error
    - 6xx: Global failure

## 1.4 SS7/Sigtran in GSM network

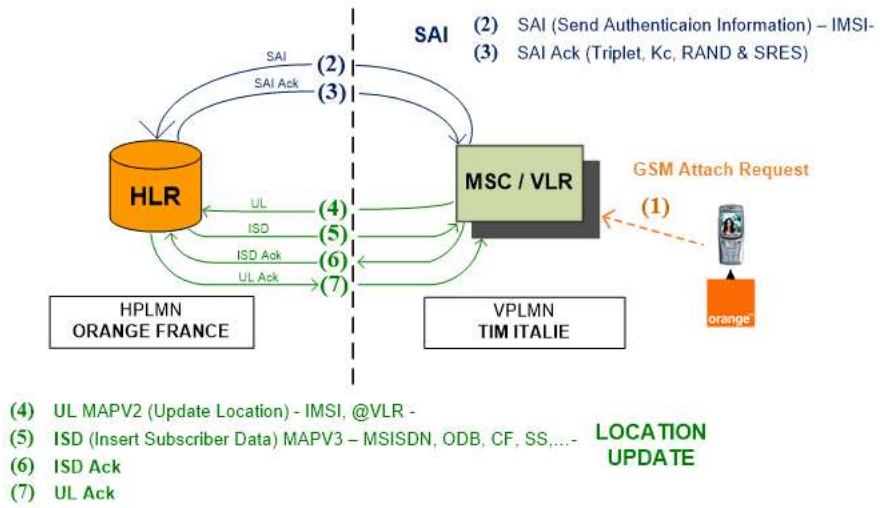
The MSC is the Central Switching function of the [GSM network](#). The MSC is connected to a SS7 network for the purpose of signaling and performing database queries



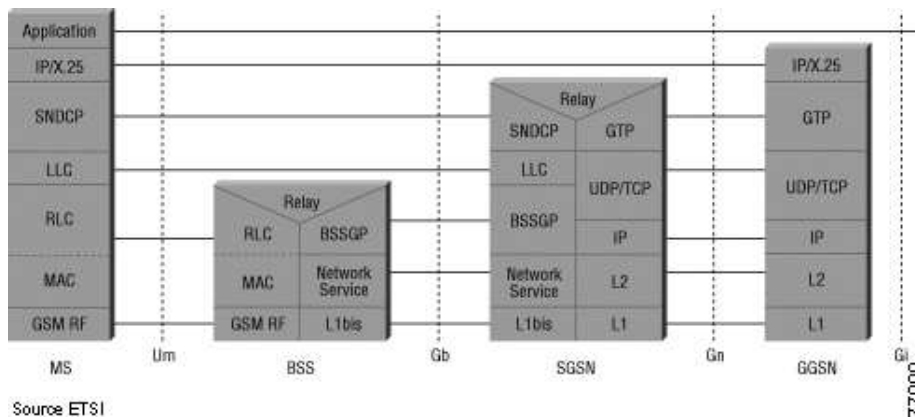
### 1.4.1 SS7/Sigtran protocol stack in GSM



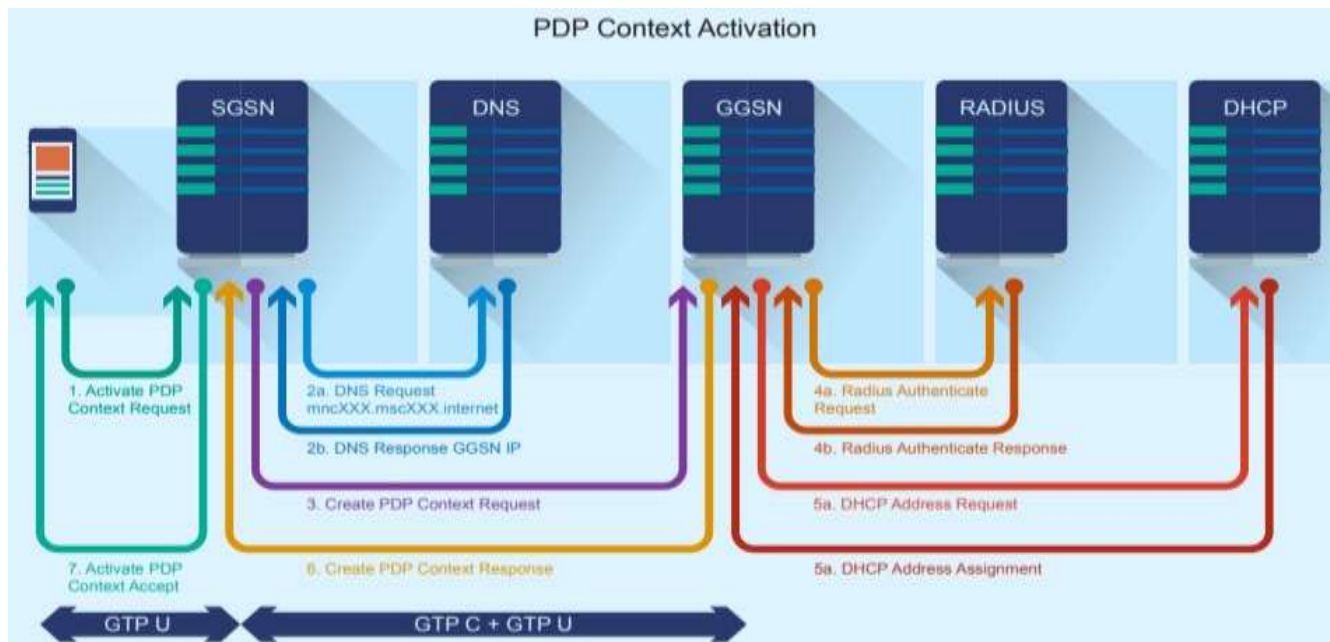
## 1.4.2 GSM attachment



## 1.5 GTP in GPRS network



- How communication work between SGSN and GGSN

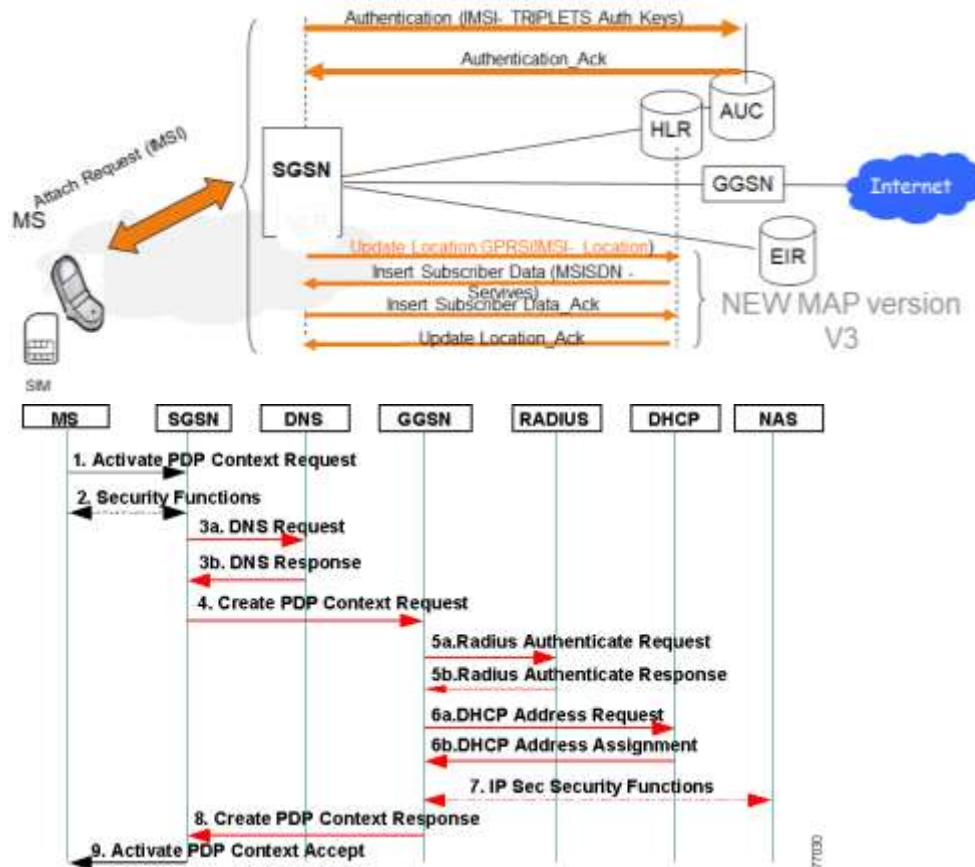


GTP uses tunnels to allow two GPRS support nodes (GSNs) to communicate over a GTP-based interface and to separate traffic into different communication flows.

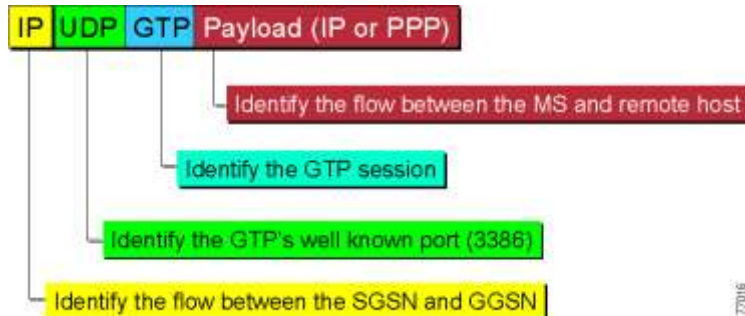
GTP creates, modifies, and deletes tunnels for transporting IP payloads between the user equipment, the GPRS support nodes (GSNs) in the GPRS backbone network and the internet.

GTP comprises three types of traffic—control plane (GTP-C), user plane (GTP-U), and charging (GTP' derived from GTP-C) traffic.

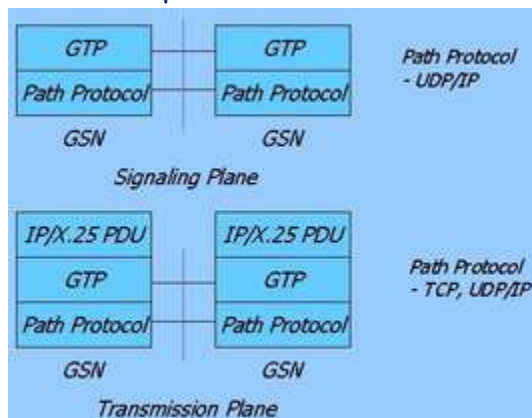
## 1.5.1 GPRS attachment and Activation



## 1.5.2 GPRS Tunneling Protocol

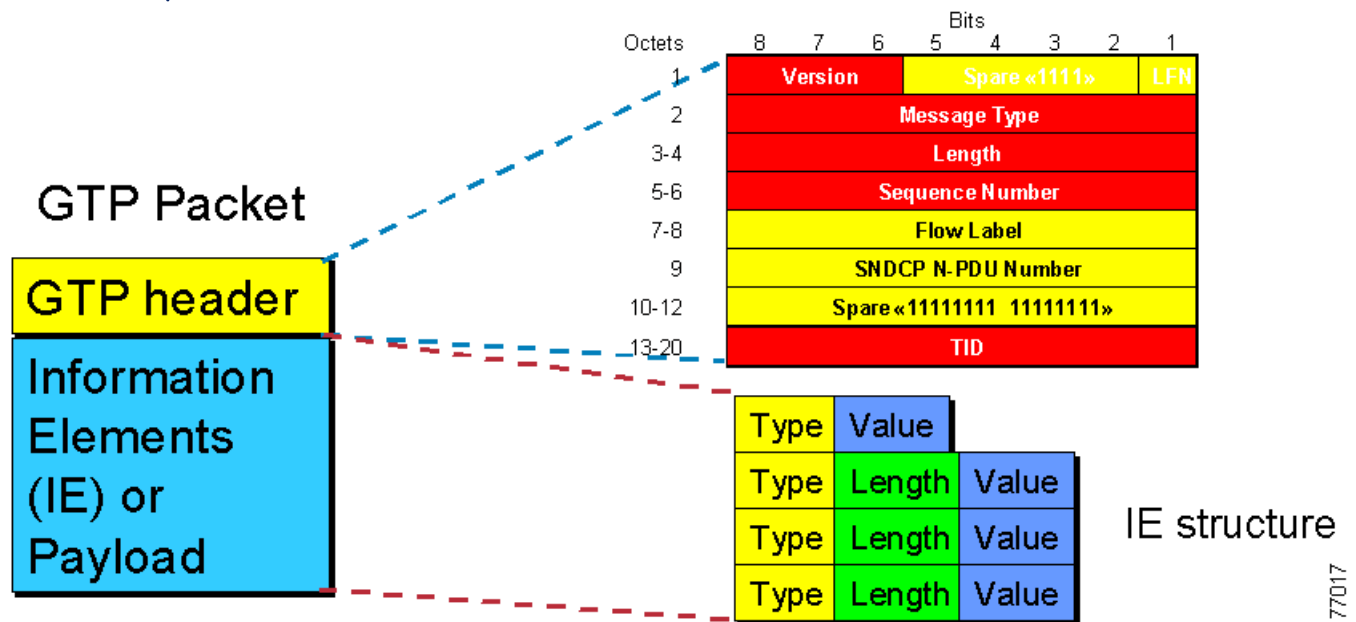


## 1.5.3 GTP protocol stack

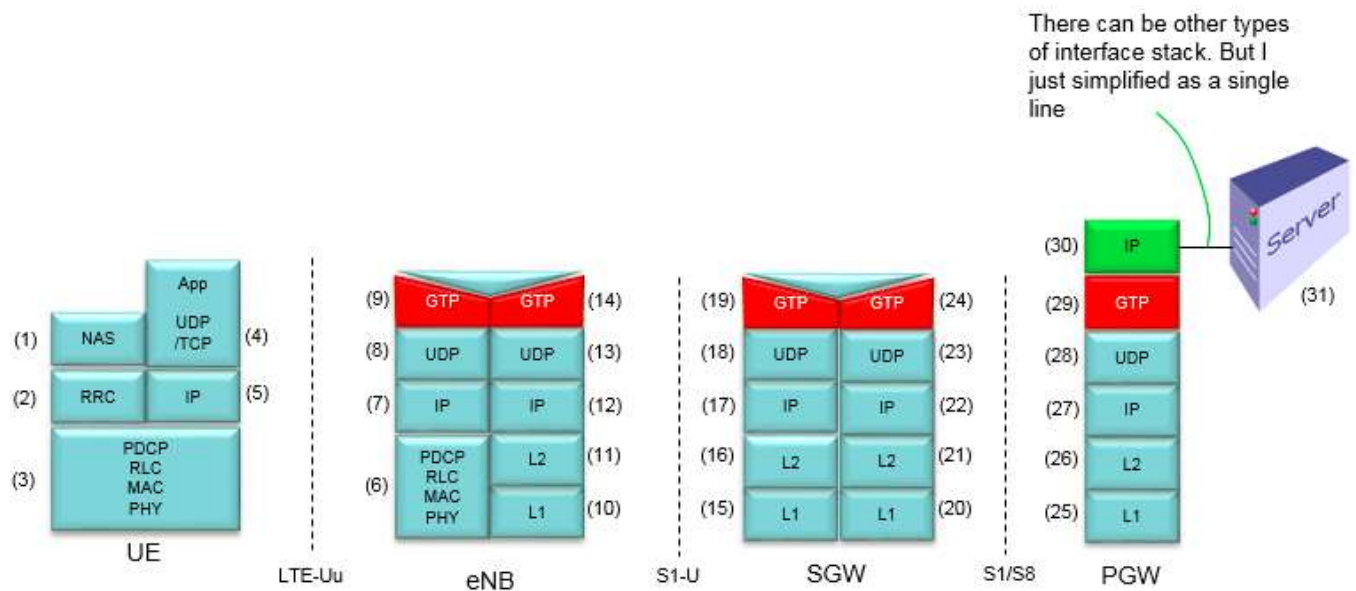




## 1.5.4 GTP packet header



## 1.6 GTP in LTE network

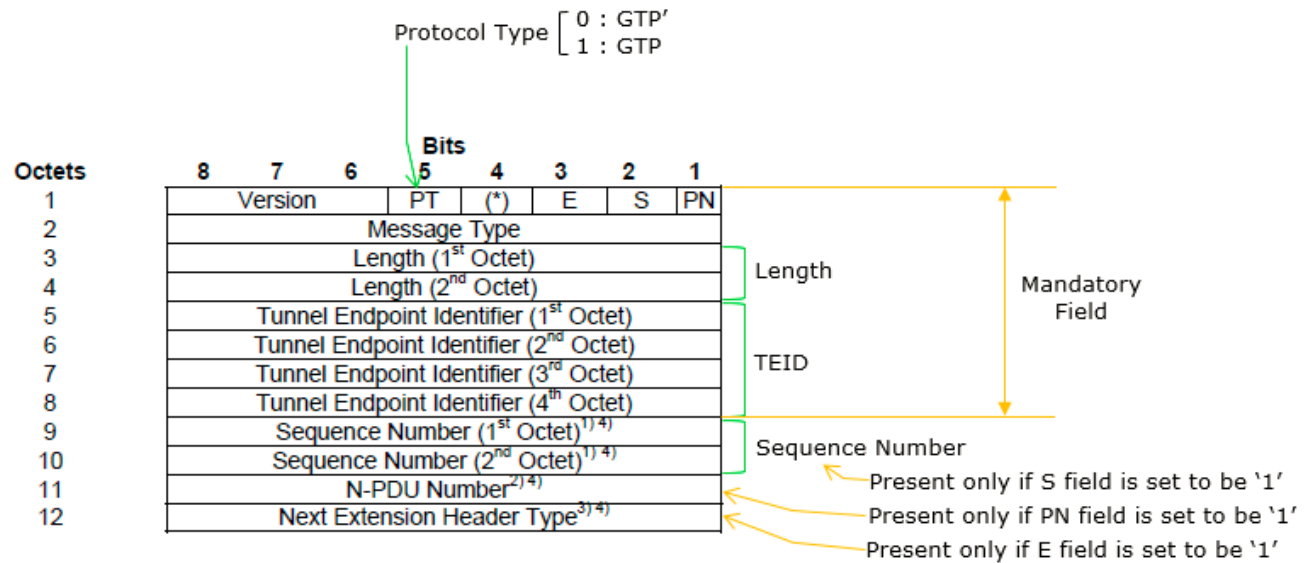




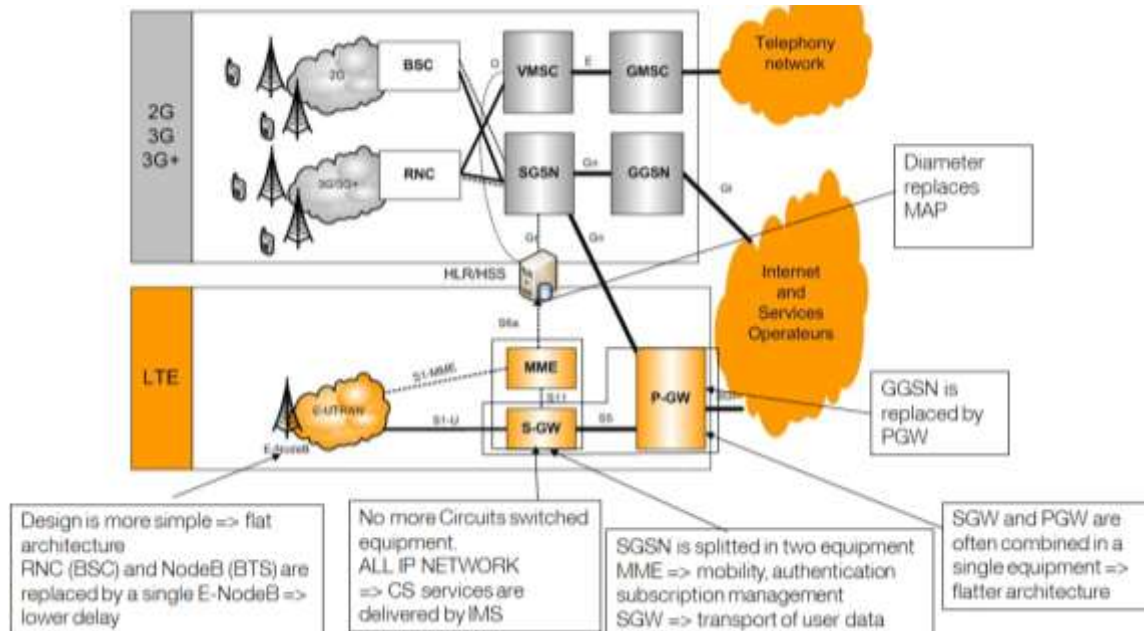
## 1.6.1 GTP packet header

Following is the GTP Header format. User Data (usually IP data) is encapsulated by a GTP packet following this header as shown in example section.

< 3GPP 29.281 - Figure 5.1-1: Outline of the GTP-U Header >



## 1.7 Diameter in LTE



- The **Diameter protocol**, standardized by the IETF Authentication, Authorization and Accounting (AAA) working group, is the successor to the RADIUS protocol and was developed to overcome several limitations of RADIUS.

AAA protocols such as TACACS+ and RADIUS were initially deployed to provide dialup Point-to-Point Protocol (PPP) and terminal server access.

Over time, with the growth of the Internet and the introduction of new access technologies, including wireless, DSL, Mobile IP, and Ethernet, routers and network access servers (NAS) have increased in complexity and density, putting new demands on AAA protocols.

RADIUS	DIAMETER
Connectionless	Connection Oriented
Uses UDP	Uses TCP or SCTP
Unreliable	Reliable
UDP Ports 1812/1813 and 1645/1646	TCP and SCTP port 3868
Hop by Hop Security	Hop by Hop and End to End Security
No Capability Negotiation	Application and Security Level Negotiation
No Server Initiated Message	Server Initiated Message is used
Static Configuration	Static and Dynamic Configuration
Vendor Specific Attributes	Vendor Specific Attributes and Messages

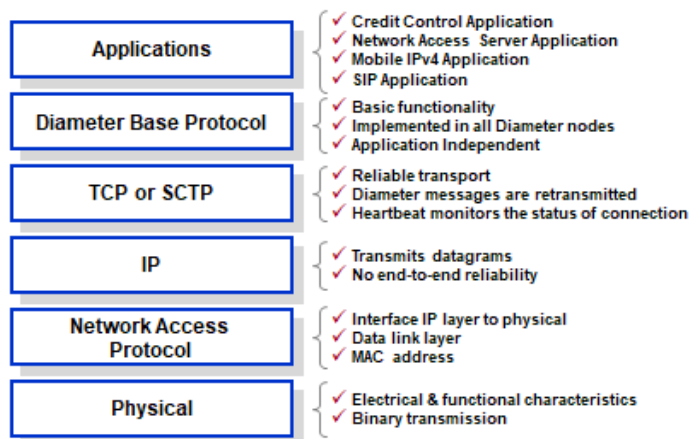
## 1.7.1 Diameter base

Diameter is composed of a **Base protocol** to which an extension called "Application" must be added.

Diameter Base provides mechanisms for: Reliable transport, Error handling, Accounting, Capabilities negotiation

Diameter Base does not provide the messages necessary for authentication and authorization. They are specific to each application.

## Diameter Base Protocol Stack



## 1.7.2 Diameter application

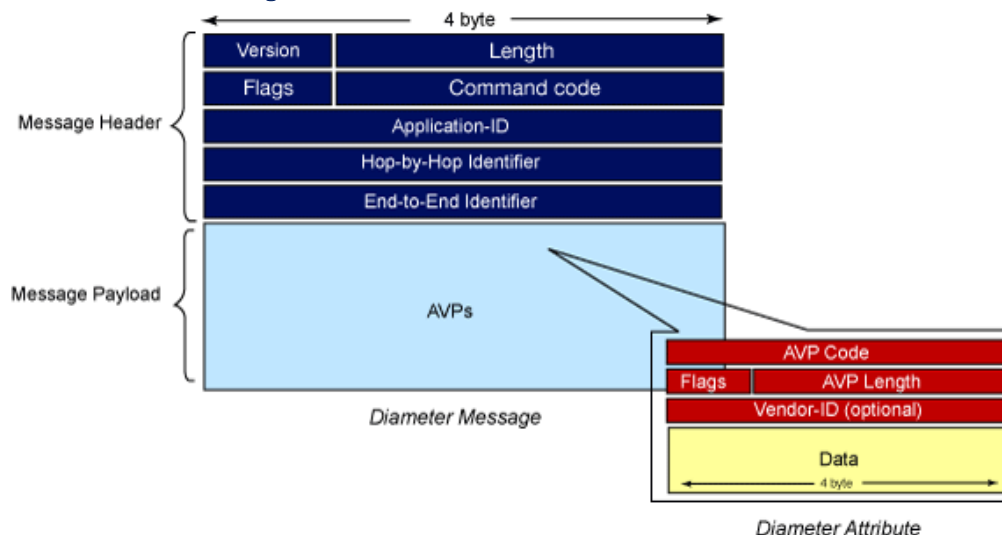
A Diameter application has nothing to do with the "software" meaning of the term. This is a protocol based on Diameter Base.

An application defines a set of commands (requests and responses) and Attribute-Value pairs (AVP) to enable authentication and authorization in a given context.

The applications are described in RFCs and 3GPP specifications. Below, some applications standardized by the IETF:

- RFC 4004 Diameter Mobile IPv4 Application (rfc4004)
- Diameter Network Access Server Application (rfc4005)
- Diameter Extensible Authentication Protocol (EAP) Application (rfc6733)
- Diameter Session Initiation Protocol (SIP) Application (rfc4740)

## 1.7.3 Diameter message format



- **Length:** Contains the size of the message (header + payload)
- **Flags:** The flags are:
  - 'R' Used to indicate whether the message is a request or a response.
  - 'P' Used to indicate whether the message can be forwarded or not.
  - 'E' Used to indicate whether the message contains an error (valid only for replies).
  - 'T' Used to indicate whether the message is a forwarded message.
- **Command Code:** Code to uniquely identify each type of request. The response to the request has the same code. However, its 'R' bit allows it to be differentiated from the request.
- **Application-ID:** Each Diameter Application has a unique identifier. This field therefore makes it possible to identify the application concerned by the message. If it is a message defined in Diameter Base then this ID is '0'.
- **Hop-by-Hop identifier:** A Diameter architecture can be made up of a client, a server and several intermediate Diameter nodes (cf. Diameter Agents). Each message therefore has a hop-by-hop identifier, in other words, modified by each node crossed by the message.
- **End-to-End identifier:** End-to-end identifier of a message. The response to a request has the same identifier as this request. Thus, a client can detect the response to a request that it has issued.
- **The payload:** is made up of a set of attribute-value pairs (AVP).

## 1.7.4 Diameter architecture

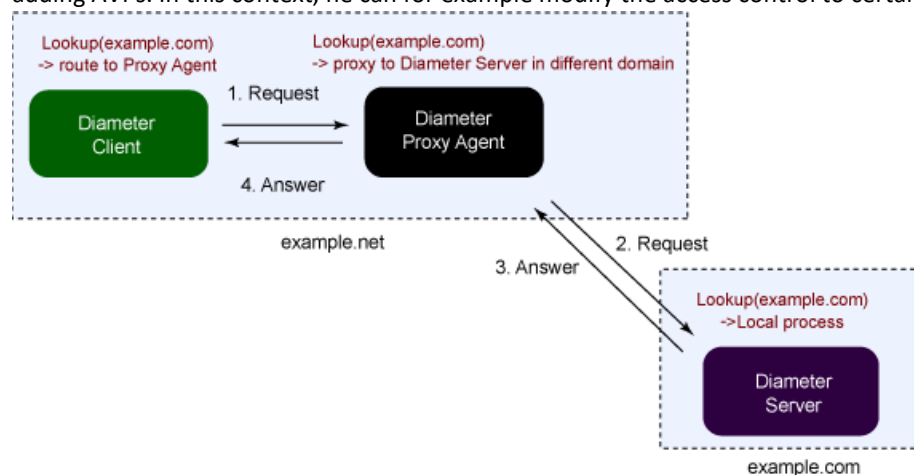
A Diameter architecture is made up of different nodes called "Diameter agents". Each agent has a well-defined role in the protocol specifications. All agents can initiate queries. In this sense, they form a peer-to-peer network. The four types of existing agents are:

### ▪ The relay agent:

The role of this agent is to route the messages to the correct destination according to the information contained therein such as the application id or the "Destination-Realm" AVP.

Typically, the Proxy is placed between the Diameter client and several servers of different applications. Thus, depending on the target application of a request sent by the client, the proxy will be able to transmit it to the right server.

This avoids configuring the client to take each server into account. In addition, the proxy can modify the messages by adding AVPs. In this context, he can for example modify the access control to certain resources for a given domain



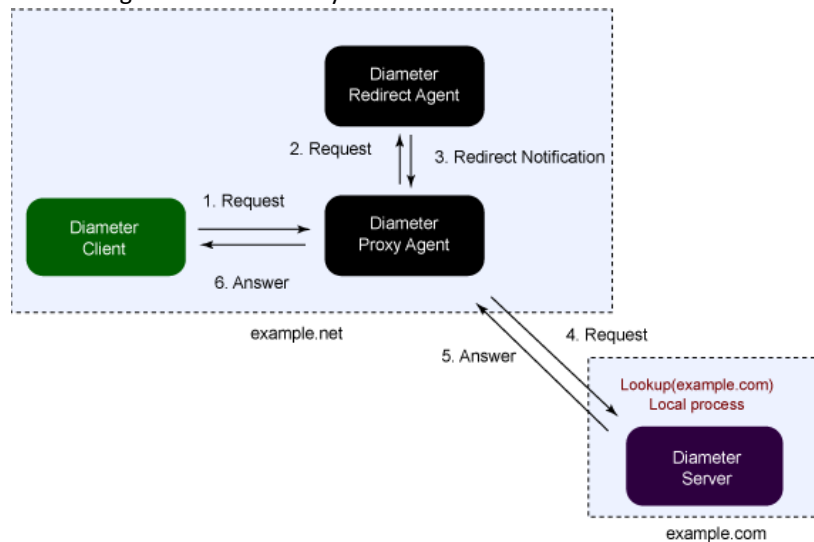
- **The proxy agent**

The role of a relay is the same as a proxy except that it cannot modify messages.

- **The redirect agent**

The redirection agent centralizes routing information. It can be queried by any node not knowing where to send a message. The redirect agent then responds with the redirect information.

The use of this agent makes it possible to alleviate the local configurations to the nodes which no longer need to keep the routing information locally.



- **The translation agent**

The translation agent allows Diameter's interoperability with other AAA protocols. Take the example of RADIUS. The translation agent changes RADIUS messages to their Diameter equivalent (if any).

The benefit may be to ensure a smooth migration to Diameter, retaining RADIUS clients and servers during the transition phase.



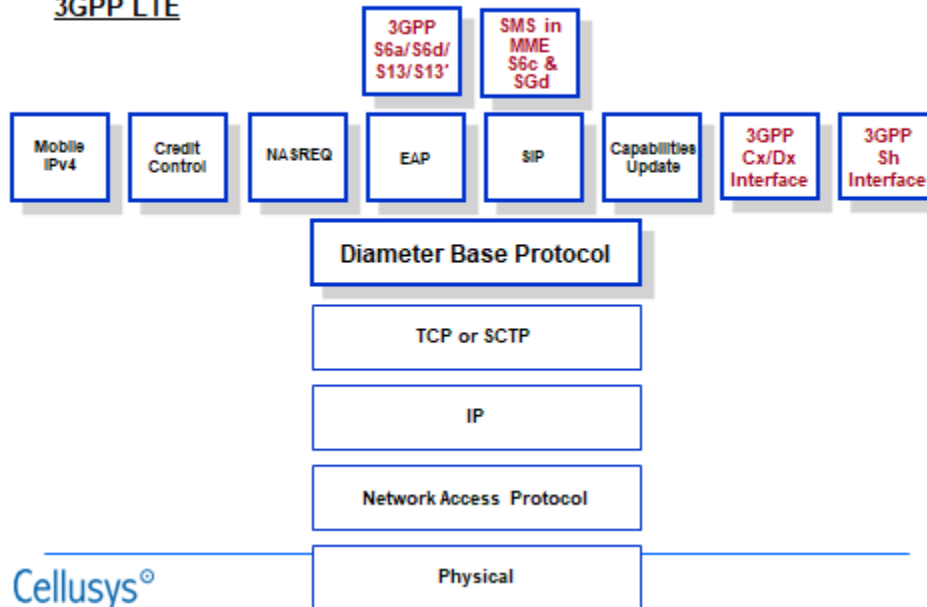
## 1.7.5 Diameter protocol stack

In previous 3GPP releases and architectures, functions like managing the mobile's location, handling subscriber data, authentication, fault recovery and checking the **Mobile Equipment's** (ME) identity were all handled using SS7.

Now starting with this new architecture in LTE EPS, those functions are handled by Diameter on interfaces called "S6a/S6d/S13/S13." In addition, LTE networks allow an optional architecture called SMS in MME. And, yes that also uses Diameter on interfaces "S6c and SGd." So now our Diameter application tree looks like this:

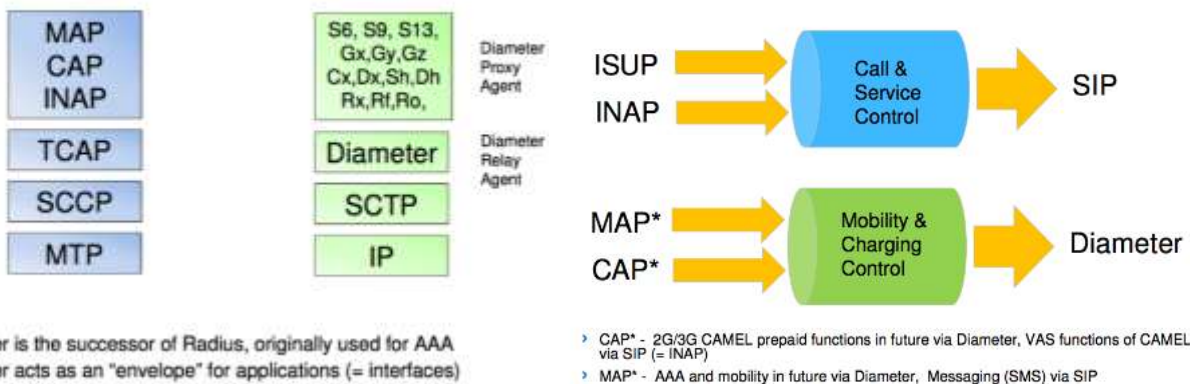
## Diameter's Expanding Applications

3GPP LTE



## Comparing the SS7 and Diameter Protocol Stacks

## Mapping of SS7 to IP protocols



The s6a interface is between MME and HSS in the LTE network and **s6d is between SGSN and HSS.**

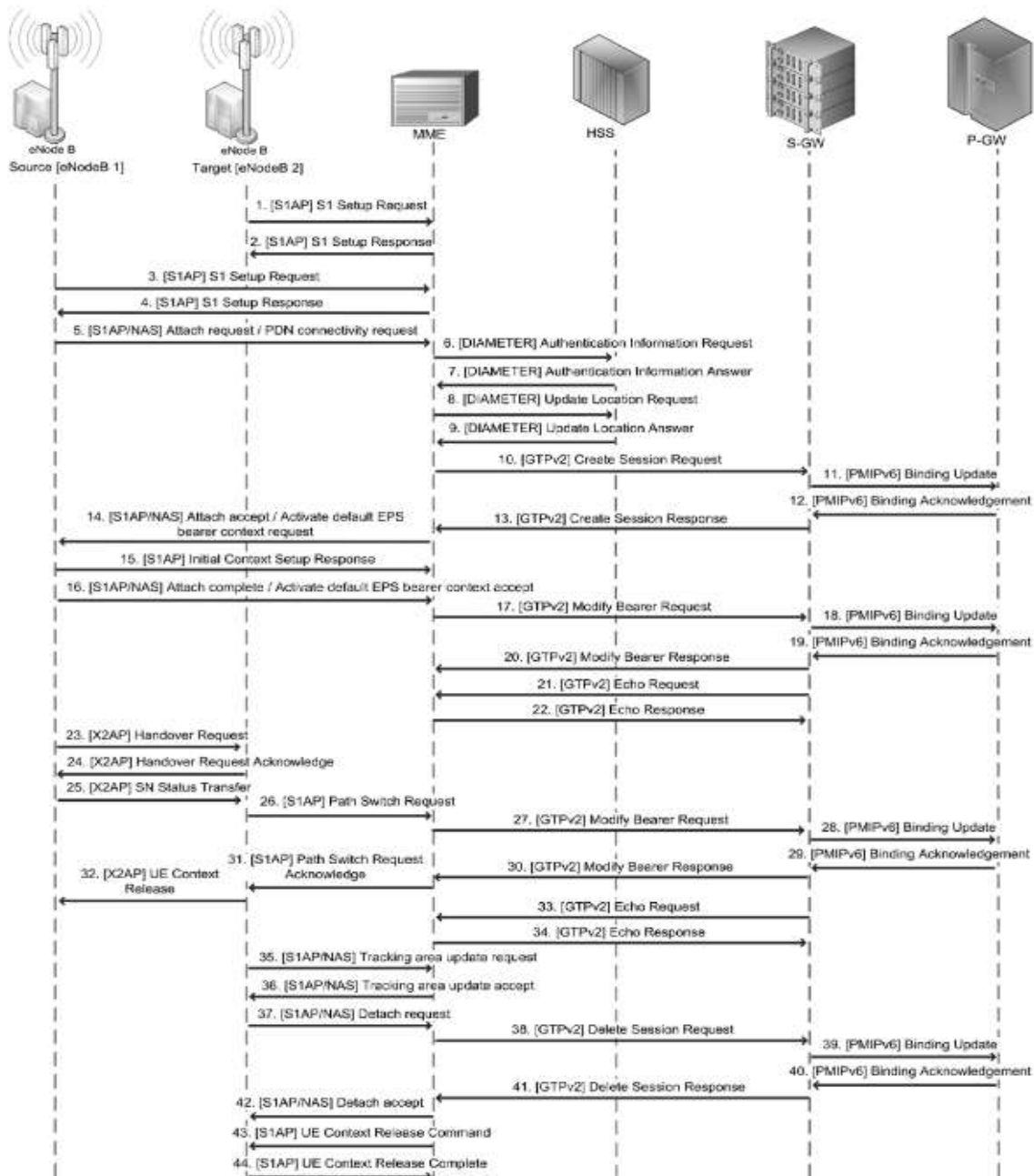
### 1.7.7 Summary

As a recap, Diameter is an IETF-defined AAA protocol. It is in a *Request/Answer* format. It delivers parameters called **Attribute Value Pairs (AVP)**. Along with the base protocol, the IETF wrote several applications for Diameter. Additionally, it is used in 3GPP networks in the IMS, in LTE for mobility management and for *Policy and Charging Control* PCC. Though we won't redraw our 3GPP application tree, 3GPP also uses Diameter for other interfaces. These include:

- **Generic Authentication Architecture (GAA)**
- 3GPP to **Wireless LAN (WLAN)** Interworking
- Location Services (LCS)
- EPS AAA Interfaces

However, the primary ones are used in IMS, LTE and PCC

## 1.7.8 LTE attachment





## 2 GSM | GPRS | VOIP | VOLTE | LTE threats attack

### 2.1 GSM threat attacks

#### 2.1.1 Attacker's profile

An attacker can be a person or a group of people sufficiently qualified to build a node to emulate that of a mobile operator.

**To access an SS7 network**, attackers can acquire an existing provider's connection on the black (underground) market and obtain authorization to operate as a mobile carrier in countries with lax communications' laws.

**In addition**, any hacker who happens to work as a technical specialist at a telecommunications operator, would be able to connect their hacking equipment to the company's SS7 network.

**In order to perform certain attacks**, legitimate functions of the existing communication network equipment must be used.

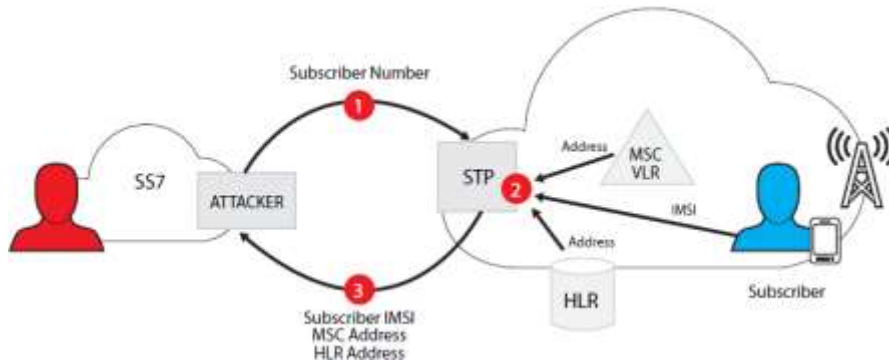
**There is also an opportunity** to penetrate a provider's network through a cracked edge device (GGSN or a femtocell).

**Besides having different ways of accessing an SS7 network**, attackers likely also have different motives for doing so including performing fraudulent activities, obtaining a subscriber's confidential data or disrupting service for certain subscribers or the whole network.

#### 2.1.2 IMSI disclosure (Requesting MSC)

**Goal:** Analyze a service provider's network to obtain subscriber information.

- This attack is based on requesting the Mobile Switching Center (MSC) Visitor Location Register (VLR) address, and the IMSI.
- The request is part of the SMS delivery protocol, which allows the source network to receive information about the subscriber's location for further routing of the message.
- The initial data includes the target subscriber number



**Result:** In case of successful exploitation, an attacker obtains the following data:

+ Subscriber's IMSI + Servicing MSC/VLR address + Home Location Register (HLR) address where the subscriber's account data is located

The MSC/VLR address will determine the subscriber's location down to the regional level. Moreover, the intruder can use the obtained data in more complex attacks (as described below).

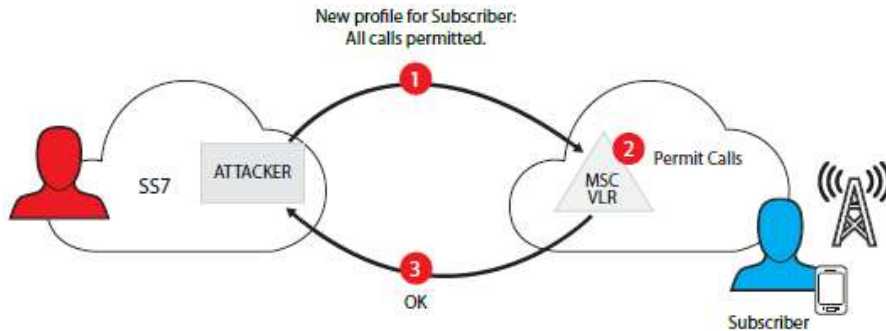


## 2.1.3 Subscriber Profile Manipulation (Send fake subscriber profile to VLR)

**Goal:** Spoof the network with fake subscriber profile data

**Description:** When a subscriber registers on a switch, his/her profile is copied from the HLR database to the VLR database.

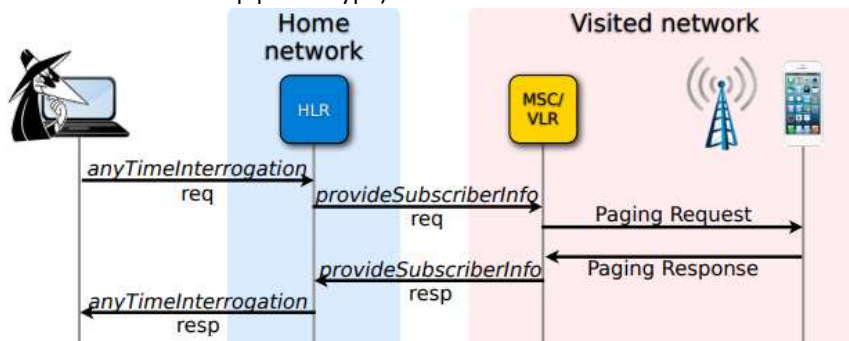
The profile contains information about active and inactive subscriber services, call forwarding parameters, the on-line billing platform address, etc. An attacker can send a fake subscriber profile to the VLR.



**Result:** A fake profile will fool the MSC/VLR into providing services to the subscriber based on altered and fraudulent parameters. For example, the subscriber will be able to make voice calls that bypass the billing system.

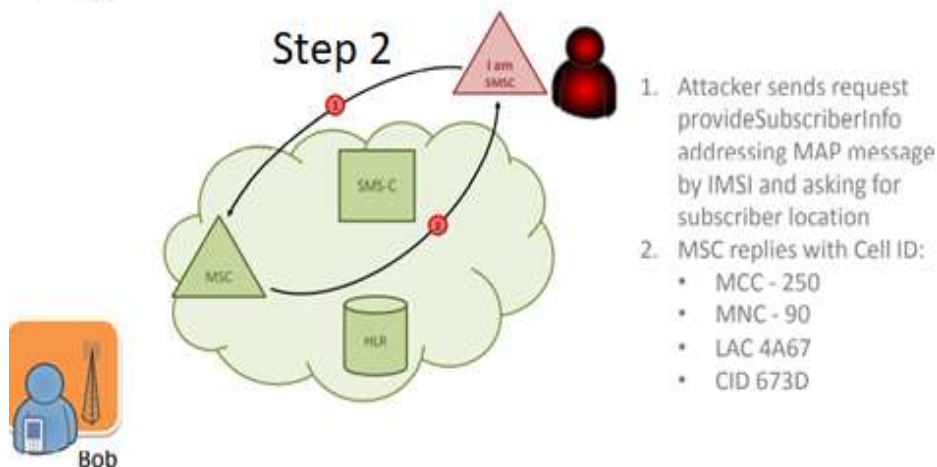
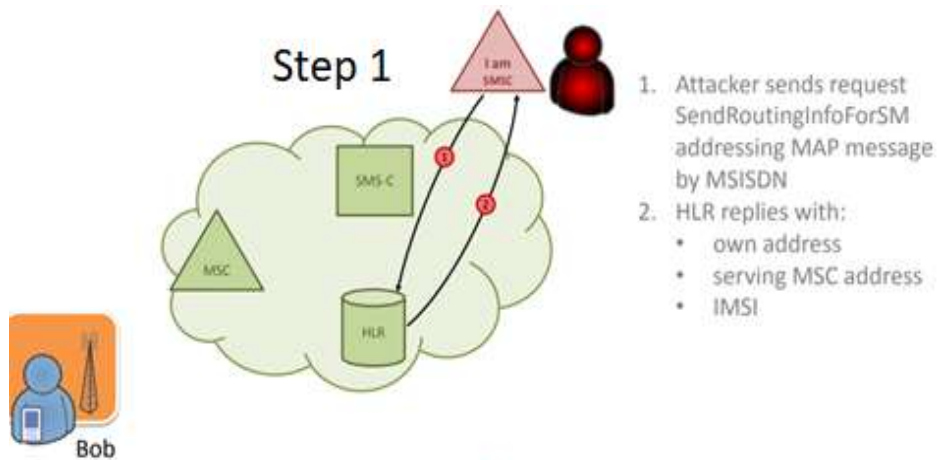
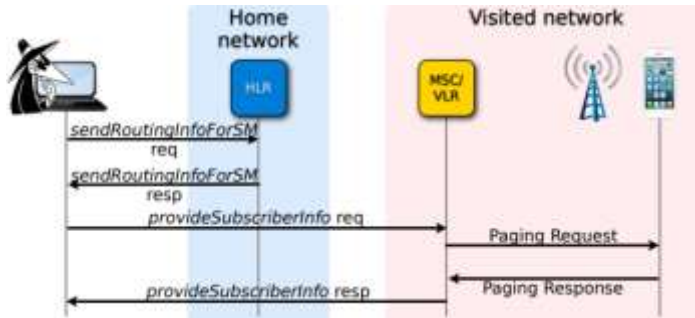
## 2.1.4 Cell Level Tracking using MAP's anyTimeInterrogation (ATI) service

- MAP's anyTimeInterrogation (ATI) service can query the subscriber's HLR for her Cell-Id and IMEI (phone serial number, can be used to look up phone type)



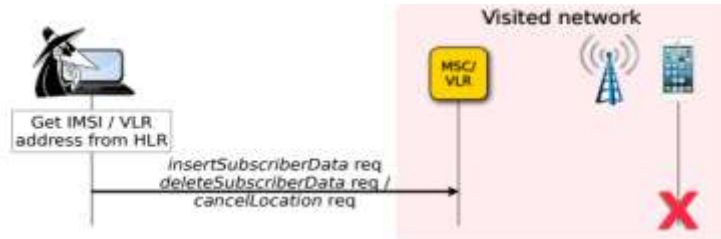
## 2.1.5 Cell Level Tracking using MAP's SendRoutingInfoForSM (Fake SMSC)

- Instead, query the MSC/VLR directly
- But MSC/VLR use IMSIs (International Mobile Subscriber Identifiers), not phone numbers, to identify subscribers
- ask the HLR for the subscriber's IMSI and Global Title of the current MSC/VLR
- When the attacker knows the IMSI of the subscriber and the Global Title, the MSC/VLR can be asked for the cell id of the subscriber

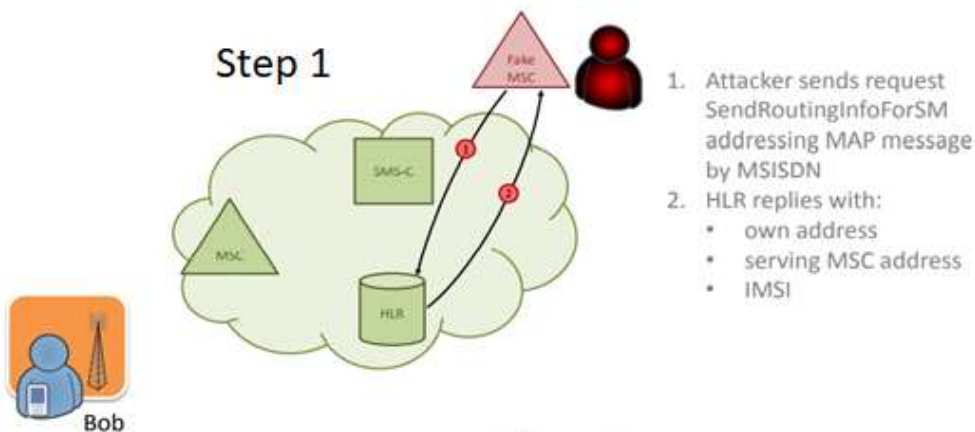


## 2.1.6 Denial of Service (Fake MSC)

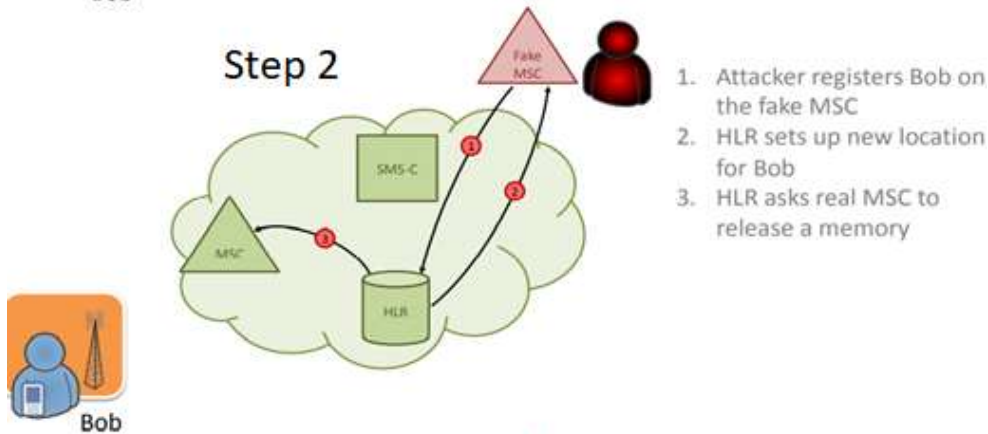
- It is not only possible to read subscriber data - it can also be modified, since most network's VLR/MSC don't do any plausibility checks
- Control every aspect of what a subscriber is allowed to do: enable or disable incoming and/or outgoing calls / SMS or data or delete the subscriber from the VLR altogether



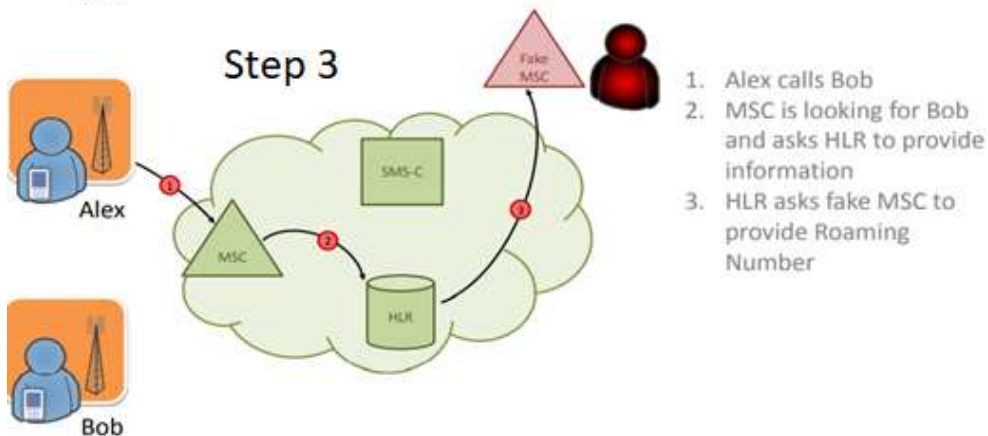
### Step 1



### Step 2



### Step 3



## 2.1.7 DOS call (using numerous roaming number requests)

**Goal:** Denial of service for incoming MSC calls

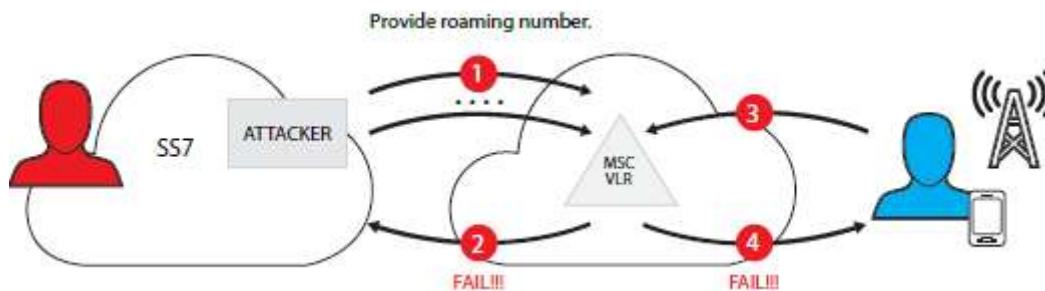
**Description:** This attack is based on the procedure of assigning a roaming number (MSRN) when receiving a voice call.

When a call is received, the current subscriber's MSC/VLR is identified, after which a voice channel is established to this switch using a temporary roaming number.

Normally, a roaming number lives for a split second. However, the default values of timers responsible for holding a roaming number, which are specified on the equipment, are 30—45 seconds.

If an attacker sends numerous roaming number requests, to a switch using default parameters, then the pool of available numbers will be used up quickly.

As a result, the switch will not be able to process incoming mobile calls.



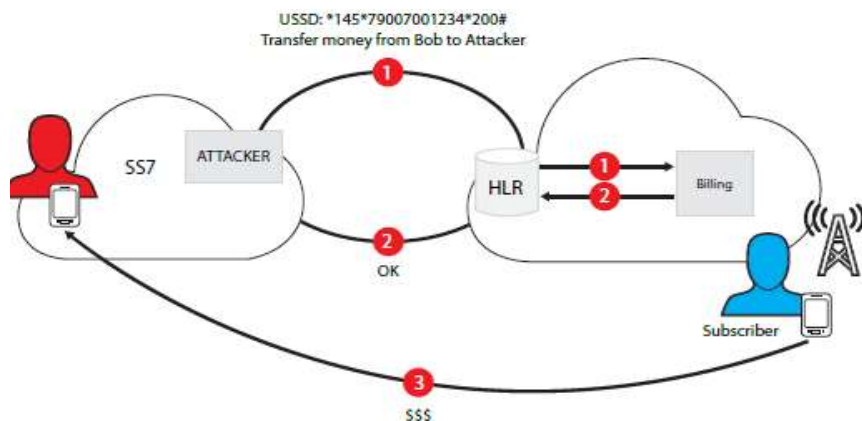
## 2.1.8 USSD Request Manipulation

**Goal:** Send USSD requests directly to HLR

**Description:** This attack is a good example of using a legitimate message with a USSD request sent from VLR to HLR. The initial data is the target subscriber number, the HLR address and the USSD string.

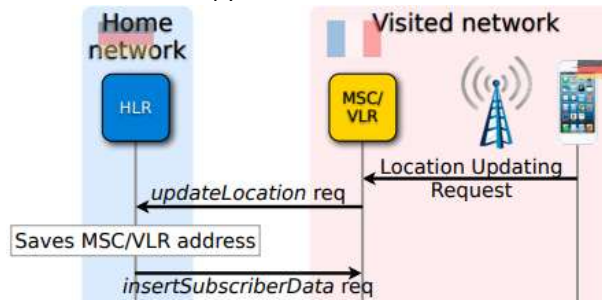
The subscriber number is usually known from the beginning.

The HLR address can be obtained as outlined in 4.1 and USSD requests are described on the service provider's site.

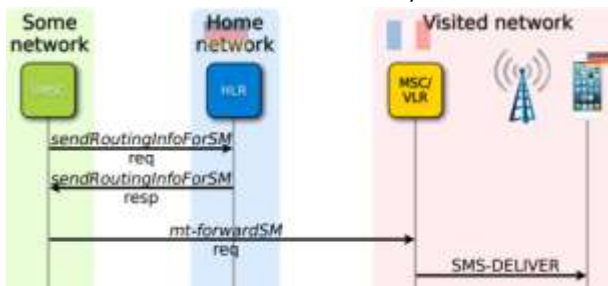


## 2.1.9 HLR Stealing Subscribers (Roaming scenario)

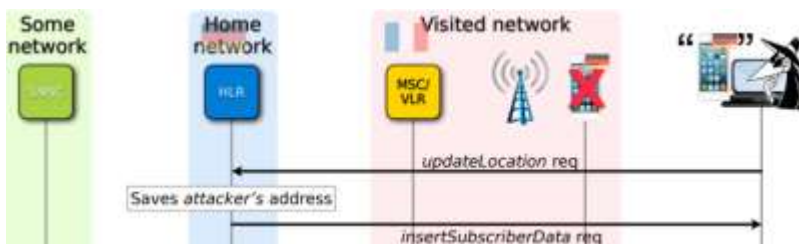
- When a subscriber travels to another region or country, the VLR/MSC sends a MAP updateLocation request to the subscriber's HLR
- The HLR sends a copy of the subscriber's data to the VLR/MSC and saves the address of the VLR/MSC



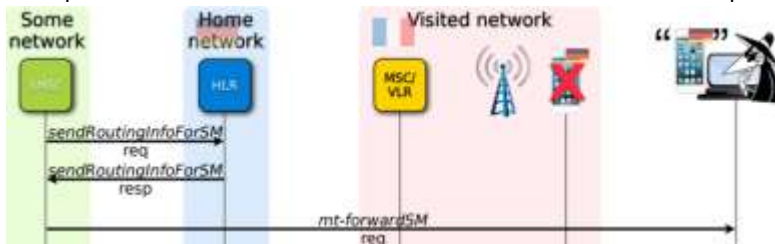
- Now, when somebody wants to call or text the subscriber, the HLR gets asked for routing information (sendRoutingInfo...) and hands out the address of the VLR/MSC



- The updateLocation procedure is also not authenticated
- An attacker can simply pretend that a subscriber is in his "network" by sending the updateLocation with his Global Title to the subscriber's HLR

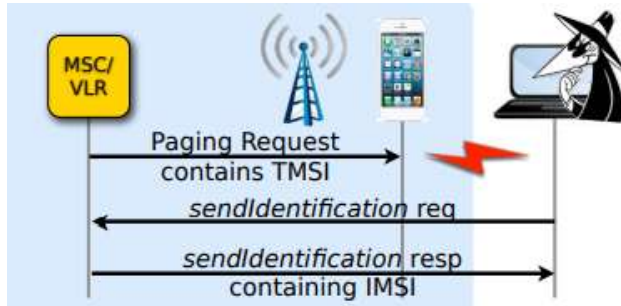


- Now, calls and SMS for that subscriber are routed to the attacker
- Example: Subscriber's bank sends text with mTAN. Attacker intercepts message and transfers money to his own account



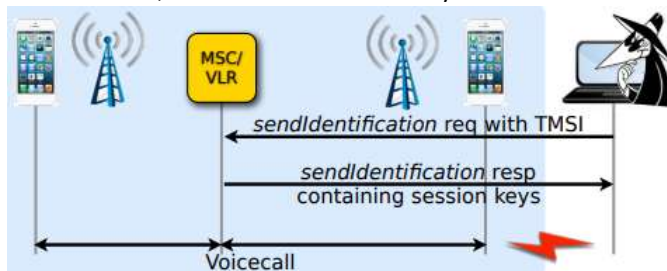
## 2.1.10 Hybrid Attacks: TMSI De-anonymization

- An attacker can find out the phone numbers of subscribers around him:
  - Paging of subscribers (e.g. to notify them of an incoming call) has to happen unencrypted
  - TMSI (Temporary Mobile Subscriber Identifier) is normally used for paging so that the real identity of the subscriber (IMSI) does not have to be sent over the air unencrypted
- Attacker captures TMSI over the air, e.g. with OsmocomBB
- The MSC can be asked to hand out the IMSI if the TMSI is known
- With updateLocation, the attacker can figure out the MSISDN belonging to the IMSI



### 2.1.10.1 Hybrid Attacks: Intercept Calls

- The MSC can also be asked for the session key for the subscriber!
- If the attacker captures an encrypted GSM or UMTS call, he can then decrypt it using the session key
- Passive attack, no IMSI catcher necessary





## 2.1.11 Intercepting outgoing calls

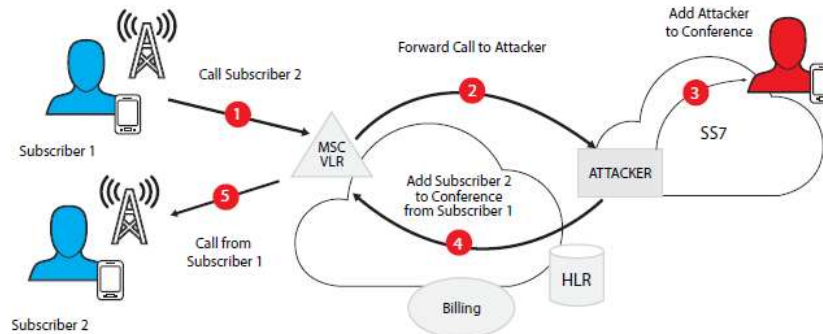
**Goal.** Redirecting outgoing subscriber voice calls and data messages to an attacker's device.

**Description.** This attack is an extension of Subscriber Profile Manipulation in VLR attack, described in **1.7 section**.

An attacker substitutes a billing platform address with their equipment address, in the subscriber's profile.

When the subscriber makes a call, the billing request along with the number of the destination subscriber are sent to the attacker's equipment.

The attacker can then redirect the call and create a three-way (destination subscriber, calling subscriber and an attacker) conference call.



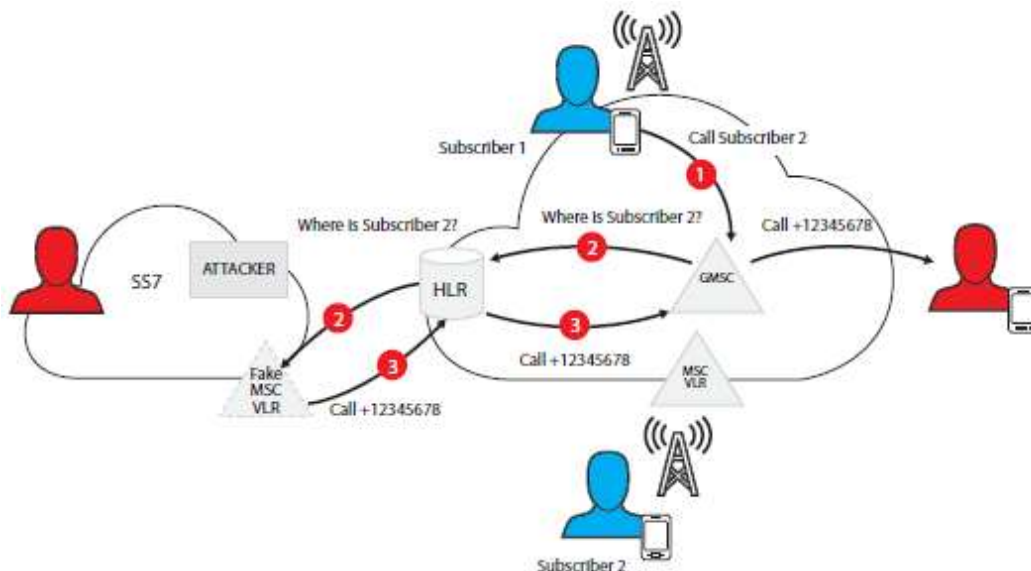
## 2.1.12 Redirecting incoming calls

**Goal:** Change voice call routing and redirect incoming calls

**Description:** This attack is for incoming calls and is an extension of the attack described in **section 1.10**.

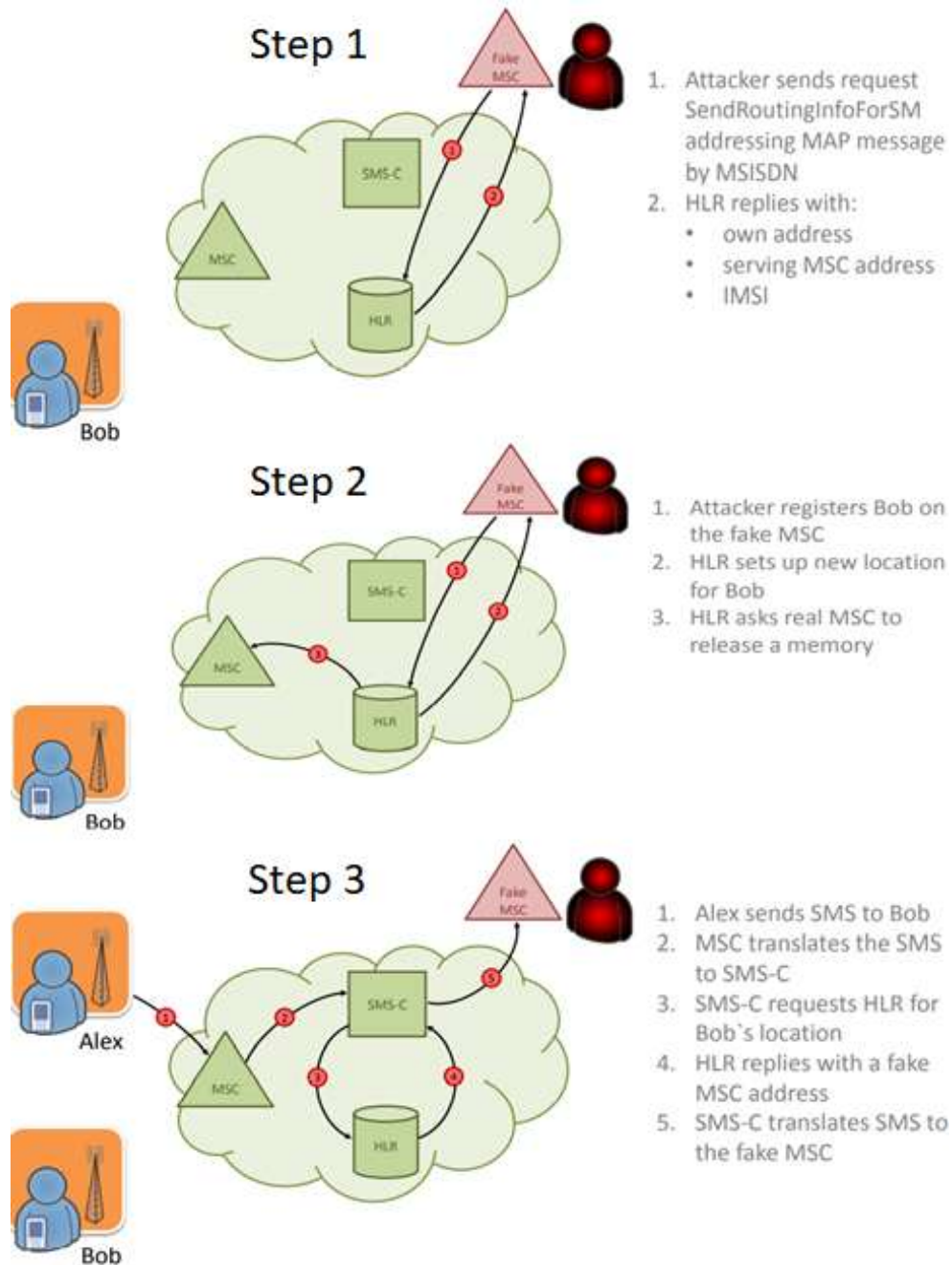
When a call is terminated, the gateway MSC (GMSC) sends a request to the HLR to identify the MSC/VLR that currently serves the subscriber. This data is necessary to route the call to the appropriate switch.

After successfully performing the attack in **section 1.10**, the HLR will redirect the received request to a fake MSC/VLR, which in turn will send the Mobile Station Roaming Number (MSRN) to redirect the call. The HLR transfers this number to the GMSC, which redirects the call to the provided MSRN.



## 2.1.13 SMS intercept (using Fake MSC)

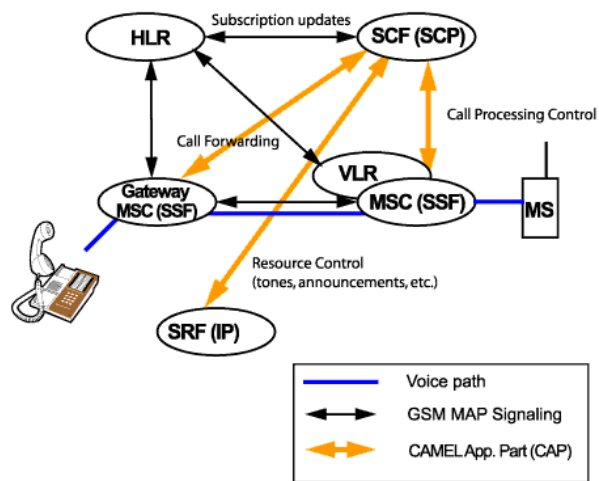
- A virus on a smartphone – and what if a certain subscriber is a target? How to infect him particularly?
- Reissue SIM? It works only once.
- Radio signal interception (GSM A5/1)? You need to be nearby.
- Via SS7 network is a solution



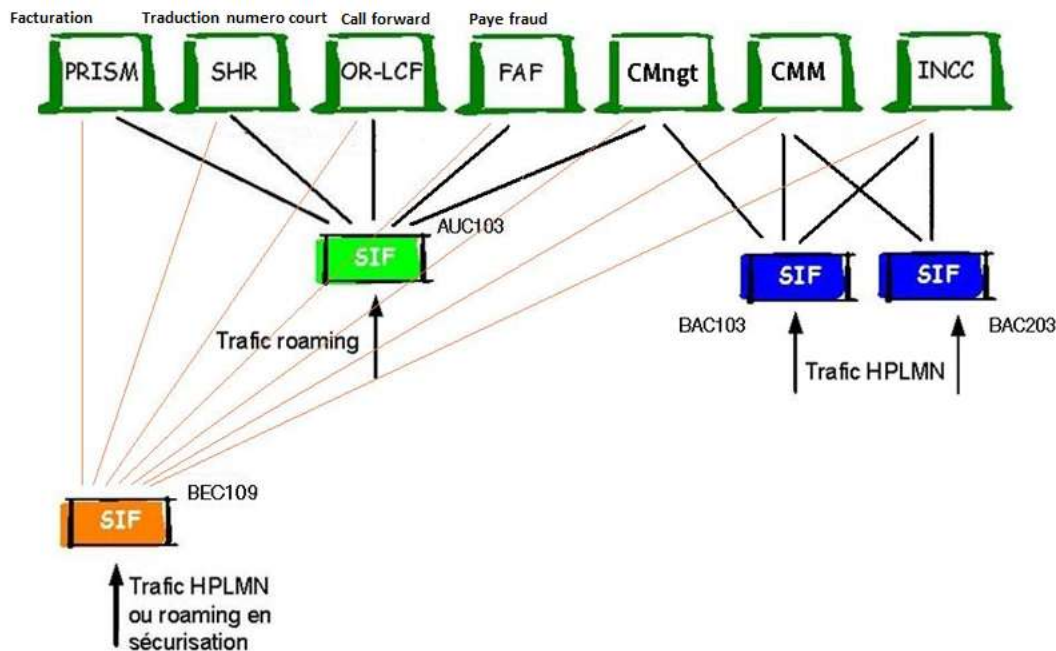


## 2.1.14 Intercepting calls with CAMEL (Roaming scenario)

Just for your information [CAMEL](#) is a means of adding intelligent applications to mobile (rather than fixed) networks. This is the architecture

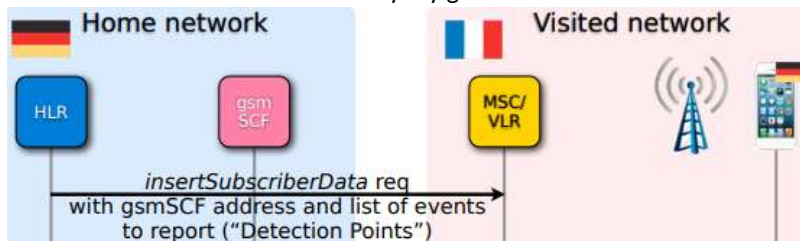


And these are the service offered by CAMEL

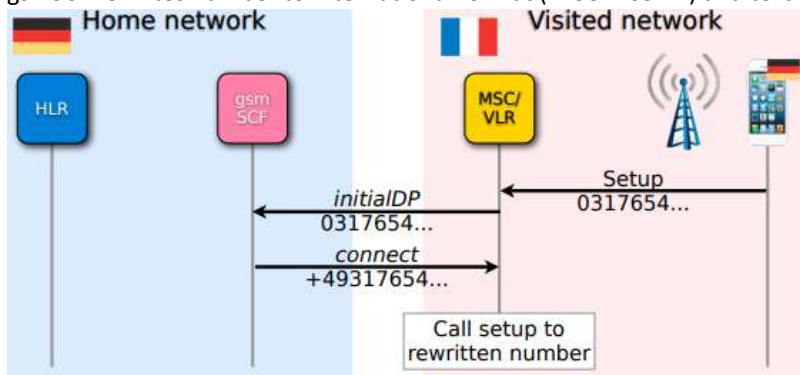


# MOBILE NETWORK HACKING

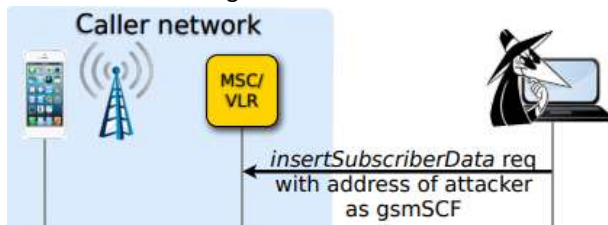
- This how the threat attack come in CAMEL technology:
- German HLR tells French VLR "notify my gsmSCF at address +4917... whenever the subscriber wants to make a call"



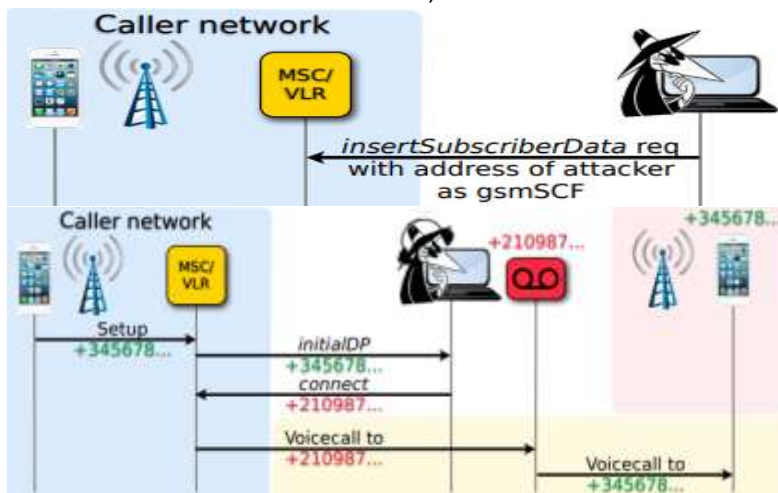
- Subscriber wants to make a phone call, but dials number in German national format (0317654...)
- MSC asks gsmSCF in home network what to do with the call
- gsmSCF rewrites number to international format (+49317654...) and tells MSC to continue with the new number



- Attacker overwrites gsmSCF address in subscriber's MSC/VLR with its own, "fake gsmSCF" address



- Subscriber wants to call +345678..., but the MSC now contacts the attacker instead of the subscriber's gsmSCF
- Attacker rewrites number to +210987..., his recording proxy (e.g. an Asterisk PBX)
- MSC sets up call to +210987..., which bridges it to the original +345678...
- Both subscribers can talk to each other, while the attacker records the conversation



## 2.1.15 SPAM Message in mobile network

Spam refers to unsolicited calls or messages sent in bulk to a telephone line. Spam can be either of a commercial nature or of a fraudulent nature. Fraudulent spam generally falls under one of the following two practices:

- Scam the purpose of which is to extract money from the victim;
- Theft of personal data, the purpose of which is to obtain sensitive information such as credit card numbers or usernames and passwords for connecting to a website.

**For this, fraudulent spam responds to several operating modes:**

### ▪ Spam SMS:

- sending fraudulent SMS, which encourages calling a premium rate number, generally 0899,
- sending an SMS to a premium rate number, generally 5 characters,
- Or clicking on a link on a page Internet.

The messages received have a familiar and encouraging nature, such as:

- "Hi, it's me, you didn't call me. I'm waiting for your call back on 0899 (...).
- "Or" Hello, a package has been waiting for you for 10 days and will leave if you don't pick it up by tomorrow. Please call us on 0899 (...).

### ▪ Voice spam:

- Emission of calls broadcasting a pre-recorded message in order to encourage the called party to call back a surcharged number in 089.

The messages are familiar, encouraging but can sometimes be very anxiety-provoking such as:

"Hello, these are the emergencies of XYZ Hospital. Your partner has just had a serious accident. Please call us on 0899 (...). ";

### ▪ Ping call:

transmission of short calls (one or two maximum rings) without giving the recipient time to pick up the receiver in the hope that the latter will call back the number presented without paying attention or out of curiosity.

While "ping calls" historically called back surcharged "089" numbers directly, this practice has evolved since Arcep banned the use of 089 numbers as a caller ID in 2012 (decision no. -0856).

### ▪ Spoofing

There were nearly 26 billion scam calls in 2019, according to data collected by [YouMail](#), and scammers are getting smarter. Now they are using a technique called spoofing to make it easier to scam you.

Spoofing is when someone makes your phone number pop up on a caller ID when it really isn't you that's making the call.

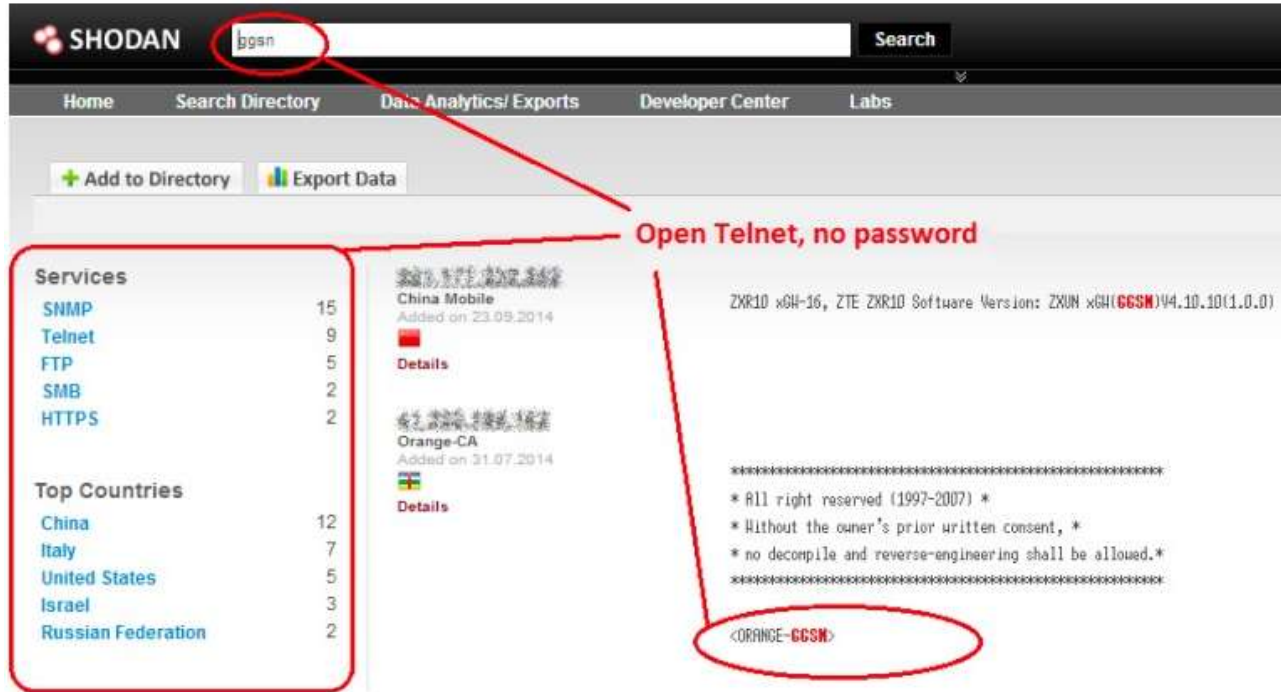
For example, a scammer once spoofed my daughter's phone number to make me think she was calling me. The goal was to trick me into answering the phone. It worked, because what if it was an emergency and my daughter needed me? When a scammer gets you to pick up, they have the chance to trick you into whatever scheme they've come up with, like tricking you into giving them your credit card information.

It doesn't take much to spoof a phone number. There are apps and websites that allow scammers to simply type in a phone number and make a call. It's super easy and quick, which makes it appealing to scammers.

## 2.2 GPRS threats attack

### 2.2.1 Searching for mobile operator's facilities on the Internet

- We already know that GGSN must be deployed as an edge device. Using Shodan.io search engine for Internet-connected devices, we can find the required devices by their banners.



Search result displays about 40 devices using this abbreviation in their banners.

The screenshot provides a list of some devices that use this abbreviation, including devices with open Telnet and turned off password authentication.

- An attacker can perform an intrusion into the network of the operator in the Central African Republic by connecting to this device and implementing the required settings.
- Having access to the network of any operator, the attacker will automatically get access to the GRX network and other operators of mobile services. One single mistake made by one single operator in the world creates this opportunity for attack to many other mobile networks.
- There are more ways of using the compromised boundary host, for example, DNS spoofing attack (more information about attacks is considered below).

## 2.2.2 IMSI brute force

**Goal:** To find a valid IMSI.

**Attack vector:** An attacker conducts attacks from the GRX network or the operator's network.

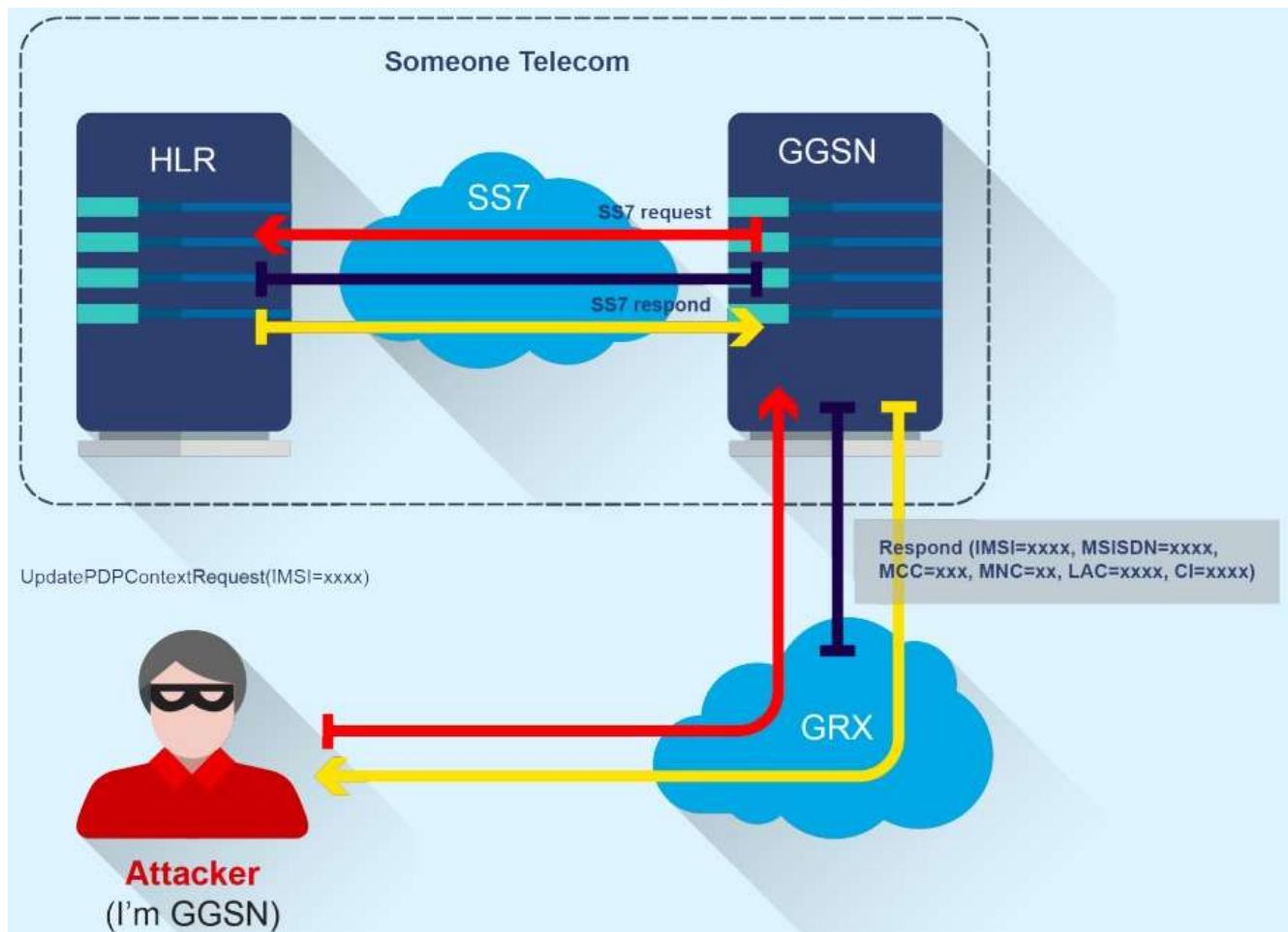
**Description:** IMSI is the SIM card Number (International Mobile Subscriber ID). It consists of 15 digits, the first three identify the Mobile Country Code (MCC), and the next two digits are the Mobile Network Code (MNC).

- You can choose the required operator on the website [www.mcc-mnc.com](http://www.mcc-mnc.com), enter the MCC and MNC
- And then brute force the remaining 10 digits by sending a «Send Routing Information for GPRS Request» message via GRX.

This message can be sent to any GSN device, which converts the request into an SS7 format (CS core network component) and sends it to HLR where it is processed by SS7 network.

If the subscriber with this IMSI uses the Internet, we can get the SGSN IP address serving the mentioned subscriber. Otherwise, response will be as follows: «Mobile station Not Reachable for GPRS».

**Result:** Obtaining a list of valid IMSI for further attacks.



## 2.2.3 The disclosure of subscriber's data via IMSI

**Goal:** To obtain a phone number, location data, information about the model of a subscriber's mobile device via IMSI.

**Attack vector:** An attacker conducts attacks from the GRX network or the operator's network.

**Description:** An attacker can use this vulnerability after the success of the previous attack or if he/she gets a subscriber's IMSI via a viral application for the subscriber's smartphone.

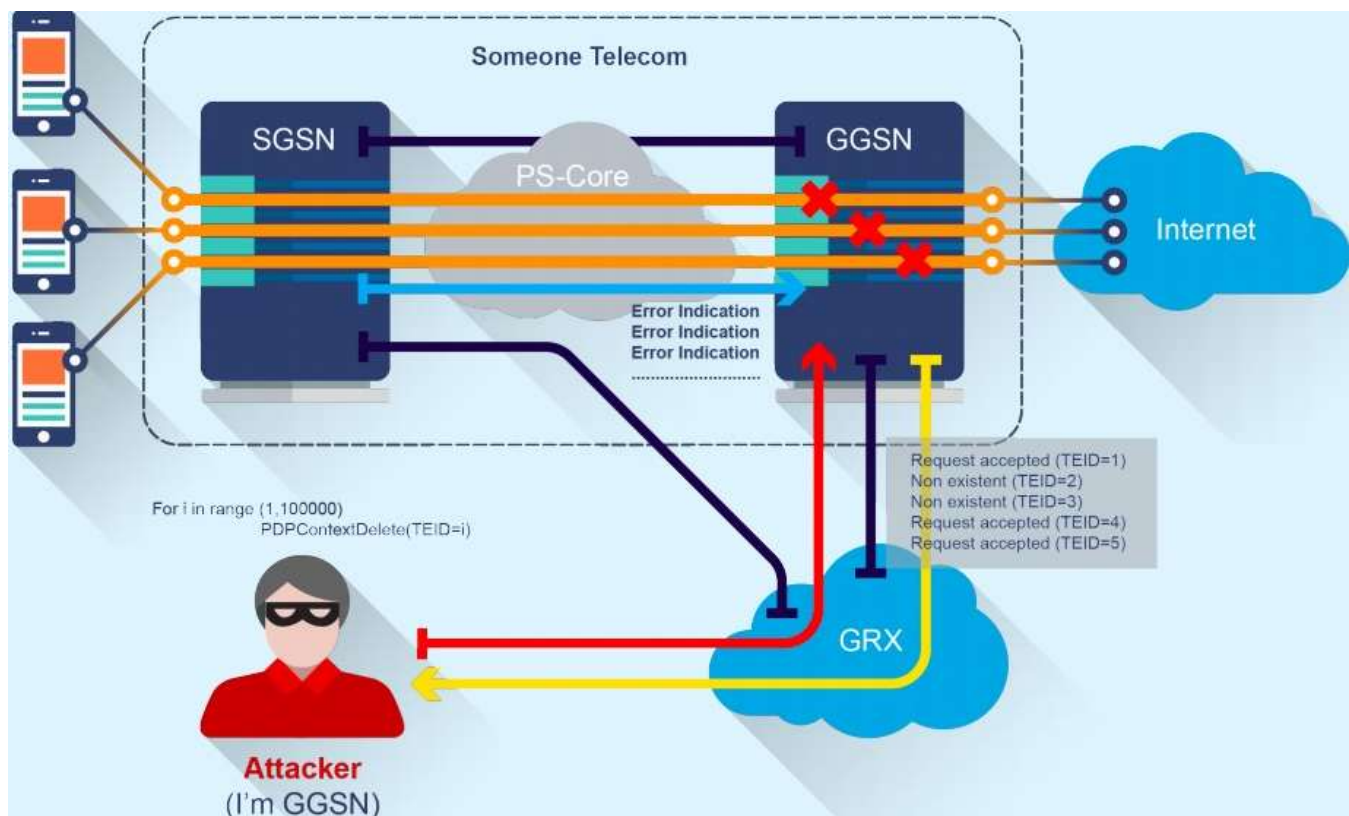
The attacker needs to know the SGSN IP address, garnered from the previous attack.

After that, the attacker sends an Update PDP Context Request to the SGSN IP address requesting the subscriber's location; the GSN Control Plane is spoofed with the attacker's IP address.

The response contains MSISDN (Mobile Subscriber Integrated Services Digital Number), IMEI (International Mobile Equipment Identity, it helps to identify the model of a subscriber's phone) and the current subscriber's mobile radio base tower (MCC, MNC, LAC, CI).

Consequently, the attacker can find the subscriber's location accurate to several hundred meters using the following website: <https://xinit.ru/bs/> or <http://opencellid.org/>.

**Result:** The required information about the subscriber is obtained.





## 2.2.4 Disconnection of authorized subscribers from the Internet

**Goal:** To disconnect the connected subscribers.

**Attack vector:** An attacker conducts attacks from the GRX network or the operator's network.

**Description:** The attack is based on sending the «PDP context delete request» packets to the target GGSN with all the TEID listed.

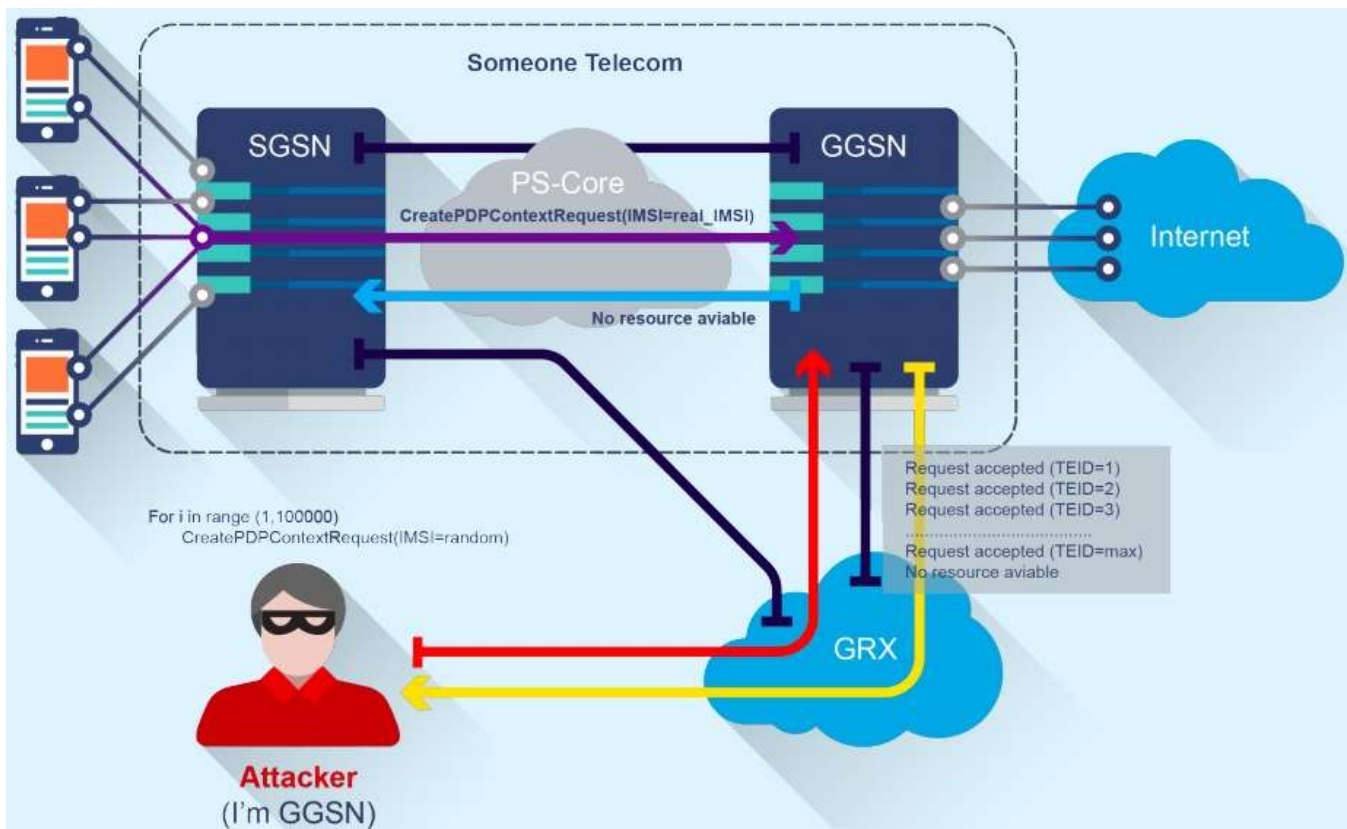
The PDP Context information is deleted, which causes disconnection of authorized subscribers.

At the same time, GGSN unilaterally closes tunnels and sends the responses on this event to the attacker.

A valid SGSN used by the subscriber to set up the connection doesn't have information about closing connections, so tunnels continue to occupy the hardware resources.

The subscriber's Internet stops working, but the connection is displayed as active.

**Result:** All subscribers connected to this GGSN will be disconnected. The amount of subscribers served by one GGSN is 100,000— 10,000,000.



## 2.2.5 Blocking the connection to the Internet

**Goal:** To block the establishment of new connections to the Internet.

**Attack vector:** An attacker conducts attacks from the GRX network or the operator's network.

**Description:** The attack is based on sending the «Create PDP context request» packets with IMSI list, thus the exhaustion of the available pool of PDP tunnels occurs.

For example, the maximum number of PDP Context Cisco 7200 with 256 MB of memory is 80,000, with 512 MB — 135,000: it is not difficult to brute force all possible combinations.

Moreover, more and more IP addresses from DHCP pool are issued and they may be exhausted.

It does not matter what will be exhausted first — the DHCP pool or the PDP pool,  
After all, GGSN will response with «No resource available» to all valid connection requests.

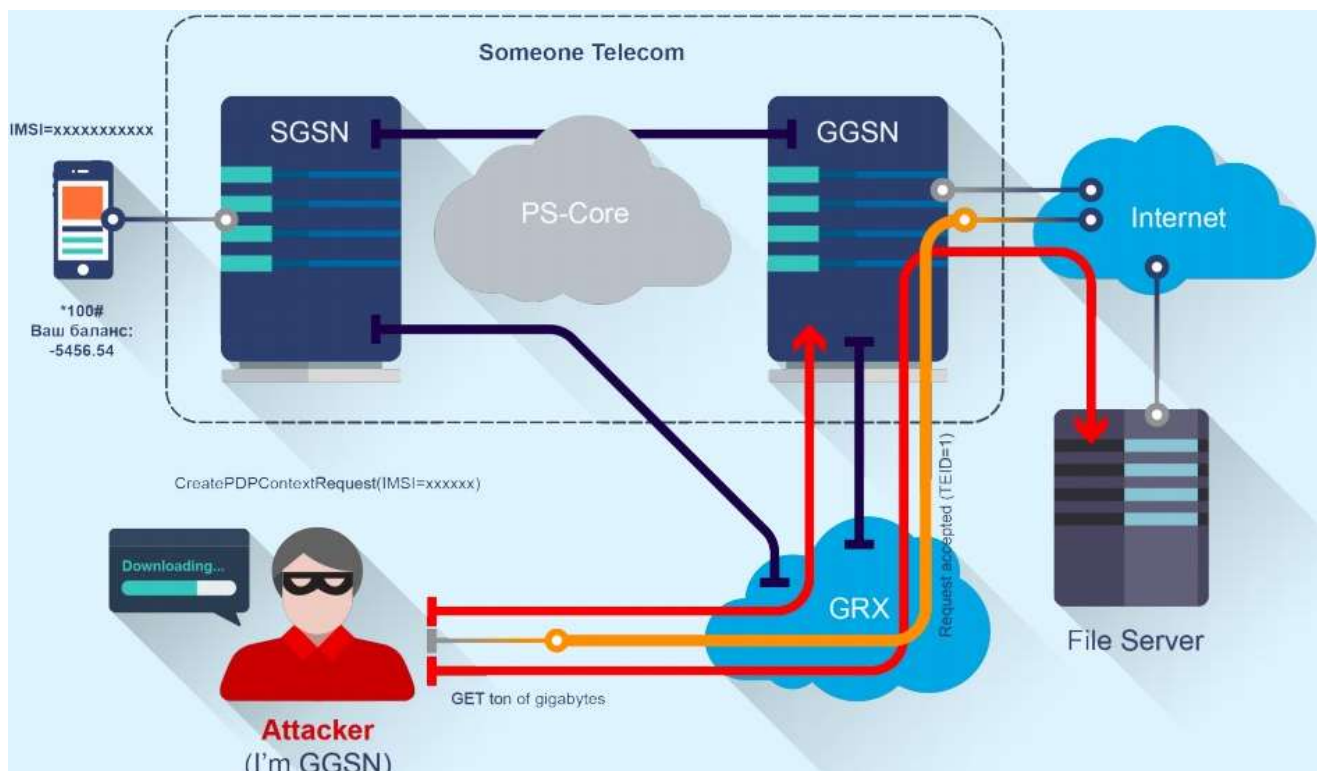
Moreover, GGSN cannot close tunnels, because when you try to close one, GGSN sends an attacker «Delete PDP context request» with the number of the tunnel to be closed.

If there is no response (actually, there isn't any response because an attacker does not want this to happen), GGSN sends such requests over and over again. The resources remain occupied.

In case of successful implementation of this attack, authorized subscribers will not be able to connect to the Internet and those who were connected will be disconnected as GGSN sends these tunnels to the attacker's address.

This attack is an analogue of the DHCP starvation attack at the GTP level.

**Result:** The subscribers of the attacked GGSN will not be able to connect to the Internet. The amount of subscribers served by one GGSN is 100,000–10,000,000.





## 2.2.6 Internet at the expense of others

**Goal:** The exhaustion of the subscriber's account and use of the connection for illegal purposes.

**Attack vector:** An attacker conducts attacks from the GRX network or the operator's network.

**Description:** The attack is based on sending the «Create PDP context request» packets with the IMSI of a subscriber known in advance.

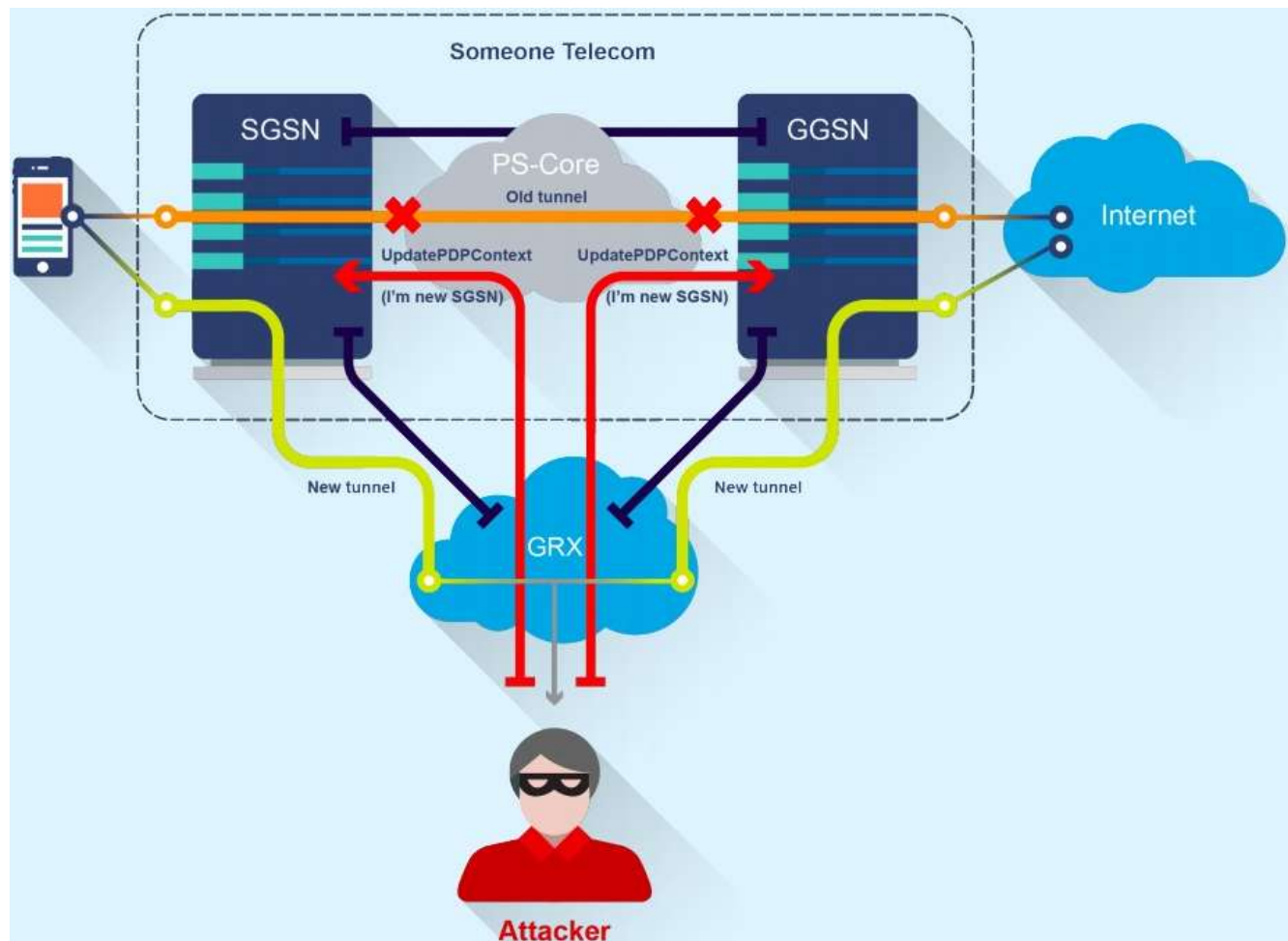
Thus, the subscriber's credentials are used to establish connection.

Unsuspecting subscriber will get a huge bill.

It is possible to establish connection via the IMSI of a non-existent subscriber, as subscriber authorization is performed at the stage of connecting to SGSN and GGSN receives already verified connections.

Since the SGSN is compromised, no verification is carried out.

**Result:** An attacker can connect to the Internet with the credentials of a legitimate user.



## 2.2.7 Data interception (Using a spoofed GSN addresses to SGSN and GGSN)

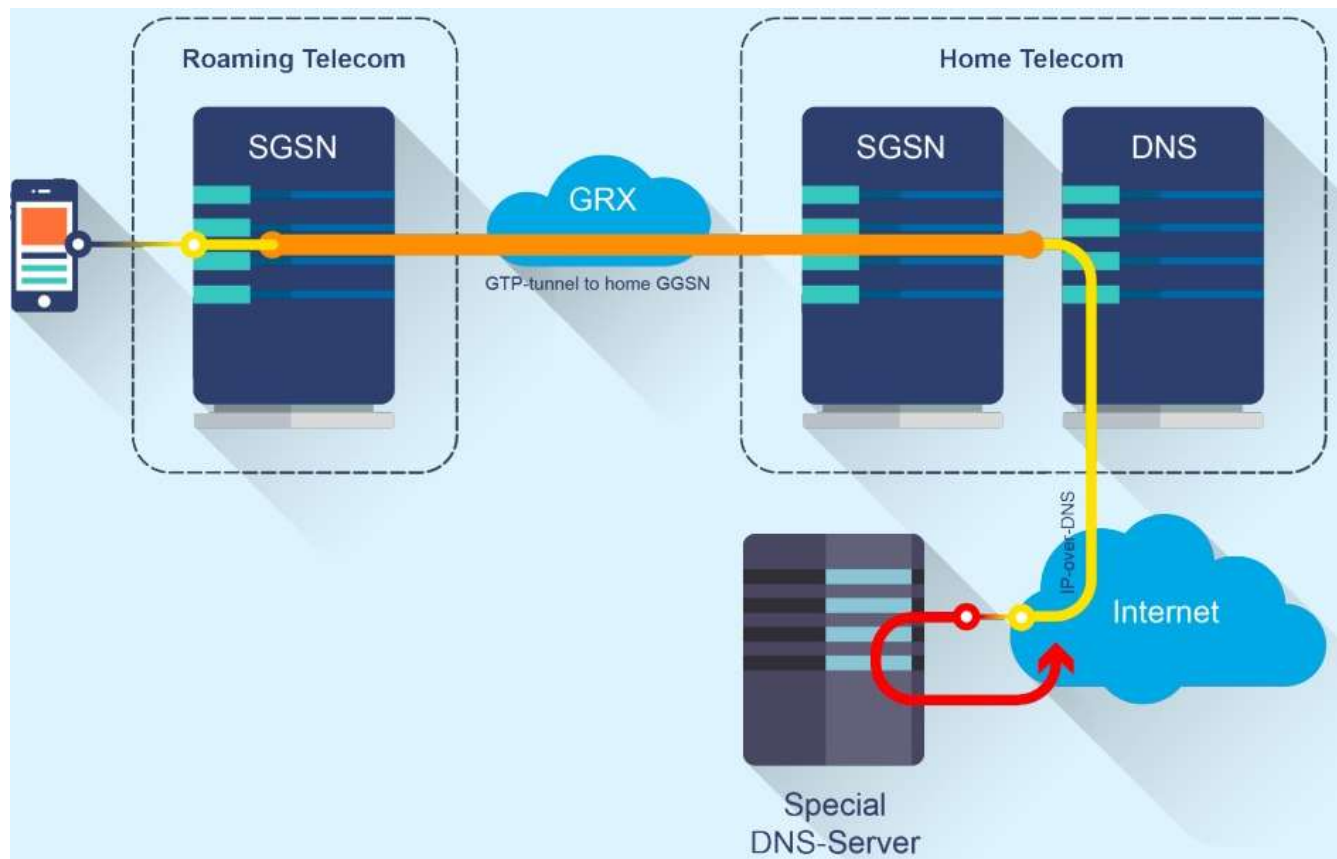
**Goal:** To listen to the traffic of the victim and conduct a fishing attack.

**Attack vector:** An attacker conducts attacks from the GRX network or the operator's network.

**Description:** An attacker can intercept data sent between the subscriber's device and the Internet by sending an «Update PDP Context Request» message with spoofed GSN addresses to SGSN and GGSN.

This attack is an analogue of the ARP Spoofing attack at the GTP level.

**Result:** Listening to traffic or spoofing traffic from the victim and disclosure of sensitive data.



## 2.2.8 DNS tunneling

**Goal:** To get non-paid access to the Internet from the subscriber's mobile station.

**Attack vector:** The attacker is the subscriber of a mobile phone network and acts through a mobile phone.

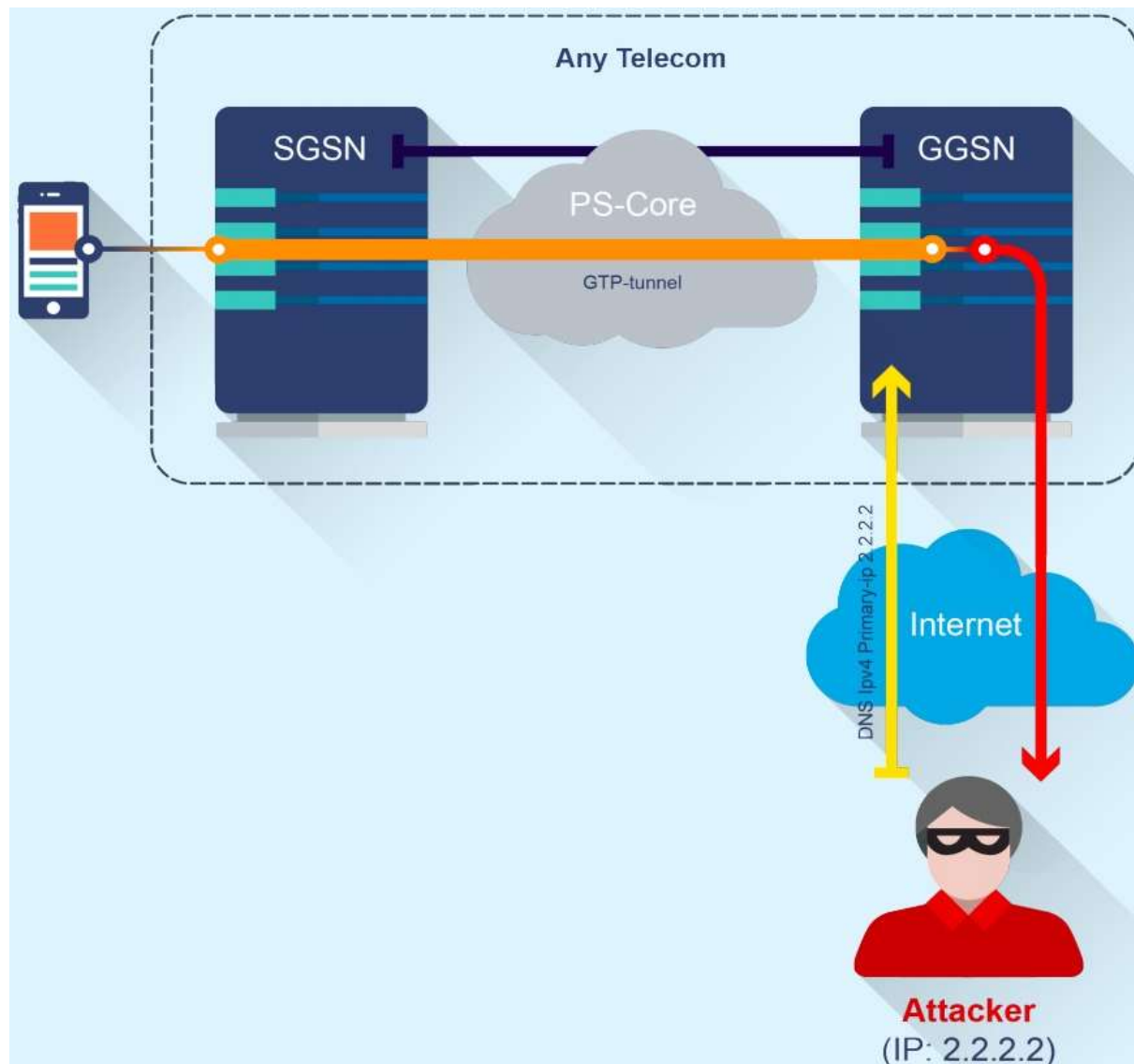
**Description:** This is a well-known attack vector, rooted in the days of dial-up, but the implementation of low-price and fast dedicated Internet access made it less viable.

However, this attack can be used in mobile networks, for example, in roaming when prices for mobile Internet are unreasonably high and the data transfer speed is not that important (for example, for checking email).

The point of this attack is that some operators do not rate DNS traffic, usually in order to redirect the subscriber to the operator's webpage for charging the balance.

An attacker can use this vulnerability by sending special crafted requests to the DNS server; to get access one needs a specialized host on the Internet.

**Result:** Getting non-paid access to the Internet at the expense of mobile operator.



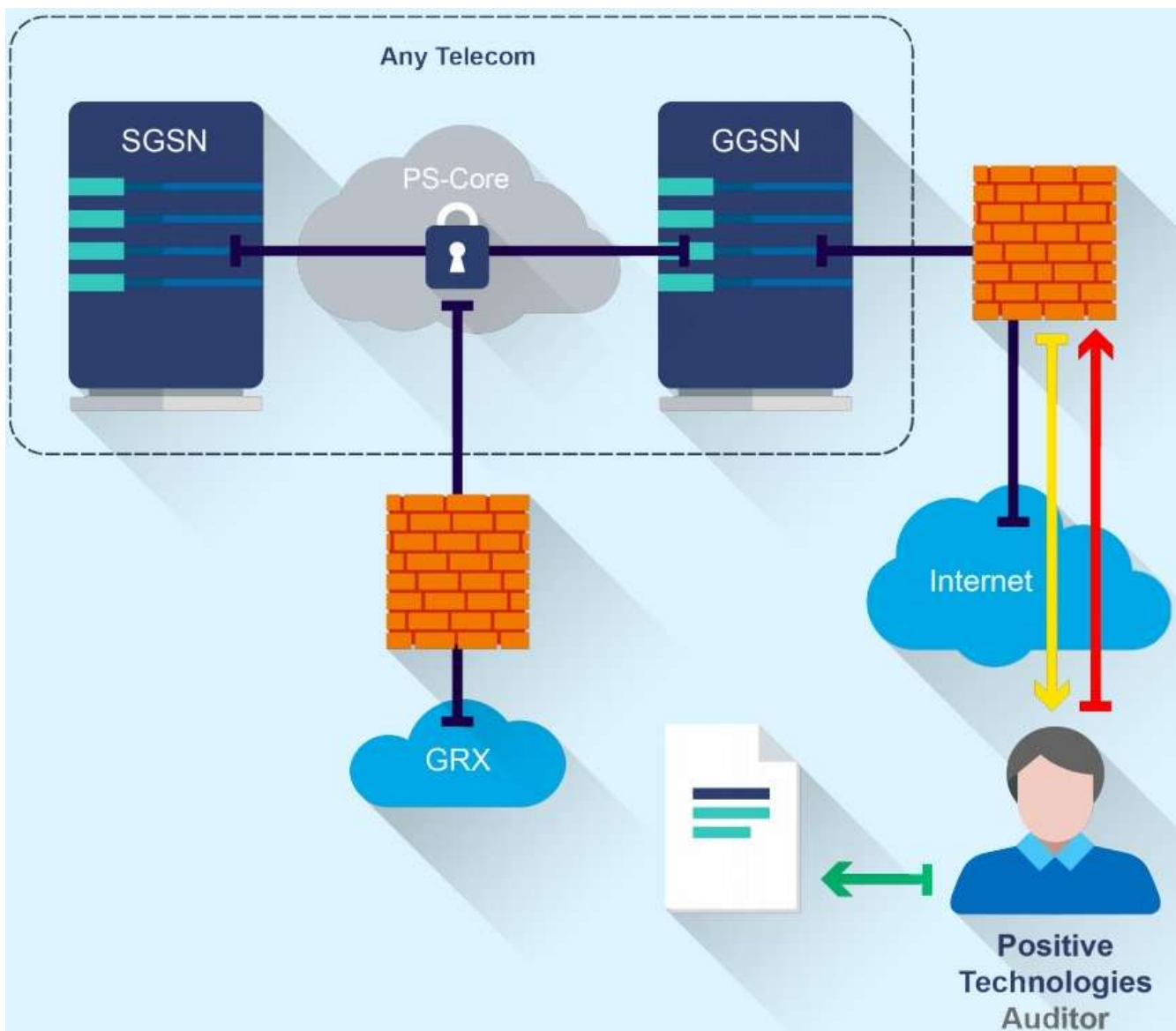
## 2.2.9 Substitution of DNS for GGSN

**Goal:** To listen to the traffic of the victim, to conduct a fishing attack.

**Attack vector:** An attacker acts through the Internet.

**Description:** If an attacker gets access to GGSN (which is quite possible as we could see), the DNS address can be spoofed with the attacker's address and all the subscriber's traffic will be redirected through the attacker's host. Thus, listening to all the mobile traffic of the subscriber is possible.

**Result:** An ability to listen to traffic or spoof traffic from all subscribers and then gather confidential data to engage it in fishing attacks.



## 2.3 VOIP Threats attack

- To perform VoIP information gathering, we need to collect as much useful information as possible about the target. As a start, you can do a simple search online. For example, job announcements could be a valuable source of information. For example, the following job description gives the attacker an idea about the VoIP:

**Job Description**

**Position:** SBC Voice Engineer / Architect (Sonus SBC 1000)  
**Location:** Remote  
**Job Status:** Project Based

Later, an attacker could search for vulnerabilities out there to try exploiting that particular system. Searching for phone numbers could also be a smart move, to have an idea of the target based on its voicemail, because each vendor has a default one. If the administrator has not changed it, listening to the voicemail can let you know about your target. If you want to have a look at some of the default voicemails, check <http://www.hackingvoip.com/voicemail.html>. It is a great resource for learning a great deal about hacking VoIP.

- Google hacking is an amazing technique for searching for information and online portals. We discussed Google hacking using Dorks. The following demonstration is the output of this Google Dork—in URL: Network Configuration Cisco:

### Network Configuration - Cisco Systems, Inc.

222.249.148.238/NetworkConfiguration

DHCP Server, 255.255.255.255. BOOTP Server, No. MAC Address, 0012008FA2DB. Host Name, SEP0012008FA2DB. Domain Name. IP Address, 222.249.148.238. Subnet Mask, 255.255.255.128. TFTP Server 1, 211.153.8.90. Default Router 1, 222.249.148.254. Default Router 2. Default Router 3. Default Router 4.

b

- You can find connected VoIP devices using the Shodan.io search engine:

Q

Explore
Enterprise Access
Contact Us

**TOTAL RESULTS**

71,449

**TOP COUNTRIES**

Italy	56,960
Germany	5,484
Taiwan	1,180
Korea, Republic of	1,013
United States	608

**TOP SERVICES**

SIP	58,082
SNMP	2,891
Telnet	2,398
HTTP	2,089
Telnet + SSL	1,624

**RELATED TAGS:** h34hdh3sd

**151.55.44.227**

Wind Telecomunicazioni

Added on 2015-01-26 16:30:43 GMT

Italy, Bergamo

[Details](#)

**151.49.156.41**

Wind Telecomunicazioni

Added on 2015-01-26 16:29:43 GMT


Italy, Ca' Bianca

[Details](#)

```
SIP/2.0 404 Not Found
From: <sip:nn@nn>;tag=root
To: <sip:nn2@nn2>;tag=c49e29-97172ce3-13c4-5506-181bcf-109314ee-181bcf
Call-ID: 50008
CSeq: 42 OPTIONS
User-Agent: DLink VoIP Stack
Supported: replaces,timer,100rel
Via: SIP/2.0/UDP nn;received=233.160.26.191;rport=26810;branch=foo
Content:...
```

- VoIP devices are generally connected to the internet. Thus, they can be reached by an outsider. They can be exposed via their web interfaces; that is why, sometimes leaving installation files exposed could be dangerous, because using a search engine can lead to indexing the portal. The following screenshot is taken from an online Asterisk management portal:

And this screenshot is taken from a configuration page of an exposed website, using a simple search engine query:

 <b>Network Setup</b> Cisco IP Phone CP-6921 ( SEPc89c1d37ed38 )		
<a href="#">Device Information</a>	DHCP Server	134.121.140.30
<a href="#">Network Setup</a>	MAC Address	C89C1D37ED38
<a href="#">Network Statistics</a>	Host Name	SEPc89c1d37ed38
<a href="#">Ethernet Information</a>	Domain Name	
<a href="#">Network</a>	IP Address	134.121.252.234
<a href="#">Device Logs</a>	Subnet Mask	255.255.255.0
<a href="#">Console Logs</a>	TFTP Server 1	
<a href="#">Core Dumps</a>	TFTP Server 2	
<a href="#">Status Messages</a>	Default Router 1	134.121.252.1
<a href="#">Debug Display</a>	Default Router 2	
<a href="#">Streaming Statistics</a>	Default Router 3	
<a href="#">Stream 1</a>	Default Router 4	
<a href="#">Stream 2</a>	Default Router 5	
	DNS Server 1	134.121.139.10
	DNS Server 2	134.121.80.36
	DNS Server 3	

- After collecting juicy information about the target, from an attacker perspective, we usually should perform scanning.

Banner grabbing is a well-known technique in enumeration, and the first step to enumerate a VoIP infrastructure is by starting a banner grabbing move.

In order to do that, using the Netcat utility would help you grab the banner easily, or you can simply use the Nmap script named banner: `nmap -sV --script=banner <target>`

```

root@kali: /home/ghost
File Edit View Search Terminal Help
root@kali: /home/ghost# nc -h
[vl.10-41]
connect to somewhere: nc [-options] hostname port[s] [ports] ...
listen for inbound: nc -l -p port [-options] [hostname] [port]
options:
-c shell commands      as '-e'; use /bin/sh to exec [dangerous!!]
-e filename            program to exec after connect [dangerous!!]
-b                    allow broadcasts
-g gateway             source-routing hop point[s], up to 8
-G num                source-routing pointer: 4, 8, 12, ...
-h                    this cruff
-i secs               delay interval for lines sent, ports scanned
-k                    set keepalive option on socket
-l                    listen mode, for inbound connects
-n                    numeric-only IP addresses, no DNS
-o file               hex dump of traffic
-p port               local port number
-r                    randomize local and remote ports
-q secs               quit after EOF on stdin and delay of secs
-s addr               local source address
-T tos                set Type Of Service
    
```



- For a specific vendor, there are a lot of enumeration tools you can use; **EnumIAX** is one of them. It is a built-in enumeration tool in Kali Linux to brute force Inter-Asterisk Exchange protocol usernames:

```
ghost@kali: ~  
File Edit View Search Terminal Help  
enumIAX 0.4a  
Dustin D. Trammell <dtrammell@tippingpoint.com>  
  
Usage: enumiax [options] target  
options:  
-d <dict> Dictionary attack using <dict> file  
-i <count> Interval for auto-save (# of operations, default 1000)  
-m # Minimum username length (in characters)  
-M # Maximum username length (in characters)  
-r # Rate-limit calls (in microseconds)  
-s <file> Read session state from state file  
-v Increase verbosity (repeat for additional verbosity)  
-V Print version information and exit  
-h Print help/usage information and exit  
ghost@kali:~$
```

- Automated Corporate Enumerator (ACE)** is another built-in enumeration tool in Kali Linux:

```
ghost@kali: ~  
File Edit View Search Terminal Help  
ghost@kali:~$ ace  
ACE v1.10: Automated Corporate (Data) Enumerator  
Usage: ace [-i interface] [-m mac address] [-t tftp server ip address] [-c cdp mode] [-v voice vlan id] [-r vlan interface] [-d verbose mode]  
  
-i <interface> (Mandatory) Interface for sniffing/sending packets  
-m <mac address> (Mandatory) MAC address of the victim IP phone  
-t <tftp server ip> (Optional) tftp server ip address  
-c <cdp mode 0|1> (Optional) 0 CDP sniff mode, 1 CDP spoof mode  
-v <voice vlan id> (Optional) Enter the voice vlan ID  
-r <vlan interface> (Optional) Removes the VLAN interface  
-d (Optional) Verbose | debug mode  
  
Example Usages:  
Usage requires MAC Address of IP Phone supplied with -m option  
Usage: ace -t <TFTP-Server-IP> -m <MAC-Address>
```

- svmap is an open source built-in tool in Kali Linux for identifying SIP devices. Type `svmap -h` and you will get all the available options for this amazing tool:

```
ghost@kali: ~  
File Edit View Search Terminal Help  
ghost@kali:~$ svmap -h  
Usage: svmap [options] host1 host2 hostrange  
Scans for SIP devices on a given network  
  
examples:  
  
svmap 10.0.0.1-10.0.0.255 172.16.131.1 sipvicious.org/22 10.0.1.1/24 1.1.1.1-20 1.1.2-20.* 4.1.*.*  
svmap -s session1 --randomize 10.0.0.1/8  
svmap --resume session1 -v  
svmap -p5060-5062 10.0.0.3-20 -m INVITE  
  
Options:  
--version show program's version number and exit  
-h, --help show this help message and exit  
-v, --verbose Increase verbosity  
-q, --quiet Quiet mode  
-p PORT, --port=PORT Destination port or port ranges of the SIP device - eg  
-p5060,5061,8000-8100  
-P PORT, --localport=PORT Source port for our packets  
-x IP, --external=IP
```



### 2.3.1 VOIP attack: DOS

**Denial-of-Service (DoS)** is a threat to the availability of a network. DoS could be dangerous too for VoIP, as ensuring the availability of calls is vital in modern organizations. Not only the availability but also the clearness of calls is a necessity nowadays. To monitor the QoS of VoIP, you can use many tools that are out there; one of them is CiscoWorks QoS Policy Manager 4.1:

Support / Product Support / End-of-Sale and End-of-Life Products / CiscoWorks QoS Policy Manager /

## CiscoWorks QoS Policy Manager 4.1

### Product Overview

Series: [CiscoWorks QoS Policy Manager](#) Status: Not Orderable

Latest Version: [CiscoWork QoS Policy Manager 4.1.2](#) End-of-Sale Date: 03-FEB-2014 [Details](#)

End-of-Support Date: 04-FEB-2017 [Details](#)

Documentation Downloads Communities

Top Categories

[Compatibility Information](#) [Install and Upgrade Guides](#) [More Categories](#)

To measure the quality of VoIP, there are some scoring systems, such as the **Mean Opinion Score (MOS)** or the R-value based on several parameters (jitter, latency, and packet loss). Scores of the mean opinion score range from 1 to 5 (bad to very clear) and scores of R-value range from 1 to 100 (bad to very clear). The following screenshot is taken from an analysis of an RTP packet downloaded from the Wireshark website:

rtp\_example.raw

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Filter: rtp

No.	Time	Source	Destination	Protocol	Length	Info
34	1.643045	10.1.3.143	10.1.6.18	RTP	294	PT=ITU-T G.711 PCMA,
35	1.673013	10.1.3.143	10.1.6.18	RTP	294	PT=ITU-T G.711 PCMA,
36	1.703144	10.1.3.143	10.1.6.18	RTP	294	PT=ITU-T G.711 PCMA,
37	1.733258	10.1.3.143	10.1.6.18	RTP	294	PT=ITU-T G.711 PCMA,
38	1.763370	10.1.3.143	10.1.6.18	RTP	294	PT=ITU-T G.711 PCMA,
39	1.793553	10.1.3.143	10.1.6.18	RTP	294	PT=ITU-T G.711 PCMA,
40	1.796448	10.1.6.18	10.1.3.143	RTP	294	PT=ITU-T G.711 PCMA,
41	1.822283	10.1.3.143	10.1.6.18	RTP	294	PT=ITU-T G.711 PCMA,
42	1.828461	10.1.6.18	10.1.3.143	RTP	294	PT=ITU-T G.711 PCMA,
43	1.852274	10.1.3.143	10.1.6.18	RTP	294	PT=ITU-T G.711 PCMA,
44	1.858319	10.1.6.18	10.1.3.143	RTP	294	PT=ITU-T G.711 PCMA,
45	1.882264	10.1.3.143	10.1.6.18	RTP	294	PT=ITU-T G.711 PCMA,
46	1.889465	10.1.6.18	10.1.3.143	RTP	294	PT=ITU-T G.711 PCMA,
47	1.912282	10.1.3.143	10.1.6.18	RTP	294	PT=ITU-T G.711 PCMA,
48	1.918568	10.1.6.18	10.1.3.143	RTP	294	PT=ITU-T G.711 PCMA,
49	1.942272	10.1.3.143	10.1.6.18	RTP	294	PT=ITU-T G.711 PCMA,
50	1.948433	10.1.6.18	10.1.3.143	RTP	294	PT=ITU-T G.711 PCMA,

Frame 34: 294 bytes on wire (2352 bits), 294 bytes captured (2352 bits)

Ethernet II, Src: 3ComCorp\_22:20:17 (00:04:76:22:20:17), Dst: Iskratel\_10:01:66 (00:d0:50:10:01:66)

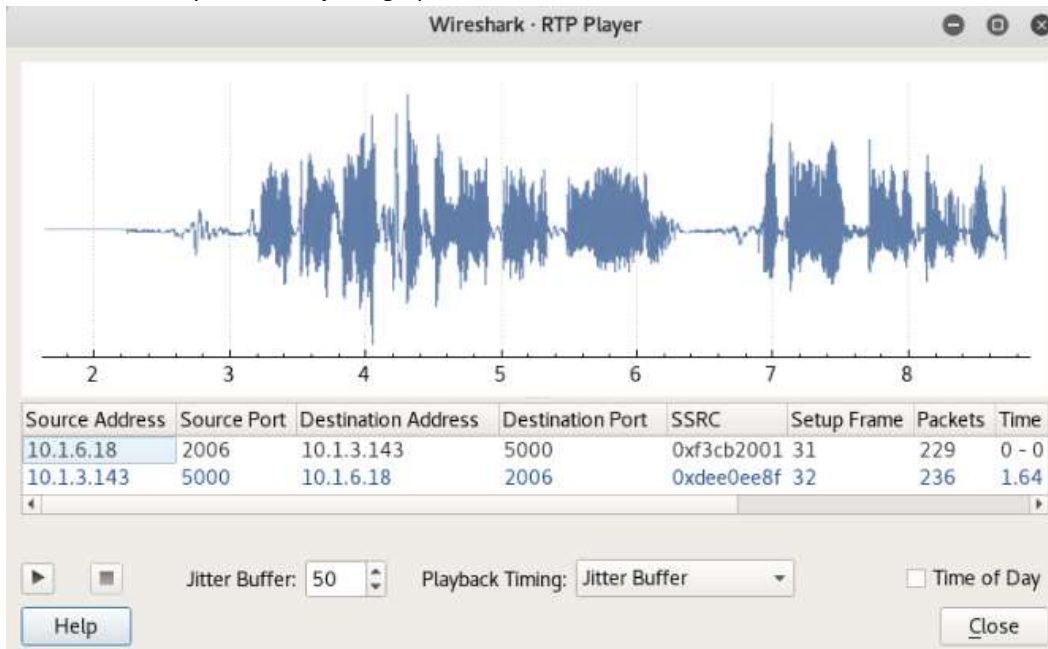
Internet Protocol Version 4, Src: 10.1.3.143, Dst: 10.1.6.18

User Datagram Protocol, Src Port: 5000, Dst Port: 2006

```

0000 00 d0 50 10 01 66 00 04 76 22 20 17 08 00 45 10 ..P..f..v" ...E.
0010 01 18 00 00 40 00 00 11 1c 23 0a 01 03 8f 0a 01 ....@.@. #.....
0020 06 12 13 88 07 d6 01 04 52 c2 80 88 e6 fd 00 00 ..... R.....
0030 00 f0 de e0 ee 8f d5 d5 d5 d5 d5 d5 d5 d5 .....
0040 d5 d5 d5 d5 d5 d5 d5 d5 d5 d5 d5 d5 .....
0050 d5 d5 d5 d5 d5 d5 d5 d5 d5 d5 d5 d5 .....
  
```

You can also analyze the RTP jitter graph:



VoIP infrastructure can be attacked by the classic DoS attacks. We saw some of them previously:

- Smurf flooding attack
- TCP SYN flood attack
- UDP flooding attack

One of the DoS attack tools is iaxflood. It is available in Kali Linux to perform DoS attacks. **IAX** stands for **Inter-Asterisk Exchange**.

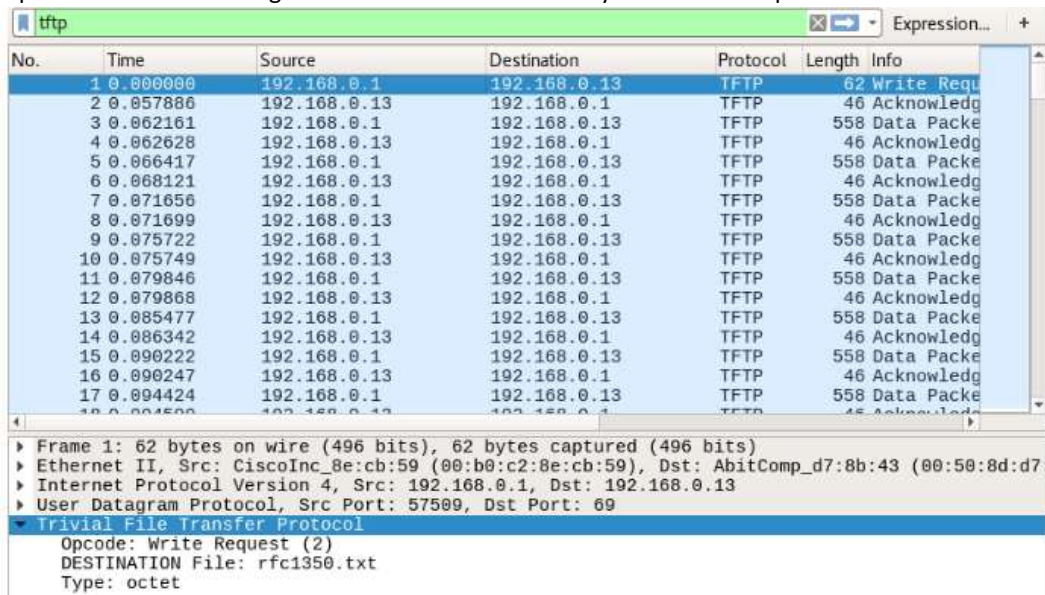
Open a Kali terminal and type `iaxflood <Source IP> <Destination IP> <Number of packets>`:

```
ghost@kali: ~  
File Edit View Search Terminal Help  
ghost@kali:~$ iaxflood -h  
usage: iaxflood sourcename destinationname numpackets  
ghost@kali:~$
```

The VoIP infrastructure can not only be attacked by the previous attacks attackers can perform packet Fragmentation and Malformed Packets to attack the infrastructure, using fuzzing tools.

### 2.3.2 VOIP attack: Eavesdropping

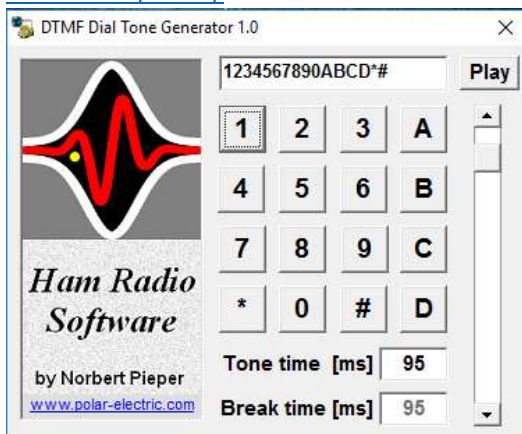
**Eavesdropping** is one of the most serious VoIP attacks. It lets attackers take over your privacy, including your calls. There are many eavesdropping techniques; for example, an attacker can sniff the network for TFTP configuration files while they contain a password. The following screenshot describes an analysis of a TFTP capture:



No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	192.168.0.1	192.168.0.13	TFTP	62	Write Request
2	0.057880	192.168.0.13	192.168.0.1	TFTP	46	Acknowledgment
3	0.062161	192.168.0.1	192.168.0.13	TFTP	558	Data Packet
4	0.062628	192.168.0.13	192.168.0.1	TFTP	46	Acknowledgment
5	0.066417	192.168.0.1	192.168.0.13	TFTP	558	Data Packet
6	0.068121	192.168.0.13	192.168.0.1	TFTP	46	Acknowledgment
7	0.071656	192.168.0.1	192.168.0.13	TFTP	558	Data Packet
8	0.071699	192.168.0.13	192.168.0.1	TFTP	46	Acknowledgment
9	0.075722	192.168.0.1	192.168.0.13	TFTP	558	Data Packet
10	0.075749	192.168.0.13	192.168.0.1	TFTP	46	Acknowledgment
11	0.079846	192.168.0.1	192.168.0.13	TFTP	558	Data Packet
12	0.079868	192.168.0.13	192.168.0.1	TFTP	46	Acknowledgment
13	0.085477	192.168.0.1	192.168.0.13	TFTP	558	Data Packet
14	0.086342	192.168.0.13	192.168.0.1	TFTP	46	Acknowledgment
15	0.090222	192.168.0.1	192.168.0.13	TFTP	558	Data Packet
16	0.090247	192.168.0.13	192.168.0.1	TFTP	46	Acknowledgment
17	0.094424	192.168.0.1	192.168.0.13	TFTP	558	Data Packet

Frame 1: 62 bytes on wire (496 bits), 62 bytes captured (496 bits) on interface 0  
 Ethernet II, Src: CiscoInc\_8e:cb:59 (00:b0:c2:8e:cb:59), Dst: AbitComp\_d7:8b:43 (00:50:8d:d7:8b:43)  
 Internet Protocol Version 4, Src: 192.168.0.1, Dst: 192.168.0.13  
 User Datagram Protocol, Src Port: 57509, Dst Port: 69  
 Trivial File Transfer Protocol  
 Opcode: Write Request (2)  
 DESTINATION File: rfc1350.txt  
 Type: octet

Also, an attacker can harvest phone numbers and build a valid phone numbers databases, after recording all the outgoing and ongoing calls. Eavesdropping does not stop there, attackers can record your calls and even know what you are typing using the **Dual-Tone Multi-Frequency (DTMF)**. You can use the DTMF decoder/encoder from this link <http://www.polar-electric.com/DTMF/>:



**Voice Over Misconfigured Internet Telephones (VOMIT)** is a great utility to convert Cisco IP Phone conversations into WAV files. You can download it from its official website <http://vomit.xtdnet.nl/>:

## vomit - voice over misconfigured[1] internet telephones

The **vomit** utility converts a Cisco IP phone conversation into a wave file that can be played with ordinary sound players. Vomit requires a tcpdump output file. Vomit is not a VoIP sniffer also it could be but the naming is probably related to H.323.

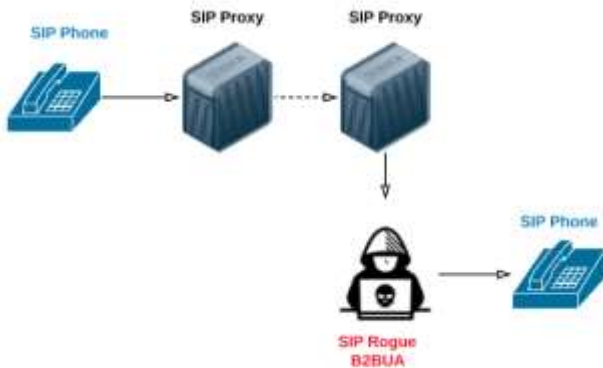
**Download**

- [vomit-0.2c.tar.gz](#) - Released 2004-01-02 (requires [libnet](#))
- [vomit-0.2.tar.gz](#) - Released 2001-12-12 (requires [libnet](#))
- [phone\\_dump.gz](#) - sample dump from a telephone conversation that I had at [CITI](#)

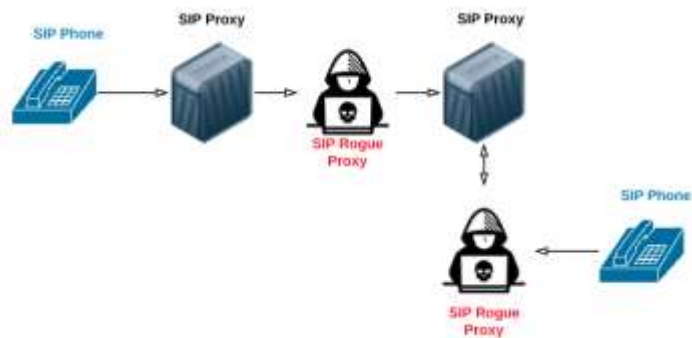
## 2.3.3 VOIP attack: SIP attacks

Another attacking technique is SIP rogues. We can perform two types of SIP rogues. From an attacker's perspective, we can implement the following:

**Rogue SIP B2BUA:** In this attacking technique, the attacker mimics SIP B2BUA:



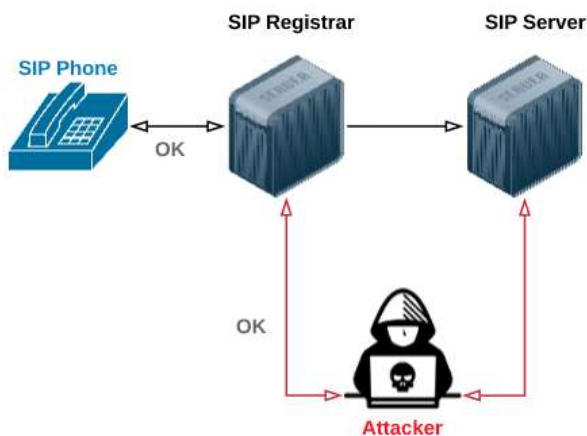
**SIP rogue as a proxy:** Here, the attacker mimics a SIP proxy:



## 2.3.4 VOIP attack: SIP registration hijacking

**SIP registration hijacking** is a serious VoIP security problem. Previously, we saw that before establishing a SIP session, there is a registration step. Registration can be hijacked by attackers.

During a SIP registration hijacking attack, the attacker disables a normal user by a Denial of Service, for example, and simply sends a registration request with his own IP address instead of that user's because, in SIP, messages are transferred clearly, so SIP does not ensure the integrity of signalling messages:





If you are a Metasploit enthusiast, you can try many other SIP modules. Open a Metasploit console by typing `msfconsole` and search SIP modules using `search SIP`:

```
ghost@kali: ~
File Edit View Search Terminal Help
+ -- ==[ Free Metasploit Pro trial: http://r-7.co/trymsp ]

msf > search SIP
[!] Module database cache not built yet, using slow search

Matching Modules
=====

  Name                               Disclosure Date  Rank    Description
  ----                               -
  auxiliary/scanner/sip/enumerator    normal          SIP Username Enumerator (UDP)
  auxiliary/scanner/sip/enumerator_tcp normal          SIP Username Enumerator (TCP)
  auxiliary/scanner/sip/options       normal          SIP Endpoint Scanner (UDP)
  auxiliary/scanner/sip/options_tcp   normal          SIP Endpoint Scanner (TCP)
  auxiliary/scanner/sip/sipdroid_ext_enum normal          SIPDroid Extension Grabber
  auxiliary/server/capture/sip        normal          Authentication Capture: SIP
  auxiliary/voip/sip_deregister        normal          SIP Deregister Extension
  auxiliary/voip/sip_invite_spoof     normal          SIP Invite Spoof
  exploit/windows/browser/aol_icq_downloadagent 2006-11-06     excellent America Online ICQ ActiveX Control Arbitrary File
Download and Execute
  exploit/windows/local/agnitum_outpost_acs 2013-08-02     excellent Agnitum Outpost Internet Security Local Privilege
Escalation
  exploit/windows/sip/aim_triton_cseq 2006-07-10     great    AIM Triton 1.0.4 CSeq Buffer Overflow
  exploit/windows/sip/sipxezphone_cseq 2006-07-10     great    SIPfoundry sipXezPhone 0.35a CSeq Field Overflow
  exploit/windows/sip/sipxphone_cseq 2006-07-10     great    SIPfoundry sipXphone 2.6.0.27 CSeq Buffer Overflow

msf >
```

To use a specific SIP module, simply type `use <module>`. The following interface is an example of SIP module usage

```
Terminal
File Edit View Search Terminal Help

= [ metasploit v4.12.22-dev ]
+ -- ==[ 1577 exploits - 906 auxiliary - 272 post ]
+ -- ==[ 455 payloads - 39 encoders - 8 nops ]
+ -- ==[ Free Metasploit Pro trial: http://r-7.co/trymsp ]

msf > use auxiliary/scanner/sip/options
msf auxiliary(options) > show options

Module options (auxiliary/scanner/sip/options):

  Name      Current Setting  Required  Description
  ----      -
  BATCHSIZE 256              yes       The number of hosts to probe in each set
  RHOSTS    [0.0.0.0]         yes       The target address range or CIDR identifier
  RPORT     5060              yes       The target port
  THREADS   10                yes       The number of concurrent threads
  TO        nobody            no        The destination username to probe at each host

msf auxiliary(options) >
```

## 2.3.5 VOIP attack: Spam over Internet Telephony

**Spam over Internet Telephony (SPIT)**, sometimes called **Voice spam**, is like email spam, but it affects VoIP. To perform a SPIT attack, you can use a generation tool called **spitter**.

## 2.3.6 VOIP attack: Embedding malware

**Malware** is a major threat to VoIP infrastructure. Your insecure VoIP endpoints can be exploited by different types of malware, such as Worms and VoIP Botnets.

Softphones are also a highly probable target for attackers. Compromising your softphone could be very dangerous because if an attacker exploits it, they can compromise your VoIP network. Malware is not the only threat against VoIP endpoints. VoIP firmware is a potential attack vector for hackers. Firmware hacking can lead to phones being compromised.

## 2.3.7 VOIP attack: Viproy test kit

**Viproy VoIP penetration testing kit (v4)** is a VoIP and unified communications services pentesting tool presented at Black Hat Arsenal USA 2014 by Fatih Ozavci:



### Viproy VoIP Penetration Testing and Exploitation Kit (v4.1)

Project Page : <https://www.github.com/fozavci/viproy-voipkit>  
Download : [Viproy\\_4.1](#)  
Author : [Fatih Ozavci](#)

To download this project, clone it from its official repository, <https://github.com/fozavci/viproy-voipkit>:

```
# git clone https://github.com/fozavci/viproy-voipkit.
```

The following project contains many modules to test SIP and Skinny protocols:

A terminal window titled 'ghost@security: ~/viproy-voipkit/modules/auxiliary/voip' showing the output of a 'ls' command. The terminal has a black background with white text. The command 'ls' is entered, and the output lists various Ruby modules for testing SIP and Skinny protocols, arranged in two columns.

```
ghost@security: ~/viproy-voipkit/modules/auxiliary/voip
ghost@security:~/viproy-voipkit/modules/auxiliary$ ls
spoof voip
ghost@security:~/viproy-voipkit/modules/auxiliary$ cd voip
ghost@security:~/viproy-voipkit/modules/auxiliary/voip$ ls
viproxy.rb                                viproy_sip_message.rb
viproy_boghe_invite_exploit_poc.rb        viproy_sip_negotiate.rb
viproy_boghe_msrp_exploit_poc.rb          viproy_sip_options.rb
viproy_cisco_autoregistration.rb          viproy_sip_proxybouncescan.rb
viproy_cucdm_callforward.rb               viproy_sip_register.rb
viproy_cucdm_speeddials.rb                viproy_sip_subscribe.rb
viproy_message_with_invite.rb             viproy_sip_trusthacking.rb
viproy_msrp_fuzzer_with_invite.rb          viproy_sip_udpampdos.rb
viproy_msrp_header_fuzzer_with_invite.rb  viproy_skinny_callforward.rb
viproy_msrp_with_invite.rb                viproy_skinny_call.rb
viproy_polycom_confextractor.rb            viproy_skinny_register.rb
viproy_sip_bruteforce.rb                  viproy_training_sample.rb
viproy_sip_enumerate.rb                   viproy_voip_mitmprxtcp.rb
viproy_sip_invite.rb                      viproy_voip_mitmprxudp.rb
viproy_sip_invite-sdptest.rb
ghost@security:~/viproy-voipkit/modules/auxiliary/voip$
```

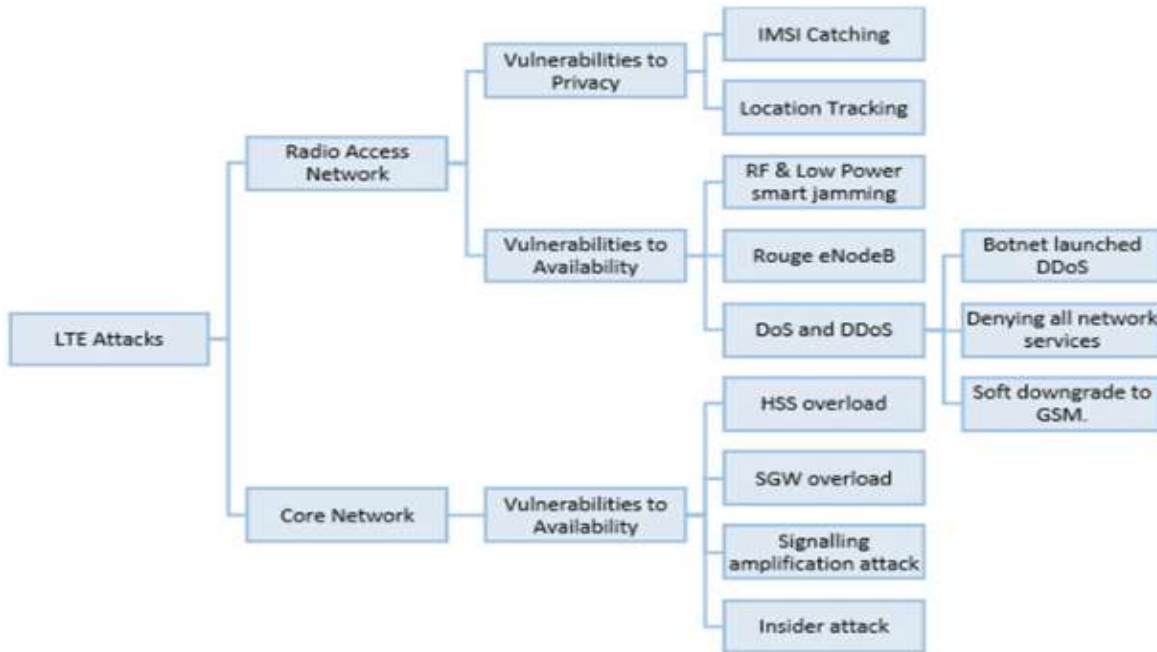
To use them, copy the lib, modules, and data folders to a Metasploit folder in your system.

Thus, in this article, we demonstrated how to exploit the VoIP infrastructure. We explored the major VoIP attacks and how to defend against them, in addition to the tools and utilities most commonly used by penetration testers.

If you've enjoyed reading this, do check out [Advanced Infrastructure Penetration Testing](#) to discover post-exploitation tips, tools, and methodologies to help your organization build an intelligent security system.

## 2.4 LTE threats attack

The vulnerabilities towards radio access network and core network respectively is depicted in the figure down below



### 2.4.1 IMSI Catching active and passive attack

- **When a mobile device is switched on and attempts a connection to the network:**
  - The only way to go through the authentication process is: the IMSI.
  - Secondly, during some event when network has never retrieved a Temporary Mobile Subscriber Identity (TMSI) or it is lost, for regular LTE operations, the mobile device has to disclose in the clear its IMSI in such circumstances.
- ✓ Since the IMSI is transmitted in the system information messages before the actual authentication and encryption takes place, this is precisely where the IMSI catcher exploits the network.
- **An IMSI catching can happen in two separate ways:**
  - **Passive way** is to simply observe/eavesdrop the wireless traffic over the air interface and store all the observed IMSIs by decoding system information messages.
  - **A semi-passive** adversary is, in addition to passive monitoring, able to trigger signaling messages to subscribers using interfaces and actions that are legitimately available in LTE or in higher layer systems. For example, a semi-passive adversary can trigger paging messages to subscribers by sending a message via a social network or initiating a call. The adversary is assumed to be aware of social identities of subscribers. For example, these identities can be a Facebook profile or a mobile phone number of the subscriber. A semi-passive adversary is analogous to the 'honest-but-curious' or 'semi-honest' adversary model used for cryptographic protocols
  - **And Active way**, a rogue eNodeB set-up can be accomplished, which will impersonate the real network and simply command each mobile device in its vicinity to identify itself. These commands are forced to disclose user identity: the IMSI.

Disclosure of the IMSI can compromise user information, location information, and even conversation information.



## 2.4.2 Location tracking

- **Method 1: Passive attacks** can retrieve IMSI or GUTI to decide whether the target user is present in that area.
- The Cell Random Network Temporary Identifier (C-RNTI) is a PHY layer identifier, uniquely defined per device within a given cell.
- The figure down below show the C-RNTI assignment during RACH procedure in radio access network. By examining pull notifications in social media applications or silent text messages, an attacker can identify the current C-RNTI of the mobile user's UE during RACH procedure.
- Now, a passive eavesdropper can look for the probable user location in the obtained Tracking Area (TA).

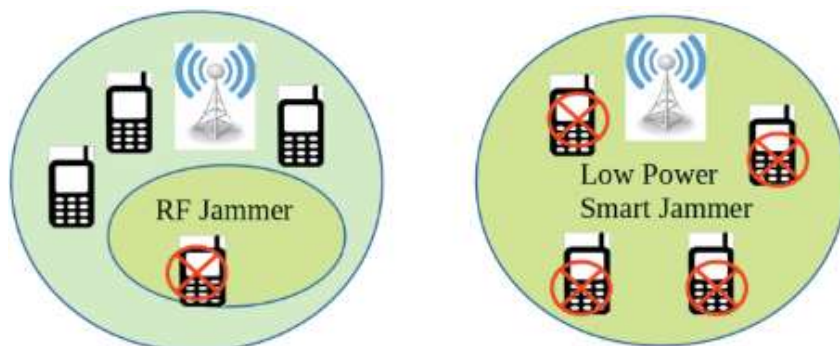


- **Method 2: Also with a passive attack** can take place during handover process; knowing that handovers are network triggered in LTE.
- **Method 3: with semi-passive attacks** (For precise tracking of user location) can produce signaling messages through Volte calls or social media applications like WhatsApp or Facebook and confirm a particular cell within the Tracking Area (TA) for retrieval of paging information.
- **Method 4: with active attacks:** an attacker deploys a rogue eNodeB in the network and reprimands the vulnerabilities present in RRC protocol stack for a more fine-grained location tracking.
- The attacker's main concern is to take advantage of Measurement Report (MR) or Radio Link Failure (RLF) report messages which provides signal strengths, even GPS coordinates under some circumstances of the victim UE.
- The distance between the victim UE and the rogue eNodeB can be easily calculated using trilateration technique or directly from GPS coordinates.

## 2.4.3 RF and Low Power Smart Jamming.

RF and smart jamming are commonly present attacks at PHY layer and to great extent can make network appear unresponsive

- **RF jammers** deliberately disrupt radio communications by decreasing the Signal-to-Noise Ratio (SNR) of the received signal without raising any alerts, causing Denial of Service (DoS).
- The first instance of RF jamming occurred in GSM networks and it was proposed that a local jamming of GSM base station can be accomplished with floods of text messages.
- In legacy GSM networks, text messages share resources with control signaling channels which make jamming quiet feasible.



- Why **Smart Jamming in LTE?**, However, in LTE standards, text message traffic does not share resources with control signaling channels, thus making text based flooding attack on RAN impossible.
- Smart jamming can be performed by saturating one or more of the control channels in both downlink and uplink that are necessary for the UE to access the spectrum.
- Instead of saturating the entire control channel, the attacker will target narrower control channels leading to less power consumption. The Physical Control Format Indicator Channel (PCFICH) is distinctly a sparse channel, turning it to be more vulnerable to sophisticated jamming techniques.

The PCFICH essentially carries all control information's required to decode Physical Downlink Control Channel (PDCCH) for the UE. According to LTE specifications, since the radio resource allocation of broadcast and downlink synchronization channels (PBCH, PDCH, PSS and SSS) is known beforehand, smart jamming is an easy improvement over basic RF jamming.

- ✓ An attacker would block downlink reception of one or more of the aforementioned control channels; by simply tuning a commercially available off-the-shelf (OTS) radio jammer at the targeted center frequency of the LTE band and transmission bandwidth of at least 1.08 MHz.
- ✓ Similar attack would be possible in uplink control channels too and; given the fact that an attacker is challenging lower-power UEs, the required power to accomplish the jamming will be relatively low.

## 2.4.4 Rogue eNodeB

- **A rogue eNodeB is a fake base station, illegitimately setup in the LTE network and controlled by an attacker through various widely available open-source software platforms.**
- Under normal conditions, UE always try to scan the nearby eNodeBs and prefers to establish connection with the eNodeB having the highest signal strength.
- **How to build a Rogue eNodeB? Before answer the question we need to understand the difference between Rogue GSM and LTE.**
  - ✓ During GSM attacks, the rogue BTS was operated with signal power higher than the neighboring base stations.
  - ✓ However, in LTE this procedure will not sustain, as per LTE specifications, when the UE is quite nearer to a serving eNodeB, it apparently avoids scanning neighboring eNodeBs to reduce power utilization.
- **But great news is that a new feature referred as "absolute priority based cell reselection" in LTE can be exploited to overcome the aforementioned limitation and establish a rogue eNodeB.**
  - ✓ In this feature, the UE in IDLE state should periodically scan and attach to eNodeB operating with the highest priority frequency.
- Hence, during active attacks, the UE will forcibly attach to rogue eNodeB operating on a frequency having highest cell reselection priority, even when it is closely located to a real eNodeB.
- This cell reselection priority list is present in system information messages broadcasted by a real eNodeB.
- By means of passive or semi-passive attacks, these cell reselection priority list can be sniffed and apparently used to configure the rogue eNodeB.
- **Once the rogue eNodeB is established** with necessary network parameters of a real eNodeB, an attacker can now launch potentially severe threats like :
  - Man-In-The-Middle (MITM) attacks,
  - DoS,
  - adding malicious messages in attach process,
  - deny mobile services to the UEs and
  - downgrade to a non-LTE network

## 2.4.5 DoS and DDoS Attacks

Denial of Service (DoS) and Distributed Denial of Service (DDoS) both can potentially disrupt the LTE network.

- Traditionally, the **DoS can be performed by sending floods of messages to a target** network and exhaust its bandwidth resources, eventually making the target network unavailable to legitimate UEs.
- Apart from this, other DoS attacks that can lead to network failure are downgrading to a non-LTE network or denying all network service.
- In **DDoS attacks, an attacker can produce heavy volume traffic by launching a botnet** managed via Command and Control Centers or hacked UEs that are well synchronized. Prominent attacks based on DoS and DDoS are discussed here.

### 2.4.5.1 Botnet Launched DDoS Attack

- **The DDoS attacks can potentially be launched by a botnet of mobile devices or a high volume of malicious traffic** against the LTE network.

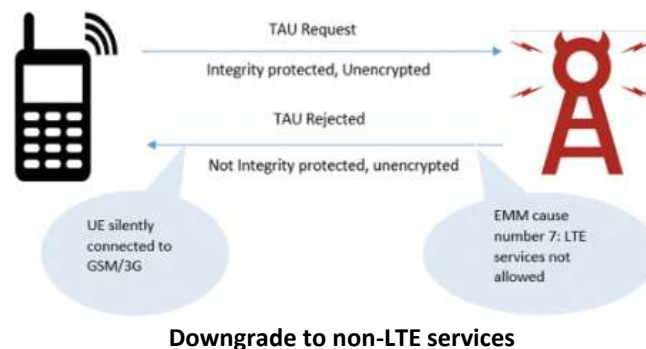
The key idea behind such attack is, many botmasters activate all botnet nodes simultaneously and create bandwidth congestion on both downlink and uplink; resulting into temporary large-scale saturation of the LTE network.

The severity of such DoS/DDoS attacks is of large extend in the core network (EPC) as compared to radio access network (RAN).

- **The upsurge in the occurrence of mobile malware and affluent virus spread** have improved the likelihood of placing various DoS attacks. Henceforth, a mobile device based botnet introduces a powerful attack vector against LTE network by means of high volume malicious traffic or signalling messages in the network; resulting in a new way of DDoS attack.

### 2.4.5.2 Soft Downgrade to Non-LTE Services

- An attacker can establish a rogue eNodeB that will reject the UE from accessing LTE services:
- **Method 1:** by abusing the Reject causes messages like “TAU Reject”, which are transmitted without any integrity protection.
  - ✓ Since, no security keys is required for the transmission of “TAU Reject” messages, the rogue eNodeB could target any LTE mobile user within its vicinity for temporary DoS.

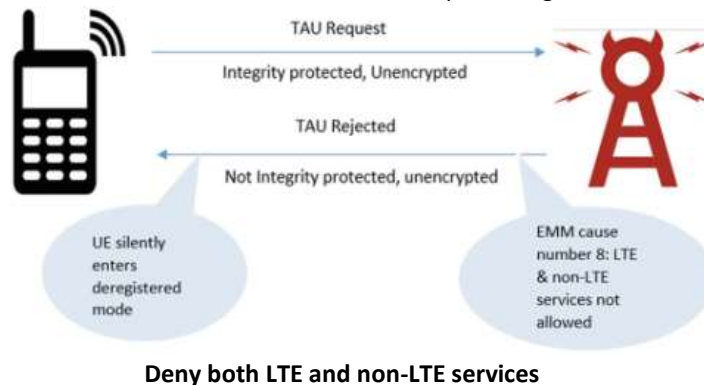


- **Method 2:** A similar threat is also feasible with “Service Reject/Attach” messages.
  - ✓ When the UE transmits “TAU Request” message to a rogue eNodeB, it is still attached to the real network, hence under the NAS security context, this message is integrity protected but not encrypted. This would turn out as an advantage to the attacker, who could easily decode it and responds with a “TAU Reject” message (EMM cause number 7: LTE services not allowed) which as per LTE specifications, does not require integrity protection.
  - ✓ Upon the reception of “TAU Reject” message, the UE will accept the reject cause and proceeds to act further, by removing all existing services associated with the real network.
  - ✓ As a result, the UE considers itself invalid for any LTE services unless a rebooting or USIM re-insertion happens.
  - ✓ Furthermore, the UE will not search for or send TAU Attach request to any nearby legitimate LTE network, triggering temporary Denial of Service (DoS) and is of less impact.

- **However, in context to gaining network services, the UE may search for GSM or 3 G network.**
- By downgrading to non-LTE networks like 2G or 3G, a DoS threat can be triggered by an attacker; which would not only open doors to attacks like a full man in the middle attack, active eavesdropping to phone calls or text messages, but also make complete loss of LTE services.
- As long as the UE does not loose connectivity to non-LTE networks, the user might not even realize it is connected by GSM or 3G network.

#### 2.4.5.3 Denying All Network Services

- **A similar threat can be accomplished by placing “TAU Reject” message with EMM cause number 8: “LTE and non-LTE services not allowed”.**
- In such scenario, the UE again considers itself invalid for any LTE services unless a rebooting or USIM re-insertion happens.
- The UE further enters into a state of “EMM-DEREGISTERED”, which makes it unknown to MME, consequently causing a persistent Denial of Service (DoS).
- The UE will never attempt to connect GSM, 3G or LTE networks despite being available.



#### 2.4.6 HSS Overload

- **Therefore, a DoS/DDoS attack achieved by means of HSS overload can severely obstruct the network operation and demote network services.**
- The HSS overload can happen when an attacker disguising a legitimate UE, constantly transmit fake IMSIs to HSS.
- Consequently, the HSS has to generate excessive authentication vectors for the UE to complete authentication process.
- This repetitive generation of authentication vectors will force HSS to consume excessive computational resources, definitely leading to HSS overload.

## 2.4.7 SGW Saturation

- Serving Gateway (SGW) may face saturation due to threats like:
  - **flood of “bearer setup messages” to the SGW**
- And a **programmable mobile phone incessantly triggering Tracking Area Update (TAU)** procedure in a short period of time.
  - ✓ During the signaling procedure, MME implements the necessary security mechanism for Tracking Area Update (TAU) that includes the authentication and integrity check of context request message. This guarantees correct signaling and legitimate users, but signaling integrity takes place before user authentication in LTE network.
  - ✓ Therefore, MME may unknowingly presume the initiating device as an already validated user and will not undergo authentication process unless signaling integrity is broken.
  - ✓ This opens the door to DoS/DDoS threats against MME through illegitimate users. The MME sends Create Bearer Request to the new Serving Gateway (SGW) whenever the UE move towards a new TA.
- **Now, if the MME is compromised by an attacker**, it will send floods of bearer setup messages to the new SGW in a very short span of time, apparently leading to SGW overload.
- Also, if a programmable mobile phone incessantly triggers TAU procedure through a stored program in a short span of time, these requests are forwarded to SGW, which again can lead to SGW overload.

## 2.4.8 Signaling Amplification Attacks

Practically, mobile networks are deployed to sustain peak traffic hours and does not have adequate radio resources available for each user at the same time.

- The scarce spectrum gives rise to advanced wireless techniques, which can lead to more efficient reuse of idle resources. For example, the RRC layer in the LTE network is responsible for reassigning radio resources from an established UE to another UE, when the connection of the former goes idle for a short span of time.
- This reassignment of radio resources takes place when an inactivity timer expires, thus triggering a disconnection of radio bearer between the established UE and the core network.
- ✓ A significant amount of control plane messages are exchanged among many nodes within the core network during each instance of radio bearer setup and disconnection.
- ✓ And these signaling overhead, if not efficiently monitored, can lead to large-scale saturation of core network, which subsequently can get exploited in context of DDoS.
- **So how this attack can be happen?**
- **Method 1:** Signaling amplification attack like launching a **botnet** of mobile device could force each UE to constantly establish and release connection with the core network.
- **Method 2:** Another threat to EPC in reference to DDoS can also take place, when a piece of **malware** can trigger all UEs to reboot simultaneously, thereby overloading the EPC with registration requests.
- ✓ It is also necessary to consider that, HSS too is involved in a significant number of signaling processes at the EPC; thus can as well suffer from signaling amplification attack.

## 2.4.9 Insider Attack

The threats to availability of wireless communication networks must take in account the problems associated with insider threat, which are often assumed unlikely to occur.

Also, with the current security threat landscape and impact of new player like Advanced Persistent Threat (APT), insider attacks have become highly relevant.

A very well-funded attacker can maliciously persuade an insider who has privileges to access core network elements, to remotely or physically shut down a particular network node in the core network. This would eventually pose an attack against availability by obstructing the normal radio communication in the LTE core network.

- **The insider attacks at RAN can be :**

- Shutdown of eNodeB,
- Purposefully jamming LTE
- Downgrade to non-LTE networks
- Launching botnet of mobile devices.

- **At core network, the insider attacks could:**

- Open doors to potentially global breakdowns like shutdown of HSS, SGW saturation or any node damage.
- The impact of the insider attacks would not be global unless the affected node is HSS or SGW.

## 2.5 VOLTE threats attack

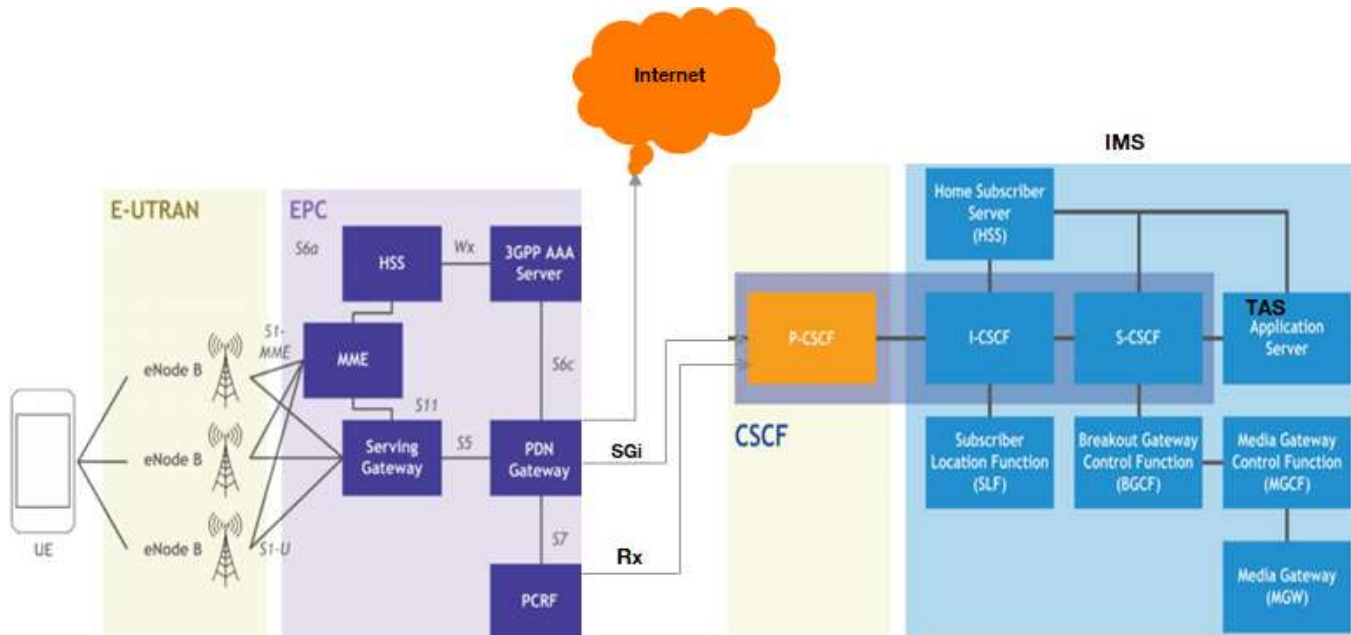
Voice over LTE (VoLTE) carries voice over 4G networks by the help of IMS core network, without IMS there is no VoLTE, Its call quality is higher than the other VoIP variants, in addition to providing better coverage.

VoLTE, as well as the other voice technologies, faces various threats from attackers.

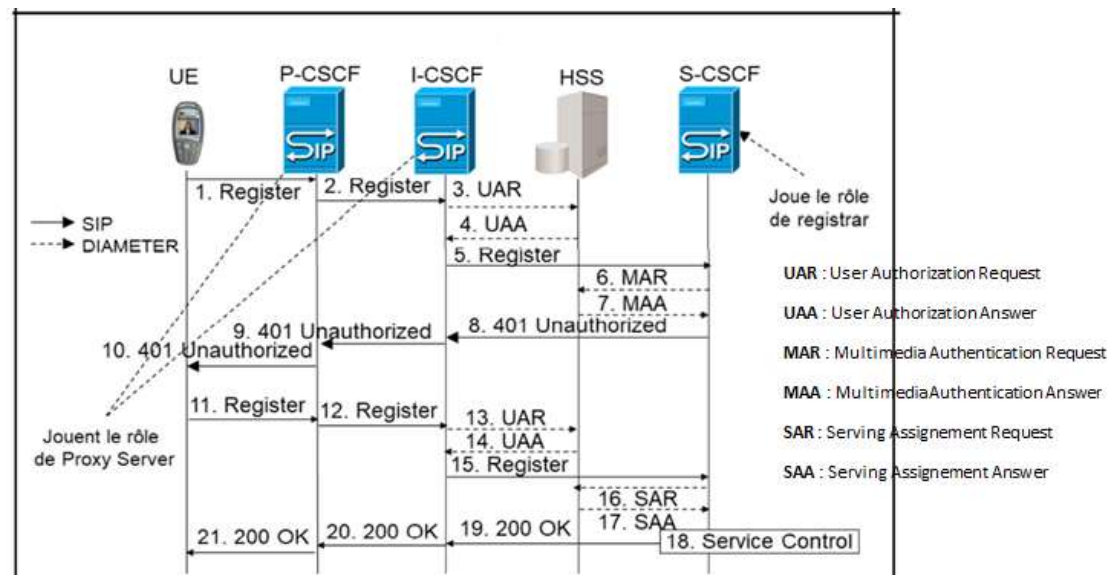
- Sniffing VoLTE interfaces
- Exposed keys in GSM SIM
- User location manipulation
- Roaming information manipulation
- Side channel attack

In another way to hack volte catch LTE

### 2.5.1 VOLTE architecture



### 2.5.2 VOLTE attachement





Here is a typical IMS SIP registration call flow:

1. The IMS client attempts to register by sending a **REGISTER** request to the P-CSCF.
2. The P-CSCF forwards the REGISTER request to the I-CSCF.
3. The I-CSCF polls the HSS for data used to decide which S-CSCF should manage the REGISTER request. The I-CSCF then makes that decision.
4. The I-CSCF forwards the REGISTER request to the appropriate S-CSCF.
5. The S-CSCF typically sends the P-CSCF a 401 (UNAUTHORIZED) response as well as a challenge string in the form of a “number used once” or “nonce”.
6. The P-CSCF forwards the 401 – UNAUTHORIZED response to the UE.
7. Both the UE and the network have stored some Shared Secret Data (SSD), the UE in its ISIM or USIM and the network on the HSS. The UE uses an algorithm per RFC 33101 (e.g. AKAv2-MD5) to hash the SSD and the nonce.”
8. The UE sends a REGISTER request to the P-CSCF. This time the request includes the result of the hashed nonce and SSD.
9. The P-CSCF forwards the new REGISTER request to the I-CSCF.
10. The I-CSCF forwards the new REGISTER request to the S-CSCF.
11. The S-CSCF polls the HSS (via the I-CSCF) for the SSD, hashes it against the nonce and determines whether the UE should be allowed to register. Assuming the hashed values match, the S-CSCF sends 200 – OK response to the P-CSCF. At this point an IPSec security association is established by the P-CSCF.
12. The P-CSCF forwards the 200 – OK response to the UE.

## References

### SS7

- # Things Hackers Can Do with Your Cell Phone Number | Reader's Digest
- # Overview - Cellular Network Infrastructure - Open Source Mobile Communications
- # SS7 Protocols for GSM | Telecom crash courses
- # GSM Network Connection to SS7 Networks - Broadband Telecommunications
- # Why SS7 was needed in GSM? - technopediasite-Ultimate Resource For Telecom Technical Support
- # SIGTRAN PROTOCOL STACK PDF
- # How To Scan Ports With SCTP On Nmap [Complete] - ElderNode Blog
- rfc4666
- # Technical-report-on-the-SS7-vulnerabilities-and-their-impact-on-DFS-transactions\_f-1-1.pdf
- # comst-2971757-pp.pdf - 08984216.pdf
- # Gotta Catch 'Em All: Understanding How IMSI-Catchers Exploit Cell Networks | Electronic Frontier Foundation
- # SCTPscan: SCTP network and port scanner - P1 Security
- # Queue | Telecom Signalling Attacks - SS7 to All IP - PDFCOFFEE.COM
- # 3G: Practical Attacks Against the SS7 Signaling Protocol - Security Compass Advisory
- # Some Notes on Utilizing Telco Networks for Penetration Tests – Insinuator.net
- # GSM Security Map
- # Overview of GSM, GPRS, and UMTS
- # 31c3-ss7-locate-track-manipulate.pdf
- # Hacking-related-books/Hacking mobile network via SS7 - interception, shadowing and more by Dmitry Kurbatov.pdf at master · pathakabhi24/Hacking-related-books · GitHub
- # SS7\_Vulnerability\_2017\_A4.ENG\_.0003.03.pdf
- # SIGNALING SYSTEM 7 (SS7) SECURITY REPORT - PDF Free Download
- # Attacking SS7-2009-Philippe Langlois-P1security-HES-v10.key - HES2010-planglois-Attacking-SS7.pdf
- # bh-eu-07-langlois.ppt - bh-eu-07-langlois-ppt-apr19.pdf
- # Hacking-related-books/Telecommunications Infrastructure - Security SS7 Signalling Security by Philippe Langlois.pdf at master · pathakabhi24/Hacking-related-books · GitHub
- # Philippe Langlois - SCTPscan Finding entry points to SS7 Networks & T...
- #  
[https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&cad=rja&uact=8&ved=2ahUKEwizrN3\\_scb0AhVCz4UKHaw3DLcQFnoECBIQAQ&url=https%3A%2F%2Fwww.cellusys.com%2Fdownload%2Fss7-vulnerabilities.pdf&usg=AOvVaw3LV\\_m\\_AluA-sujAyDY29mZ](https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&cad=rja&uact=8&ved=2ahUKEwizrN3_scb0AhVCz4UKHaw3DLcQFnoECBIQAQ&url=https%3A%2F%2Fwww.cellusys.com%2Fdownload%2Fss7-vulnerabilities.pdf&usg=AOvVaw3LV_m_AluA-sujAyDY29mZ)
- # Attacks on SS7.pdf
- # Signalling Security in Telecom SS7/Diameter/5G - Interconnect Security SS7-Diameter.pdf
- # Telecom security from ss7 to all ip all-open-v3-zeronights

### GTP

- # [GPRS Tunneling Protocol \(GTP\)](#)
- # [Vulnerabilities of Mobile Internet \(GPRS\)](#)
- # [GTP Deployments](#)
- # [Monitoring GTP Traffic | Securing GTP and SCTP Traffic User Guide for Security Devices | Juniper Networks TechLibrary](#)
- # [3GPP TS 29.274 - 29274-d70.pdf](#)
- # [Wireless Internet Networking Carriers Perspective ChihLin I Wireless](#)
- # [GTPing, How To](#)

## Diameter

- # [Diameter](#)
- # [rfc6733](#)
- # [Diameter Protocol Explained: Diameter AVP Structure](#)
- # [3GPP spec skeleton - ts\\_129109v060900p.pdf](#)
- # [Diameter Protocol Explained: Diameter Routing Agent \(DRA\)](#)
- # [What Is AAA?](#)
- # [Radius vs Diameter](#)
- # [Diameter and 3GPP - Cellusys](#)
- # [Philippe Langlois - Hacking HLR HSS and MME core network elements](#)

## VOIP

- # [IP Telephony and VoIP Tutorial - Comprehensive Guide](#)
- # [How to attack an infrastructure using VoIP exploitation \[Tutorial\] | Packt Hub](#)

## GSM

- # [Hacking GSM: Building a Rogue Base Station to Hack Cellular Devices](#)
- # [Step by Step guide on how to create 2G network at your own home – Information Technology Blog](#)
- # [GSM with Osmocom Part 4: The Base Station Controller \(BSC\) – Nick vs Networking](#)
- # [How to Build an IMSI Catcher to Intercept GSM traffic](#)
- # [dpkg - How to remove/install a package that is not fully installed? - Ask Ubuntu](#)
- # [command-not-found.com – osmo-bts-virtual](#)
- # [Setting up Yate and YateBTS with the bladeRF · Nuand/bladeRF Wiki · GitHub](#)

## SMS

- # [Quickstart With Kannel. Recently , I got opportunity to work in... | by Sudeep Parajuli | Medium](#)
- # [SMS, appels et courriers électroniques indésirables et/ou frauduleux | Arcep](#)
- # [Kannel 1.4.5 User's Guide](#)

## LTE

- # [P1security-LTE Pwnage v2 PL.pptx - D1T2 - Philippe Langlois - Hacking HLR HSS and MME Core Network Elements.pdf](#)
- # [Top 10 Cyber Threats to Private 5G/LTE Networks - Security Boulevard](#)
- # [7-deadly-threats-4g.pdf](#)
- # [LTE :Mobile Network Security](#)
- # [Paper Title \(use style: paper title\) - 20151031\\_100157.pdf](#)
- # [\(PDF\) Security Threats Against LTE Networks: A Survey: 6th International Symposium, SSCC 2018, Bangalore, India, September 19–22, 2018, Revised Selected Papers](#)
- # [securecomm\\_camera-ready.pdf](#)
- # [1510.07563.pdf](#)
- # [Microsoft Word - BH-whitepaper-LTE and IMSI catcher myths.docx - eu-15-Borgaonkar-LTE-And-IMSI-Catcher-Myths-wp.pdf](#)
- # [How to create an EVIL LTE Twin. Be very careful when playing with any... | by Adam Toscher | Medium](#)
- # [LTE Phone Number Catcher: A Practical Attack against Mobile Privacy](#)
- # [\[REPO\]@Telematika | W00t3k/Awesome-Cellular-Hacking](#)
- # [How to install GNU Radio, FFTW, RTL SDR, GrOsmoSDR, and more using PyBombs with dependencies, by rpm/deb or build from source | sMyles](#)

- # [us-20-Quintin-Detecting-Fake-4G-Base-Stations-In-Real-Time.pdf](#)
- # [Detecting false base stations in mobile networks - Ericsson](#)
- # [Easy 4G LTE IMSI Catchers for Non-Programmers.pdf](#)
- # [Hacking Cellular Networks - Lin Huan - UE Security.pdf](#)
- # [Blog – 4G and 5G reference software](#)
- # [https://www.synacktiv.com/ressources/synacktiv\\_mobile\\_communications\\_attacks.pdf](https://www.synacktiv.com/ressources/synacktiv_mobile_communications_attacks.pdf)

## Volte

- # [VoLTE in IMS | Real Time Communication](#)
- # [IMS VoLTE Architecture - Voice Over LTE Tutorial](#)
- # [VoLTE Roaming and Interconnection Standard Technology - vol15\\_2\\_037en.pdf](#)
- # [VoLTE Call Flow and Procedures - Voice Over IP Tutorial](#)

## 5G

- # [5G Security Vulnerabilities detailed by Positive Technologies; ITU-T and 3GPP 5G Security specs - Technology Blog](#)
- # [PFCP - Wikipedia](#)
- # [A guide to 5G network security insight report - Ericsson](#)
- # [5G-Implementation-Guideline-v2.0-July-2019.pdf](#)
- # [5G Protocol Stack - User Plane/Control Plane | NETMANIAS](#)

## 2G 4G VOLTE Hack

- # [alex14324/ss7](#)
- # [SigPloiter/GTScan: The Nmap Scanner for Telco](#)
- # [mngp25/OpenLTE: An open source 3GPP LTE implementation.](#)
- # [open5gs/open5gs: Open5GS is a C-language Open Source implementation for 5G Core and EPC, i.e. the core network of LTE/NR network \(Release-16\)](#)
- # [Wooniety/srsLTE-Sniffer: Stuff for srsLTE IMSI catcher](#)
- # [srsran/srsRAN: Open source SDR 4G/5G software suite from Software Radio Systems \(SRS\)](#)
- # [SigPloit – Telecom Signaling Exploitation Framework – SS7, GTP, Diameter & SIP – Julio Della Flora](#)
- # [ss7MAPer – A SS7 pen testing toolkit – Insinuator.net](#)
- # [P1 Labs » Presenting QCSuper: a tool for capturing your 2G/3G/4G air traffic on Qualcomm-based phones](#)
- # [5 best open source bladerf projects.](#)
- # [ernw/ss7MAPer: SS7 MAP \(pen-\)testing toolkit. DISCONTINUED REPO, please use: https://github.com/0xc0decafe/ss7MAPer/](#)
- # [SecuraBV/SIPWatcher](#)
- # [proceedings-2016/05 LTE Security and Protocol Exploits.md at master · shmoocon/proceedings-2016 · GitHub](#)
- # [使用GnuRadio + OpenLTE + SDR 搭建4G LTE 基站（上） TYINY的博客-CSDN博客](#)

## android

- # [How to Check if Your Android Phone is Rooted](#)
- # [Kali NetHunter | Kali Linux Documentation](#)
- # [GitHub - urbanadventurer/Android-PIN-Bruteforce: Unlock an Android phone \(or device\) by bruteforcing the lockscreen PIN. Turn your Kali Nethunter phone into a bruteforce PIN cracker for Android devices! \(no root, no adb\)](#)
- # [GitHub - Ondrik8/HARD device attack](#)

## Training

- # [Telecom Security Hands-on Course | Training | Course | Training Center - TeleScope](#)
- # [Mobile Device Hacking with SDR | Training Live Streams](#)
- # [3-DAY TRAINING 6 – Hacking Mobile Networks with Software Defined Radios « JD-HITBSecConf2018 – Beijing](#)
- # [Trainings | P1 Security | Telecom Security Network World Leader](#)
- # [4G IMSI Catcher | IMSI Catcher | IMEI Catcher | TMSI Catcher | LTE catcher](#)
- # [Electromagnetic Field GSM Network - Lime Microsystems](#)
- # [CableLabs Launches 10G Challenge: Powering the Future of Broadband Innovation](#)
- # [5G Penetration Testing and Ethical Hacking Training - Tonex Training](#)
- # [Utiliser un Raspberry Pi pour détecter les IMSI Catchers | Silicon](#)
- # [Ensuring SS7 Network Security - Newsletter](#)